ACORDO DE SUBCONTRATAÇÃO DO TRATAMENTO DE DADOS PESSOAIS

O presente Acordo de Subcontratação do Tratamento de Dados Pessoais integra as Condições Gerais de Contratação (CGC) e as Condições Específicas (doravante, em conjunto, o "Contrato"), ao abrigo do qual a SESAME HR atuará na qualidade de Subcontratante e o CLIENTE na qualidade de Responsável pelo Tratamento.

Acordo de Tratamento de Dados Pessoais sujeito ao RGPD

O presente Acordo de Subcontratação do Tratamento de Dados Pessoais apenas será aplicável caso o CLIENTE e/ou a SESAME HR estejam sujeitos ao disposto no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados, "RGPD").

CLÁUSULAS

Cláusula 1.ª – Objeto

Para efeitos da execução das obrigações previstas no Contrato, o Subcontratante poderá aceder a dados pessoais sob responsabilidade do Responsável pelo Tratamento.

Cláusula 2.ª – Identificação da informação abrangida e operações de tratamento

No âmbito da execução das obrigações decorrentes do presente Acordo, o Responsável pelo Tratamento disponibiliza ao Subcontratante determinados dados pessoais, através da sua introdução em qualquer dos Serviços contratados.

Compete ao Responsável pelo Tratamento, por si ou através dos Utilizadores Autorizados, definir as categorias de dados e os titulares dos dados que serão objeto de tratamento por parte do Subcontratante.

São autorizadas todas as operações de tratamento necessárias para a execução do Contrato.

Cláusula 3.ª – Duração

O presente Acordo entra em vigor na data de aceitação do Contrato. Trata-se de um acordo acessório ao Contrato principal, pelo que a sua vigência encontra-se vinculada à duração deste último.

Cláusula 4.ª – Obrigações do Responsável pelo Tratamento

Compete ao Responsável pelo Tratamento, para além do cumprimento das demais obrigações previstas no presente Acordo de Subcontratação do Tratamento, a realização das seguintes tarefas:

a) Cumprir todas as medidas técnicas e organizativas necessárias para garantir a segurança do tratamento, bem como dos locais, equipamentos, sistemas, programas e pessoas envolvidas nas operações de tratamento dos dados pessoais, conforme estipulado na legislação aplicável em vigor a cada momento;

b) Fornecer ao Subcontratante os dados a que se refere a cláusula 2.ª do presente Acordo, bem como as instruções necessárias para a realização do tratamento dos dados nos termos definidos pelo Responsável;

c) Assegurar, em colaboração com o Subcontratante, o exercício dos direitos dos titulares dos dados afetados pelo tratamento, designadamente os direitos de acesso, retificação, apagamento, oposição, limitação do tratamento, portabilidade dos dados e a não ser sujeito a decisões individuais automatizadas;

d) Realizar, sempre que necessário, uma avaliação de impacto sobre a proteção de dados pessoais relativamente às operações de tratamento a executar pelo Subcontratante;

e) Zelar, antes e durante a execução do tratamento, pelo cumprimento, por parte do Subcontratante, da legislação aplicável em matéria de proteção de dados;

f) Supervisionar o tratamento, incluindo a realização de inspeções e auditorias;

g) Comunicar ao Subcontratante qualquer alteração aos dados pessoais fornecidos, a fim de permitir a respetiva atualização.

Cláusula 5.ª – Dever de informação e fundamento jurídico

O Responsável pelo Tratamento garante que cumpriu o dever de prestar aos titulares dos dados todas as informações exigidas no momento da recolha dos dados pessoais, nos termos do disposto nos artigos 12.º, 13.º e 14.º do RGPD, consoante aplicável.

O Responsável pelo Tratamento garante que dispõe de um fundamento jurídico adequado para o tratamento dos dados pessoais, em conformidade com os princípios da eficácia, necessidade e proporcionalidade, ponderando a existência de outras medidas de proteção menos intrusivas, prevenindo efeitos discriminatórios e assegurando as garantias adequadas.

O Subcontratante não será, em caso algum, responsável pelo incumprimento ou cumprimento defeituoso do dever de informação, nem pela inexistência de um fundamento jurídico apropriado para o tratamento por parte do Responsável.

Cláusula 6.ª – Obrigações do Subcontratante

O Subcontratante declara e garante, perante o Responsável pelo Tratamento, o seguinte:

1. Que utilizará os dados pessoais objeto de tratamento, bem como aqueles que venha a recolher para esse fim, exclusivamente para a finalidade prevista no presente encargo. Em nenhum caso poderá utilizar os dados para finalidades próprias;

2. Que tratará e utilizará os dados pessoais a que tenha acesso apenas de acordo com as instruções do Responsável pelo Tratamento e em conformidade com as finalidades previstas no Contrato.

   As instruções relativas ao tratamento dos dados e às atividades confiadas ao Subcontratante deverão ser comunicadas por escrito.

   Caso o Subcontratante considere que o cumprimento de determinada instrução do Responsável possa implicar uma violação da legislação aplicável em matéria de proteção de dados, comunicará de imediato tal facto ao Responsável.
   Nessa comunicação, solicitará ao Responsável que altere, revogue ou confirme a instrução em causa, podendo suspender o seu cumprimento até à receção de uma decisão formal do Responsável.

3. Que, quando aplicável, manterá por escrito um registo de todas as categorias de atividades de tratamento realizadas por conta do Responsável, contendo todas as informações exigidas pelo artigo 30.º do RGPD;

4. Que assegurará a confidencialidade e o sigilo relativamente aos dados pessoais a que tenha acesso no âmbito da prestação dos Serviços;

5. Que não comunicará dados pessoais a terceiros, salvo mediante autorização expressa do Responsável pelo Tratamento ou nos casos legalmente permitidos.

   O Subcontratante poderá, todavia, comunicar dados a outros subcontratantes do mesmo Responsável, em conformidade com as instruções por este emitidas. Neste caso, o Responsável identificará previamente e por escrito a entidade destinatária, os dados a comunicar e as medidas de segurança a aplicar para a referida comunicação.

6. Que disponibilizará ao Responsável pelo Tratamento toda a informação necessária para demonstrar o cumprimento das obrigações previstas no Contrato;

7. Que prestará a assistência necessária ao Responsável para efeitos da realização de auditorias ou inspeções, efetuadas pelo próprio Responsável ou por auditor designado por este. As auditorias poderão ser realizadas periodicamente, de forma programada ou ad hoc, mediante notificação prévia e com um prazo razoável, durante o horário laboral habitual do Subcontratante;

8. Que garantirá que todas as pessoas autorizadas a tratar dados pessoais assumiram, de forma expressa e por escrito, o compromisso de respeitar as medidas de

segurança estabelecidas e de manter a confidencialidade dos dados. O cumprimento desta obrigação deverá ficar devidamente documentado pelo Subcontratante e disponível para consulta do Responsável;

9. Que designou um Encarregado da Proteção de Dados ("Data Protection Officer" — DPO), cujos dados de contacto são os seguintes: legal@sesametime.com;

10. Que colaborará com o Responsável no cumprimento das respetivas obrigações legais e lhe prestará apoio, sempre que tal se revele necessário e seja por este solicitado, nomeadamente:
    (i) na realização de avaliações de impacto sobre a proteção de dados pessoais a que tenha acesso;
    (ii) na condução de consultas prévias junto da autoridade de controlo competente.

Cláusula 7.ª – Destino dos Dados

Com o termo da prestação dos Serviços, o Subcontratante devolverá ao Responsável pelo Tratamento todos os dados pessoais a que tenha tido acesso, bem como quaisquer cópias existentes, de acordo com as instruções que para o efeito lhe sejam transmitidas, nos termos do disposto na Cláusula 13.ª do presente Acordo.

O Subcontratante poderá conservar uma cópia dos dados devidamente bloqueada, apenas durante o período em que possam emergir responsabilidades decorrentes da execução da prestação dos Serviços.

Cláusula 8.ª – Notificação de violações de segurança dos dados

O Subcontratante notificará o Responsável pelo Tratamento, sem demora injustificada e, em qualquer caso, no prazo máximo de 24 horas, sobre qualquer incidente, suspeito ou confirmado, relacionado com a proteção de dados pessoais no âmbito da sua esfera de responsabilidade. Designadamente, o Subcontratante compromete-se a comunicar ao Responsável qualquer operação de tratamento considerada ilícita ou não autorizada, bem como qualquer perda, destruição, dano, acesso indevido ou outro incidente que configure uma violação de segurança dos dados pessoais. A notificação deverá ser acompanhada de todas as informações relevantes que permitam a adequada documentação e comunicação da ocorrência às autoridades competentes ou aos titulares dos dados afetados.

Adicionalmente, o Subcontratante prestará toda a assistência necessária ao Responsável no cumprimento das obrigações de notificação previstas no RGPD, nomeadamente nos artigos 33.º e 34.º, bem como em qualquer outra norma aplicável, presente ou futura, que venha a alterar ou complementar tais obrigações.

Cláusula 9.ª – Exercício de direitos pelos titulares dos dados

O Subcontratante fornecerá ao Responsável pelo Tratamento todas as informações e/ou documentação que este solicite, com vista a dar resposta aos pedidos de exercício de direitos que possa receber da parte dos titulares dos dados pessoais tratados.

O Subcontratante deverá disponibilizar essa informação dentro de prazos razoáveis e, em qualquer caso, com antecedência suficiente que permita ao Responsável cumprir os prazos legalmente estabelecidos para a resposta aos pedidos dos titulares.

Quando os titulares dos dados exercerem os seus direitos de acesso, retificação, apagamento, oposição, limitação do tratamento, portabilidade dos dados ou a não serem sujeitos a decisões individuais automatizadas junto do Subcontratante, este deverá comunicar tal facto ao Responsável pelo Tratamento através do endereço eletrónico legal@sesametime.com.

Essa comunicação deverá ser efetuada de forma imediata, por forma a garantir o cumprimento dos prazos legais aplicáveis, e, em qualquer caso, no prazo máximo de dois dias úteis após a receção do pedido, devendo ser acompanhada de toda a informação relevante que permita ao Responsável a sua adequada resolução.

Cláusula 10.ª – Segurança

No que respeita às medidas técnicas e organizativas de segurança, o Subcontratante obriga-se a implementar mecanismos adequados que assegurem:

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

b) A reposição da disponibilidade e o acesso aos dados pessoais de forma atempada, em caso de incidente físico ou técnico;

c) A verificação, avaliação e apreciação regulares da eficácia das medidas técnicas e organizativas implementadas, de forma a garantir a segurança do tratamento;

d) A pseudonimização e cifragem dos dados pessoais, quando aplicável.

As Partes acordam, em especial, um conjunto de medidas de segurança que o Subcontratante se compromete a implementar, conforme descrito no Apêndice A ao presente Acordo de Subcontratação do Tratamento.

Caso o Responsável, após a formalização do Contrato, exija ao Subcontratante a adoção ou manutenção de medidas de segurança distintas das previstas no referido Apêndice, ou caso tais medidas se tornem obrigatórias por força de disposições legais futuras, e estas impliquem um impacto significativo nos custos de prestação dos Serviços, o Subcontratante e o Responsável acordarão as medidas contratuais adequadas para refletir o impacto financeiro dessas alterações no preço dos Serviços.

Cláusula 11.ª – Subcontratação

O Responsável pelo Tratamento concede uma autorização geral ao Subcontratante para que este possa subcontratar parte dos Serviços a terceiros (doravante designados por **Suboperadores**).

O Subcontratante deverá informar previamente o Responsável pelo Tratamento acerca dos tratamentos que pretende subcontratar, identificando de forma clara e inequívoca a entidade Suboperadora e os respetivos dados de contacto.

A subcontratação poderá ter lugar desde que o Responsável pelo Tratamento não manifeste oposição no prazo de quinze (15) dias após a comunicação referida.

O Subcontratante compromete-se a exercer a diligência devida na seleção de Suboperadores, devendo escolher apenas aqueles que ofereçam garantias suficientes de aplicação de medidas técnicas e organizativas adequadas, de modo a assegurar que o tratamento subcontratado esteja em conformidade com o disposto no RGPD e salvaguarde os direitos dos titulares dos dados.

O Suboperador, na qualidade de subcontratado do tratamento, estará igualmente obrigado a cumprir todas as obrigações impostas ao Subcontratante e a seguir as instruções definidas pelo Responsável pelo Tratamento, nos termos do presente Acordo.

O Subcontratante deverá regular a relação com o Suboperador através de contrato escrito, garantindo que este fica sujeito às mesmas condições — incluindo instruções, obrigações, medidas de segurança e requisitos formais — aplicáveis ao Subcontratante, no que respeita ao adequado tratamento dos dados pessoais e à proteção dos direitos dos titulares.

Em caso de incumprimento por parte do Suboperador, o Subcontratante manter-se-á plenamente responsável perante o Responsável pelo Tratamento pelo cumprimento integral das obrigações constantes do presente Acordo.

A lista dos Suboperadores autorizados pelo Responsável pelo Tratamento encontra-se anexa ao presente Acordo como Apêndice B.

Cláusula 12.ª – Transferências internacionais de dados

O Subcontratante não procederá a transferências internacionais de dados pessoais sob responsabilidade do Responsável pelo Tratamento, salvo se:

a) Dispuser de autorização prévia e expressa do Responsável pelo Tratamento; ou
b) As referidas transferências estiverem devidamente regularizadas nos termos dos artigos 45.º, 46.º ou 47.º do RGPD.

Sem prejuízo do disposto, os Suboperadores identificados no Apêndice B do presente Acordo poderão realizar determinadas operações de tratamento fora do Espaço Económico Europeu (EEE), desde que cumpram uma das condições estabelecidas no Capítulo V do RGPD.

Cláusula 13.ª – Responsabilidade

O Subcontratante será considerado responsável pelo tratamento no caso de utilizar os dados objeto do presente Acordo para finalidades diferentes das contratualmente previstas, de os comunicar a terceiros ou de os utilizar em desconformidade com as estipulações deste Acordo, respondendo por quaisquer infrações que tenha cometido pessoalmente.

O Responsável pelo Tratamento compromete-se a informar o Subcontratante, com carácter imediato, sobre a instauração de quaisquer procedimentos sancionatórios por parte da Comissão Nacional de Proteção de Dados (CNPD) ou de qualquer outra autoridade competente, decorrentes de tais incumprimentos ou de um cumprimento defeituoso, a fim de permitir ao Subcontratante assumir, por sua conta, a defesa legal. Neste âmbito, ambas as Partes deverão atuar de forma coordenada, salvaguardando, em todos os momentos, a imagem pública e a reputação da Parte envolvida.

Cada Parte obriga-se a manter a outra indemne contra quaisquer reclamações, indemnizações, ações ou despesas decorrentes de decisões judiciais definitivas ou laudos arbitrais, ou de acordos extrajudiciais com terceiros reclamantes, desde que resultem de incumprimentos ou de cumprimento defeituoso da legislação aplicável por parte da Parte responsável.

ACORDO DE SUBCONTRATAÇÃO DO TRATAMENTO DE DADOS PESSOAIS

O presente ACORDO DE SUBCONTRATAÇÃO DO TRATAMENTO DE DADOS PESSOAIS apenas será aplicável caso o CLIENTE e/ou a SESAME HR estejam sujeitos à Lei Geral de Proteção de Dados Pessoais na Posse de Entidades Obrigadas do México.

Identificação da informação afetada

Para efeitos da execução das prestações decorrentes do cumprimento do objeto do presente Acordo de Subcontratação do Tratamento, o Responsável pelo Tratamento coloca à disposição do Subcontratante determinados dados de carácter pessoal.

Duração

O presente Acordo de Subcontratação do Tratamento entra em vigor na data de aceitação das condições do Contrato. O presente Acordo de Subcontratação do Tratamento é acessório ao contrato principal de prestação de serviços, pelo que a sua duração está vinculada à duração do mesmo.

Obrigações do Responsável pelo Tratamento

Compete ao Responsável pelo Tratamento, para além do cumprimento de todas as obrigações que lhe sejam atribuídas ao longo do presente Acordo de Subcontratação do Tratamento, a realização das seguintes tarefas:

- Cumprir com todas as medidas de segurança técnicas, físicas e administrativas necessárias para garantir a segurança do tratamento, das instalações, equipamentos, sistemas, programas e das pessoas que intervenham na atividade de tratamento dos dados pessoais referidos, conforme estipulado na legislação vigente e aplicável em cada momento.
- Entregar ao Subcontratante os dados a que se refere a cláusula 2 do presente documento, bem como as instruções necessárias para proceder ao tratamento dos dados nos termos estabelecidos pelo Responsável.
- Responder aos direitos dos titulares dos dados afetados pelo tratamento, nomeadamente os direitos de acesso, retificação, cancelamento e oposição, em colaboração com o Subcontratante.
- Assegurar, previamente e durante o tratamento, o cumprimento da legislação aplicável em matéria de proteção de dados pessoais por parte do Subcontratante.
- Supervisionar o tratamento, incluindo a realização de inspeções e auditorias.
- Comunicar ao Subcontratante qualquer alteração que ocorra relativamente aos dados pessoais fornecidos, para que seja procedida a sua atualização.

Dever de informação e fundamento legítimo

O Responsável garante que cumpriu o dever de fornecer toda a informação aos titulares dos dados no momento da recolha dos dados objeto de tratamento, em conformidade com o disposto no Capítulo II da Lei Federal de Proteção de Dados Pessoais na Posse de Particulares.

O Responsável pelo Tratamento garante que dispõe de um fundamento legítimo adequado para o tratamento dos dados pessoais, em conformidade com os princípios de eficácia, necessidade e proporcionalidade, considerando a existência de outras medidas de proteção que possam revelar-se menos intrusivas, evitando efeitos discriminatórios e estabelecendo as garantias adequadas.

O Subcontratante não será, em caso algum, responsável pelo incumprimento ou cumprimento defeituoso do dever de informação ou da aplicação de um fundamento de legitimidade adequado.

Obrigações do Subcontratante

O Subcontratante declara e garante ao Responsável pelo Tratamento o seguinte:

- Tratar unicamente os dados pessoais de acordo com as instruções do Responsável;
- Abster-se de tratar os dados pessoais para finalidades distintas das instruídas pelo Responsável;
- Implementar as medidas de segurança em conformidade com a Lei Federal de Proteção de Dados Pessoais na Posse de Particulares, com o Regulamento da Lei Federal de Proteção de Dados Pessoais na Posse de Particulares, bem como com as demais disposições aplicáveis;
- Manter a confidencialidade relativamente aos dados pessoais tratados;
- Eliminar os dados pessoais objeto de tratamento uma vez cumprida a relação jurídica com o Responsável ou por instruções deste, salvo se existir disposição legal que imponha a conservação dos dados pessoais;
- Abster-se de transferir os dados pessoais, salvo se tal transferência for determinada pelo Responsável, resultar de uma subcontratação ou for exigida por autoridade competente, sem prejuízo da lista de Suboperadores constante no Apêndice B.

Tratando-se de um serviço de computação em nuvem, o Subcontratante declara e garante ao Responsável pelo Tratamento o seguinte:

- Dispor e aplicar políticas de proteção de dados pessoais compatíveis com os princípios e deveres previstos na Lei Federal de Proteção de Dados Pessoais na Posse de Particulares e no respetivo Regulamento;
- Disponibilizar informação transparente sobre os subcontratantes envolvidos no tratamento dos dados;

- Em caso algum o Subcontratante assumirá a titularidade ou propriedade das informações da titularidade do Responsável que tenham sido incorporadas na plataforma SESAME HR;
- Dispor, pelo menos, dos seguintes mecanismos:
    - Comunicar ao Responsável pelo Tratamento quaisquer alterações à política de privacidade do Subcontratante ou ao presente Acordo de Subcontratação do Tratamento;
    - Permitir ao Responsável limitar o tipo de tratamento dos dados pessoais;
    - Estabelecer e manter medidas de segurança adequadas à proteção dos dados pessoais;
    - Garantir a eliminação dos dados pessoais uma vez terminado o serviço prestado ao Responsável, mediante eliminação manual efetuada pelo próprio Responsável ou mediante pedido do mesmo;
    - Impedir o acesso aos dados pessoais por pessoas que não disponham de privilégios de acesso, ou, no caso de pedido fundamentado e devidamente justificado por parte de autoridade competente, informar o Responsável desse facto.

Destino dos Dados

No termo da prestação dos Serviços, o Subcontratante devolverá os dados pessoais aos quais tenha tido acesso, bem como qualquer cópia existente, conforme indicado pelo Responsável pelo Tratamento e nos termos do disposto na Cláusula 13.ª do Acordo.

O Subcontratante poderá conservar uma cópia dos dados devidamente bloqueada, enquanto possam emergir responsabilidades decorrentes da execução da prestação dos Serviços.

Notificação de violações da segurança dos dados

O Subcontratante notificará o Responsável, sem demora injustificada, qualquer incidente, suspeito ou confirmado, relativo à proteção de dados, no âmbito da sua responsabilidade. Tal violação de segurança deverá consistir na perda ou destruição não autorizada; roubo, extravio ou cópia não autorizada; utilização, acesso ou tratamento não autorizado; ou dano, alteração ou modificação não autorizada.

Exercício de direitos por parte dos titulares dos dados

O Subcontratante facilitará a informação e/ou documentação que o Responsável lhe solicite para responder aos pedidos de exercício de direitos que possa receber da parte dos titulares dos dados pessoais tratados. O Subcontratante deverá fornecer essa informação em prazos razoáveis e, em qualquer caso, com antecedência suficiente para que o Responsável possa cumprir os prazos legalmente aplicáveis para resposta ao exercício desses direitos.

Quando os titulares dos dados exerçam os direitos de acesso, retificação, eliminação e oposição junto do Subcontratante, este deverá comunicá-lo por correio eletrónico para o endereço legal@sesametime.com. A comunicação deverá ser feita de forma imediata, de modo a permitir o seu tratamento dentro dos prazos legais estabelecidos, e em nenhum caso para além de dois dias úteis após a receção do pedido, sendo enviada ao Responsável acompanhada de toda a informação que possa ser relevante para a sua resolução.

Segurança

No que respeita às medidas técnicas, administrativas e físicas de segurança, o Subcontratante deverá implementar mecanismos para:

- Garantir a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e serviços de tratamento;
- Restabelecer a disponibilidade e o acesso aos dados pessoais de forma rápida, em caso de incidente físico ou técnico;
- Verificar, avaliar e analisar, de forma regular, a eficácia das medidas técnicas, físicas e administrativas implementadas para garantir a segurança do tratamento;
- Pseudonimizar e cifrar os dados pessoais, quando aplicável.

Em particular, as Partes acordaram um conjunto de medidas que o Subcontratante deve implementar, conforme indicado no Apêndice A ao presente Acordo de Subcontratação do Tratamento.

Caso o Responsável, posteriormente à formalização do Contrato, exija ao Subcontratante a adoção ou manutenção de medidas de segurança diferentes das previstas no presente Apêndice A, ou que sejam obrigatórias por força de qualquer norma futura, e tal exigência afete de forma significativa os custos da prestação dos Serviços, o Subcontratante e o Responsável pelo Tratamento acordarão as medidas contratuais adequadas para enfrentar o impacto que tais modificações possam ter no preço dos Serviços.

Subcontratação

O Responsável pelo Tratamento concede uma autorização geral para que o Subcontratante possa subcontratar parte dos Serviços a terceiros ou entidades subcontratadas (doravante, o “Suboperador”). O Subcontratante informará o Responsável pelo Tratamento sobre os tratamentos que pretende subcontratar, identificando de forma clara e inequívoca a entidade subcontratada e os seus dados de contacto.

A subcontratação poderá ser realizada caso o Responsável não manifeste oposição no prazo de 15 dias.

O Subcontratante aplicará a diligência devida para selecionar apenas Suboperadores que ofereçam garantias suficientes para a aplicação de medidas técnicas, físicas e administrativas adequadas, de forma a que os tratamentos subcontratados estejam em conformidade com os requisitos da Lei Federal de Proteção de Dados Pessoais na Posse de Particulares, garantindo-se assim a proteção dos direitos dos titulares dos dados.

O Suboperador, que assumirá igualmente a condição de subcontratante no tratamento, estará vinculado ao cumprimento das obrigações impostas ao Subcontratante e das instruções emitidas pelo Responsável, nos termos do presente Acordo de Subcontratação do Tratamento. Cabe ao Subcontratante regular esta nova relação contratual mediante acordo escrito com o Suboperador, assegurando que este último fique sujeito às mesmas condições (instruções, obrigações, medidas de segurança...) e com os mesmos requisitos formais do Subcontratante inicial, no que respeita ao adequado tratamento dos dados pessoais e à garantia dos direitos dos titulares dos dados.

Em caso de incumprimento por parte do Suboperador, o Subcontratante continuará a ser plenamente responsável perante o Responsável pelo Tratamento pelo cumprimento das obrigações previstas no presente Acordo de Subcontratação do Tratamento.

A lista de Suboperadores autorizados pelo Responsável pelo Tratamento encontra-se anexa ao presente Acordo como Apêndice B.

Transferências internacionais de dados

O Subcontratante poderá realizar transferências internacionais de dados pessoais para Soboperadores autorizados que se encontrem fora do território nacional do México, desde que estes ofereçam garantias suficientes no que respeita à aplicação de medidas físicas, técnicas e administrativas adequadas.

Responsabilidade

O Subcontratante será considerado responsável pelo tratamento caso utilize os dados objeto do presente Acordo para finalidades distintas das previstas, os comunique ou os utilize em violação das estipulações constantes no presente Acordo, sendo responsável pelas infrações que pessoalmente tiver cometido.

Cada Parte manterá a outra isenta de qualquer reclamação, indemnização, ação ou despesa decorrente de exigências que a Parte esteja obrigada a satisfazer por decisão judicial transitada em julgado ou por sentença arbitral proferida por tribunal competente, ou ainda em virtude de acordo alcançado entre uma Parte e terceiros reclamantes, sempre que tais exigências resultem do incumprimento ou do cumprimento defeituoso da legislação aplicável.

APÊNDICE A – Medidas Técnicas e Organizativas de Segurança

A infraestrutura da SESAME HR assenta predominantemente em ambientes cloud, sendo utilizados vários fornecedores com o objetivo de garantir elevada tolerância a falhas e melhoria contínua da resiliência dos sistemas.

A aplicação possui uma arquitetura distribuída, permitindo a separação entre o frontend, a API e outros serviços essenciais ao funcionamento da solução. Esta arquitetura facilita a escalabilidade e o dimensionamento específico das partes da infraestrutura sujeitas a maior carga.

O ambiente de desenvolvimento é virtualizado, o que possibilita ao departamento técnico da SESAME HR realizar alterações de forma paralela, sob controlo de versões com recurso ao sistema GIT, garantindo a integridade do código e a rastreabilidade das alterações. O processo de integração contínua é assegurado através da plataforma GitLab.

Metodologias de desenvolvimento utilizadas:

- SOLID
- DDD (Domain Driven Design)
- Testes unitários
- Arquitetura Hexagonal
- Autenticação múltipla
- Integração contínua (CI/CD) com GitLab

Linguagens de programação

- **Backend**
  - Symfony 4
  - PHP 7.x
  - MySQL / MariaDB
  - Redis / SQS / Beanstalk
  - AWS S3
- **Frontend**
  - VueJS
  - Tailwind
  - Biblioteca de componentes proprietária
- **Aplicações móveis**

    - VueJS
    - Capacitor
    - Typescript
- **Sockets**
    - NodeJS
    - Express
    - Socket.IO

Infraestrutura

Para o processamento da informação, são utilizadas as seguintes tecnologias:

- Debian 10
- Docker
- Kubernetes (K8s)
- AWS
- Google Cloud
- OVH Cloud
- Proxmox
- HAProxy
- Cloudflare

O departamento de sistemas é responsável por garantir que todos os servidores possuem a configuração necessária ao funcionamento estável da aplicação.

Servidor de Base de Dados

- Relacional (SQL): Para as bases de dados relacionais será utilizado o sistema MariaDB;
- A base de dados deverá possuir codificação UTF-8;
- Será criado um utilizador com os seguintes privilégios:
    - Esquema (criação de objetos): Sim (criação, modificação e eliminação de tabelas);
    - Escrita (SUDI — Select, Update, Delete e Insert): Sim;
    - Leitura (SELECT): Sim.

Cópias de Segurança

São realizadas cópias de segurança completas semanais e cópias incrementais diárias.

Relativamente ao servidor de base de dados, é mantida uma cópia das cópias efetuadas, com periodicidade mensal, semanal e diária, armazenada num servidor secundário (escravo).

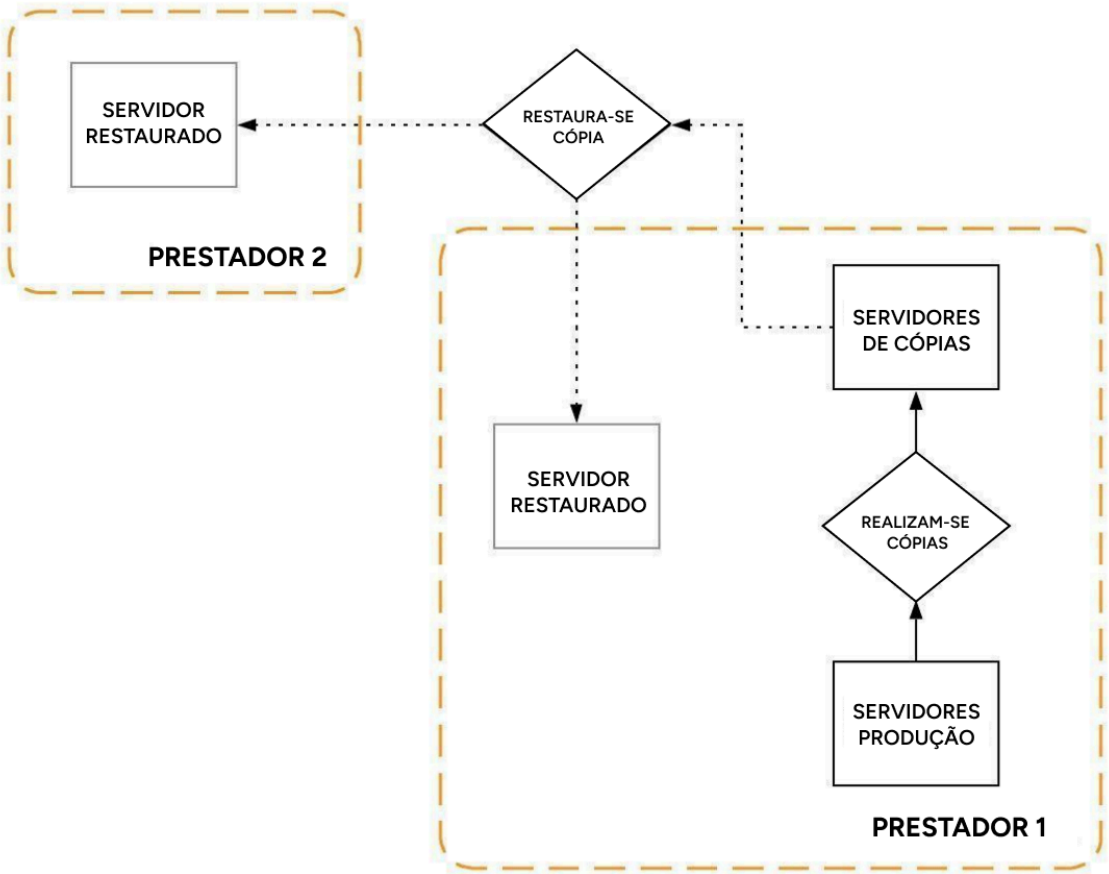
Adicionalmente, são efetuadas cópias horárias da base de dados do servidor principal.

É igualmente guardada uma cópia integral de todo o conteúdo do servidor web, bem como das configurações dos serviços críticos.

Utiliza-se um servidor de cópias de segurança localizado em França, com redundância em território polaco, de forma a garantir a disponibilidade e recuperação dos dados em caso de desastre.

O responsável designado do departamento de sistemas de informação ou de informática — ou quem legalmente o substitua — deverá elaborar e manter um procedimento documentado de verificação e testes de restauração das cópias de segurança, a realizar com uma periodicidade mensal.

Em caso de recuperação de uma cópia de segurança, será seguido o seguinte procedimento:



Medidas de Segurança da Infraestrutura

Dataenter

Dispomos de servidores contratados à OVH, líder europeia e terceiro maior fornecedor mundial de alojamento web, com mais de 150.000 servidores físicos.

O sucesso da OVH assenta no controlo total sobre toda a cadeia de alojamento, incluindo a produção dos seus próprios servidores. A OVH é reconhecida pelo elevado rigor na seleção dos componentes das suas máquinas, exigindo os mais altos padrões de qualidade.

Cada servidor é sistematicamente submetido a um conjunto de testes técnicos, com o objetivo de verificar a sua conformidade e desempenho adequado em quaisquer circunstâncias.

Assim que a máquina é concluída em fábrica, é instalada e conectada nos datacenters da OVH. De seguida, um sistema automatizado verifica se o hardware corresponde ao solicitado pelo cliente e se as respetivas especificações técnicas estão corretamente aplicadas.
Os pontos de controlo incluem:

- Processadores: conformidade, testes de carga, temperatura;
- Memória RAM: capacidade, testes de integridade (memtest);
- BIOS: versão da BIOS, suporte para virtualização;
- Discos: velocidade, testes SMART, versão do firmware, entre outros.

Adicionalmente, recorremos a serviços contratados na AWS (Amazon Web Services).
A AWS foi pioneira em soluções de computação em nuvem desde 2006, tendo desenvolvido uma infraestrutura cloud que permite inovar com rapidez e garantir elevados níveis de segurança.

Os centros de dados da AWS estão concebidos para proporcionar proteção contra riscos naturais e provocados por ação humana.
São aplicados controlos rigorosos, desenvolvidos sistemas automatizados e realizadas auditorias externas independentes com vista a assegurar a conformidade e a segurança da infraestrutura.

Os centros de dados estão projetados para antecipar e tolerar falhas, mantendo simultaneamente os níveis de serviço contratados. Em caso de incidente, os processos automatizados da AWS redirecionam o tráfego proveniente da zona afetada.
As aplicações críticas são implementadas segundo o padrão N+1, garantindo que, em caso de falha num centro de dados, exista capacidade operacional suficiente para redistribuir a carga de tráfego entre os restantes centros.

A AWS realiza monitorização contínua e procedimentos de manutenção preventiva dos seus equipamentos elétricos e mecânicos, com o objetivo de assegurar o funcionamento ininterrupto dos sistemas instalados. Estas operações de manutenção são executadas por

técnicos devidamente qualificados, segundo um plano de manutenção documentado, previamente definido e aprovado.

Proteção contra Ataques
Os nossos servidores estão protegidos por uma infraestrutura anti-DDoS disponibilizada pela OVH, operando 24 horas por dia, com capacidade para mitigar qualquer tipo de ataque de negação de serviço distribuído (DDoS), independentemente da sua duração ou dimensão.

O objetivo de um ataque DDoS é comprometer a disponibilidade de um servidor, serviço ou infraestrutura, através do envio massivo de pedidos simultâneos provenientes de múltiplos pontos da rede.

A intensidade deste “fogo cruzado” pode desestabilizar o serviço ou mesmo torná-lo completamente inoperacional.

A infraestrutura anti-DDoS da OVH permite:

- Analisar todos os pacotes de dados em tempo real e a alta velocidade;
- Redirecionar (aspirar) o tráfego de entrada do servidor para ambientes controlados;
- Mitigar os efeitos do ataque, identificando e bloqueando pacotes IP ilegítimos, permitindo simultaneamente a passagem do tráfego legítimo.

Segurança
A SESAME HR tem plena consciência da importância da segurança da informação, do tratamento adequado dos dados pessoais e da prevenção de fugas de informação.
Por essa razão, trabalha diariamente na melhoria contínua da sua política de segurança, com objetivos claros e medidas estruturadas nesse domínio.
Seguidamente, detalham-se de forma mais aprofundada os diferentes aspetos abordados no âmbito da segurança da aplicação e da infraestrutura tecnológica.

Fornecedores Cloud: a SESAME HR recorre a diferentes fornecedores de serviços em cloud com o objetivo de garantir a máxima disponibilidade e escalabilidade da aplicação.

Todos os fornecedores utilizados cumprem, pelo menos, os seguintes referenciais e certificações internacionais de segurança:

- ISO/IEC 27001, 27017 e 27018
- PCI DSS Nível 1
- Conformidade com o RGPD — Regulamento (UE) 2016/679 relativo à Proteção de Dados Pessoais
- SSAE 18 Tipo 2 — Relatórios SOC 1, SOC 2 e SOC 3

O acesso a estes fornecedores é restrito a colaboradores com um nível de acreditação elevado, geralmente responsáveis de área ou membros do departamento de sistemas, devidamente autorizados.

Servidores: o acesso aos servidores está limitado a colaboradores com elevado nível de acreditação interna.
O acesso é realizado através de um par de chaves RSA encriptadas de 2048 bits, combinado com uma palavra-passe associada a um utilizador nominal. Este método permite o registo detalhado das entradas e atividades realizadas por cada utilizador, a rastreabilidade de alterações efetuadas nas máquinas e a realização de auditorias técnicas posteriores, sempre que necessário.

Ferramentas de Terceiros: a SESAME HR utiliza ferramentas de segurança de terceiros como é o caso da Tenable.io, que se encarrega de inventariar todas as nossas máquinas, bem como os domínios que utilizamos, e de lançar periodicamente auditorias de vulnerabilidades e intrusão.

Assim, todas as semanas os nossos especialistas dispõem de novos relatórios que indicam possíveis brechas de segurança, as quais, segundo o algoritmo de IA da Tenable, serão corrigidas por ordem de prioridade recomendada.

Acesso à aplicação: o acesso à plataforma será sempre realizado através do nosso fornecedor de CDN e DNS, CloudFlare, o qual conta com um WAF integrado de última geração capaz de detetar e mitigar ataques que sejam dirigidos diretamente à aplicação.

Política de patching
Todos os serviços, e a infraestrutura que os suporta, acessíveis a partir da Internet, quer sejam de uso interno da empresa ou destinados aos nossos clientes, seguem uma política de atualizações de segurança ágil. Estes serviços são corrigidos assim que seja detetada uma falha ou vulnerabilidade importante.

No caso de atualizações não críticas, é programada uma aplicação de patches mensal ou trimestral, consoante as necessidades e a aplicação em causa.

Os serviços de caráter interno (impressoras, equipamentos de rede local dos utilizadores, centrais telefónicas, etc.) seguem uma política de atualizações periódicas programadas (de seis em seis meses, anualmente, etc.), em função das necessidades e executada pelo departamento de IT da empresa.

Dispomos igualmente de um sistema de alerta em caso de vírus, ClamAV.

APÊNDICE B – Lista de Suboperadores

OVH

Aplicação: Aplica-se ao uso essencial da plataforma. Este fornecedor aplica-se a todo o mundo, exceto aos países do continente americano (com exceção dos Estados Unidos e Canadá).

Nome do Suboperador: OVH SAS

Localização atual do tratamento: França e Alemanha

Ligação para a política de segurança do Suboperador:
https://www.ovhcloud.com/pt/personal-data-protection/security/

Amazon Web Services

Aplicação: Aplica-se ao uso essencial da plataforma. Este fornecedor aplica-se a todo o mundo, exceto aos países do continente americano (com exceção dos Estados Unidos e Canadá).

Nome do Suboperador: Amazon Web Services

Localização atual do tratamento: França e Alemanha

Ligação para a política de segurança do Suboperador:
https://aws.amazon.com/compliance/?nc1=h_ls

Mailchimp

Aplicação: Aplica-se ao uso essencial da plataforma. Este fornecedor aplica-se a todo o mundo.

Nome do Suboperador: The Rocket Science Group (Mailchimp)

Localização atual do tratamento: Estados Unidos

Ligação para a política de segurança do Suboperador:
https://mailchimp.com/gdpr/

Transferência internacional para efeitos de RGPD: O Suboperador está aderente ao EU-U.S. Data Privacy Framework.

Signaturit

Aplicação: Aplica-se à utilização da funcionalidade de assinatura eletrónica (apenas quando essa funcionalidade estiver ativada e for utilizada). Este fornecedor aplica-se a todo o mundo.

Nome do Suboperador: Signaturit Solutions S.L

Localização atual do tratamento: Espanha

Ligação para a política de segurança do Suboperador:
https://www.signaturit.com/privacy-policy/

OpenAI

Aplicação: Aplica-se em caso de contratação e utilização da SESAME IA.

Nome do Suboperador: OpenAI

Localização atual do tratamento: Estados Unidos da América

Transferência internacional para efeitos de RGPD: Conforme a política de privacidade do Suboperador.

Ligação para a política de segurança do Suboperador:
https://openai.com/pt-PT/policies/privacy-policy/

AUREN

Aplicação: Aplica-se em caso de contratação e utilização do serviço “Gestor de salários”.

Nome do Suboperador: AUREN LEGAL SP, S.L.P

Localização atual do tratamento: Espanha

Ligação para a política de segurança do Suboperador:
https://auren.com/es/en/privacy-policy-and-information-security/

IPXON

Aplicação: Aplica-se ao uso essencial da plataforma. Este fornecedor aplica-se aos países do continente americano (exceto Estados Unidos e Canadá).

Nome do Suboperador: CONEXUM INC (IPXON Networks)

Localização atual do tratamento: Brasil (apenas para clientes registados em países do continente americano, com exceção dos Estados Unidos e Canadá)

Ligação para a política de segurança do Suboperador: https://www.ipxon.com/en-gl/privacy

SWAN

Aplicação: Aplica-se em caso de contratação e utilização das funcionalidades de Controlo de Despesas e Adiantamento Salarial.

Nome do Suboperador: SWAN SAS

Localização atual do tratamento: França

Ligação para a política de segurança do Suboperador: https://cdn.prod.website-files.com/609a39f33751ff4530c610e2/65cc87d02a1db07ef2365bc1_2024-PP-PT.pdf