SUPPLHI

Adaptive SRM

# SupplHi SRM SaaS - Termos e Condições Padrão e DPA para Vendors

[Portuguese]

PÚBLICO

www.supplhi.com

# [POR] Termos e Condições padrão para a utilização do SaaS SRM por parte dos “Vendors”

Os seguintes Termos e Condições aplicam-se a todos os usuários registrados com um perfil "Vendor" (ou seja, as organizações que podem fornecer bens e/ou serviços aos usuários das organizações “Buyer”).

O perfil "Buyer" (ou seja, as organizações às quais a SupplHi fornece acesso à plataforma para a gestão da própria base de fornecedores) possui Termos e Condições dedicados.

## Nossa missão

A SupplHi é a plataforma Software-as-a-Service (SaaS), em nuvem, de Supplier Relationship Management (SRM) para o fornecimento de bens e serviços B2B. Nossa missão é permitir que cada organização cresça por meio de sua própria cadeia de fornecimento. A SupplHi, de fato, permite que as organizações Buyer realizem seus próprios processos de gestão da base de fornecedores de forma eficiente e compliant, respeitando as normas de referência e à luz das melhores práticas internacionais de mercado - trazendo ordem por meio de processos de SRM sob controle e de fácil acesso às informações, sem perder nenhum momento do seu tempo.

A SupplHi disponibiliza ao mundo B2B a sua infraestrutura digital com o objetivo de aumentar a eficiência, reduzir os custos e criar maiores oportunidades para organizações Buyer e Vendor, em nível global.

Todos os dados da plataforma SupplHi (formulários, anexos, informações, e-mails) são armazenados em estruturas de alta confiabilidade e em hospedagem localizada na União Europeia (atualmente na Irlanda) na Amazon Web Services (AWS).

Também é possível utilizar o nosso site de marketing navegando como Visitante. Nesse caso, não é necessário fazer login, mas não é possível acessar todo o conteúdo e todas as funcionalidades da plataforma. Ao utilizar os serviços que oferecemos, você passa a fazer parte da nossa rede e se compromete a usar o nosso site de forma responsável e a respeitar as suas regras de utilização.

## Acordo

Ao se registrar em nosso site, você celebra um contrato com a SupplHi S.r.l. Società Unipersonale, Via A. Calabiana, 6 - 20139 Milão, Itália, registrada na C.C.I.A.A. de Milão sob o número 09721660968, R.E.A. MI 2110015, com Código Fiscal e Número de Identificação de IVA 09721660968, info@supplhi.com (doravante simplesmente "SupplHi") e aceita todas as condições a seguir em seu nome e por conta própria ou em nome da empresa que você representa. Este acordo também rege o uso dos aplicativos móveis.

Se a sua empresa autorizou você a agir como representante, você está celebrando este acordo em nome de sua empresa. Ambos estão sujeitos às regras estabelecidas no presente acordo. Se você não estiver autorizado, ficará pessoalmente vinculado a este acordo. Ao utilizar o nosso site, você confirma ter pelo menos 18 anos e ter o direito de celebrar o presente acordo.

## Proteção de dados pessoais

Todo tratamento de dados pessoais é realizado pela SupplHi para prestar o serviço solicitado na qualidade de operador, conforme definido no art. 4, par. 1, n. 8 do Regulamento Geral sobre a

Proteção de Dados Pessoais 2016/679, em conformidade com as indicações contidas no Data Protection Agreement.

## Serviço

O papel da SupplHi é fornecer às organizações Buyer - por meio da plataforma SaaS - o acesso a informações estruturadas e constantemente atualizadas sobre os Vendors, a fim de que possam gerenciar de forma autônoma os seus próprios processos de Supplier Relationship Management (SRM). Por exemplo, a SupplHi não decide se um determinado Vendor está qualificado ou não, nem dentro da rede de organizações Buyer que usam a plataforma, nem em relação a uma organização Buyer específica, e a decisão de qualificação de um Vendor permanece sempre a cargo de cada organização Buyer individualmente.

No âmbito da prestação dos serviços às organizações Buyer e com base nos módulos e nas funcionalidades selecionadas e configuradas para cada organização Buyer específica, a SupplHi oferece os seguintes Serviços gratuitos aos Vendors:

- Gerenciar, para cada Vendor (seja uma empresa ou uma pessoa física) - por meio de códigos identificativos definidos pela SupplHi em base nacional (VAT, TIN, número de Registro), solicitados na fase de criação de um novo Vendor na plataforma - um código "SupplHi ID" único;
- Permitir a associação de um usuário Vendor a um determinado "SupplHi ID". Tal associação pode ser realizada pelo Usuário Vendor que se registra, pelo Super Usuário ou por uma organização Buyer. A associação realizada pelo Usuário a um Vendor onde já exista um Super Usuário deve ser confirmada pelo próprio Super Usuário. A associação implica a possibilidade de o Usuário visualizar e gerenciar as informações referentes ao seu Vendor de referência. A associação ocorre sob a exclusiva responsabilidade de quem a realiza e, quando necessário, de quem fornece a confirmação. A SupplHi não realiza nenhum controle a respeito, nem pode ser responsabilizada em caso de associação incorreta realizada por um Usuário, Super Usuário ou por uma organização Buyer. Um Usuário Vendor, identificado por um endereço de e-mail específico, pode ser associado a apenas um único SupplHi ID e, portanto, a um único Vendor.
- Ter um ou mais Super Usuário(s) do Vendor capaz(es) de gerenciar os direitos de visibilidade e de gestão das informações para os Usuários vinculados ao mesmo Vendor e de ceder ou estender, na plataforma e a qualquer momento, o próprio papel de Super Usuário a um colega específico;
- Hospedar na plataforma as informações fornecidas pelo Vendor nas diversas fases de registro e preenchimento, por meio de Questionários dedicados, das informações solicitadas pelas organizações Buyer, sejam elas "industry-shared" ou "customer-specific". Esclarece-se que as informações inseridas pelo Vendor na plataforma em resposta aos Questionários podem ser de dois tipos, claramente evidenciados na plataforma dentro de cada Questionário:
    - "customer-specific": as informações ficarão visíveis somente para a organização Buyer específica claramente identificável pelo Vendor. Somente essa organização Buyer específica poderá visualizá-las, copiá-las e utilizá-las.
    - "industry-shared": as informações ficarão potencialmente visíveis para todas as organizações Buyer que tenham acesso à plataforma SupplHi. Elas poderão visualizá-las, copiá-las e utilizá-las. A presença de informações "industry-shared" permite reduzir o seu esforço de preenchimento das informações típicas incluídas nos questionários de pré-qualificação e qualificação (por exemplo, presença de certificações de qualidade, número de funcionários, presença de um código de ética, etc.) para diversas organizações Buyer

e aumentar a visibilidade junto às organizações Buyer que utilizam a plataforma.

- Apoiar o Vendor nas fases de preenchimento e atualização das informações solicitadas pelas organizações Buyer dentro dos Questionários, gerando a lista de informações faltantes e realizando - de forma automática ou manual - a atividade de "Quality Assurance" voltada a garantir a coerência das informações fornecidas pelo Vendor em relação ao solicitado;
- Assim que o Vendor atingir 100% de conclusão das informações e após a atividade de "Quality Assurance", com base no tipo das informações ("industry-shared" ou "customer-specific"), tornar visíveis às organizações Buyer às quais a SupplHi concede acesso na plataforma as informações fornecidas pelo Vendor;
- Permitir que o Vendor amplie os próprios canais comerciais para a venda de fornecimentos B2B por meio da visibilidade adquirida junto às organizações Buyer que utilizam a plataforma. Ressaltamos que, ao utilizar o nosso site, você permite que todos os usuários das organizações Buyer visualizem e extraiam de forma simples as informações "industry-shared" que você carrega em nossa plataforma, utilizando as ferramentas que disponibilizamos, e que tais informações podem, portanto, circular na rede mesmo fora do nosso controle;
- Notificar o Vendor sobre informações em fase de vencimento e permitir a atualização na plataforma;
- Permitir que o Vendor se candidate aos processos de Qualificação perante uma organização Buyer específica;
- Permitir a visualização de um ou mais resultados de classificação e pontuação (scoring) do Vendor, com base na configuração realizada para cada organização Buyer;
- Por meio da funcionalidade "Vendor Actions", permitir descrever as ações de melhoria empresarial que o Vendor está implementando;
- Permitir que o Vendor receba RFx (solicitações de informações, propostas, cotações) por parte das organizações Buyer por meio dos contatos fornecidos pelo Vendor;
- Por meio do módulo "Management of Contractual Documents" e da funcionalidade "Document Exchange", permitir a troca de documentos específicos;
- Por meio do módulo denominado "SupplAuth", permitir tecnicamente o acesso a outros sistemas aplicativos configurados pela organização Buyer (por exemplo, sistemas de gestão de pedidos ou de licitação). O sistema de autorização é controlado exclusivamente pela organização Buyer, sem que a SupplHi possa de forma alguma decidir os níveis de autorização para outros aplicativos;
- Apoiar o Vendor por meio da publicação de manuais e Perguntas Frequentes (FAQ) dedicadas aos usuários Vendor e das atividades de Help Desk por meio do sistema de tickets presente na plataforma.

Eventuais Serviços adicionais e relações entre o Vendor e a SupplHi são regidos pelos Termos e Condições do Serviço específico.

A SupplHi compromete-se a implementar medidas de segurança da informação adequadas aos *padrões* do setor, para a proteção de todos os dados e para a prestação de um serviço da melhor qualidade possível.

## Custo do serviço

A SupplHi fornece gratuitamente aos Vendors os Serviços descritos neste contrato.

## Conta e obrigações do Usuário

Ao utilizar o nosso site, você declara não estar sujeito a restrições por parte da SupplHi na utilização dos Serviços e se compromete a:

1. ativar apenas uma conta pessoal e garantir que a sua empresa tenha apenas uma conta SupplHi como Vendor;
2. fornecer o seu nome real e o nome real da sua empresa;
3. respeitar todas as disposições legais aplicáveis e as políticas internas, como, por exemplo, a lei de proteção de dados pessoais, de propriedade intelectual, sobre spam, etc.;
4. utilizar os Serviços oferecidos pela SupplHi apenas para fins profissionais e não pessoais;
5. não agir de forma incorreta, publicando conteúdos inadequados ou imprecisos, não contatar outros usuários para qualquer forma de comunicação indesejada, nem adotar condutas não conformes com a lei, ou que sejam difamatórias, ofensivas, obscenas, discriminatórias ou de qualquer forma questionáveis;
6. não utilizar ou tentar utilizar a conta de terceiros;
7. não prejudicar outra pessoa ou qualquer outra empresa que utilize o nosso site.

Você se compromete a escolher uma senha segura, a mantê-la em sigilo e a não compartilhar a conta com mais ninguém. Todos os usuários que se registram na plataforma SupplHi estão sujeitos a uma *política de senhas*.

Para criar o perfil da sua empresa, você responderá às perguntas na plataforma e, quando necessário, atualizará as suas respostas. Para esse fim, você garante que as informações fornecidas à SupplHi:

- sejam precisas;
- sejam atualizadas prontamente;
- não contenham nada que viole o direito de terceiros, que a sua empresa não o autorize a compartilhar ou que seja de outra forma ilícito. A título exemplificativo, você se compromete a não violar os direitos de propriedade intelectual ou industrial de terceiros, incluindo patentes, marcas, segredos comerciais, direitos autorais ou outros direitos, a não inserir conteúdos que não sejam destinados ou que não sejam exatos em relação ao campo a ser preenchido (por exemplo, a inserção de um número de telefone no campo "e-mail" ou em qualquer outro campo);
- reflitam os bens e serviços efetivamente oferecidos como Vendor.

## Informações fornecidas

Quando você nos fornece informações relativas à sua organização, outras pessoas podem visualizar, copiar e utilizar tais informações. Em particular, as informações e os conteúdos que você nos fornece serão visualizados pelos usuários das organizações Buyer.

Informamos que, a fim de fornecer aos Vendors e às organizações Buyer o nosso serviço, e por motivos de *compliance*, todas as interações ou alterações no seu perfil como Vendor na plataforma são registradas e armazenadas pela SupplHi. Por esses motivos, você e a SupplHi poderão acessar tais informações. Apenas dados empresariais e nenhum dado pessoal - com exceção do e-mail do usuário - serão armazenados para esse fim.

A fim de fornecer o nosso serviço a Vendors e organizações Buyer, todas as interações ou alterações no perfil do seu Vendor na plataforma são registradas e disponibilizadas às organizações Buyer. Os dados pessoais eventualmente tratados pela SupplHi para esse fim serão gerenciados em conformidade com o princípio de minimização previsto no art. 25 do GDPR e com todas as medidas de segurança previstas no Data Protection Agreement.

A fim de oferecer aos usuários um serviço mais completo, as informações que você nos fornece poderão ser exibidas juntamente com outras informações que as organizações Buyer que utilizam a SupplHi podem legitimamente utilizar em relação à sua empresa e aos serviços que ela presta (por exemplo: pontuações de solidez financeira fornecidas por agências de classificação de risco financeiro).

As informações que você carrega em nosso site segundo um dos dois modos – "industry-shared" e "customer-specific" acima definidos poderão ser visualizadas e extraídas pelas organizações Buyer de acordo com as seguintes regras.

- As informações "customer-specific" não serão acessíveis a outras organizações Buyer da SupplHi, e a troca de informações também pode estar sujeita a acordos específicos - quando existentes - entre a sua organização e a organização Buyer individual.
- A SupplHi é estruturada para não permitir que os seus concorrentes visualizem as informações "industry-shared" que você nos fornece diretamente por meio do nosso site. Para tanto, a nossa plataforma é projetada de modo a gerenciar os direitos de visibilidade de acordo com a organização Buyer específica. De fato, organizações Buyer específicas têm acesso a informações "industry-shared" específicas segundo critérios pré-estabelecidos e, em particular, com base nas categorias de fornecimento da Categorização Padrão SupplHi e nas áreas geográficas de utilização. Esse acesso controlado é implementado para impedir que Vendors e organizações Buyer verticalmente integrados tenham acesso a informações que permitam comparações com concorrentes em base individual. No caso de empresas que atuam tanto como organizações Buyer quanto como Vendor, são fornecidos dois perfis separados, de modo que o perfil da organização Buyer não tenha acesso às informações das empresas ativas nas mesmas famílias de fornecimento em que o Vendor está registrado. No entanto, com a utilização deste serviço, permite-se que as informações estejam disponíveis na Internet e, portanto, ressaltamos novamente que elas não permanecerão em sigilo.

Nenhuma das atividades relacionadas a terceiros é imposta pela SupplHi, que fornece apenas a possibilidade técnica de disponibilizar as informações às organizações Buyer. Por esse motivo, a SupplHi não pode ser responsabilizada por danos, perdas diretas ou indiretas ou outros problemas decorrentes do desenvolvimento autônomo de tais relações com terceiros.

## Gestão das informações e das associações entre Vendor e SupplHi ID

Cada um é responsável por tudo o que ocorre em sua própria conta. A SupplHi não modificará o conteúdo das informações que você nos fornece, as quais serão publicadas sob a sua responsabilidade em nossa plataforma. No entanto, poderemos modificar o layout das informações caso isso seja necessário para torná-las mais legíveis para terceiros.

Quando você visualiza ou utiliza conteúdos e informações de terceiros publicados em nosso site, faz isso por sua conta e risco. A SupplHi não controla as informações fornecidas pelas organizações Buyer ou por outros sujeitos e não pode garantir a sua precisão.

A SupplHi não se responsabiliza pelos conteúdos ou informações fornecidos por você, por outros usuários ou por terceiros, nem por eventuais danos decorrentes da sua publicação, do seu uso ou da confiança neles depositada por usuários ou terceiros.

Ao utilizar o nosso site, você também declara compreender que as informações que você carrega na SupplHi não são confidenciais, mas serão acessíveis aos usuários da SupplHi de acordo com as regras acima especificadas, podendo ainda tornar-se conhecidas de forma geral em decorrência de ações realizadas por terceiros ou Usuários, pelas quais a SupplHi não poderá ser considerada de forma alguma responsável. A SupplHi também não é de forma alguma responsável por qualquer consequência prejudicial ou dano que possa decorrer para você ou para terceiros em razão da divulgação de tais informações.

A associação de um usuário Vendor a um determinado "SupplHi ID", conforme descrito acima, ocorre sob a exclusiva responsabilidade de quem a realiza e de quem fornece a confirmação. A SupplHi não realiza nenhum controle a respeito, nem pode ser responsabilizada em caso de associação incorreta realizada por um Usuário, Super Usuário ou por uma organização Buyer.

Caso a SupplHi seja informada de um compartilhamento de informações ilícitas, incorretas ou inadequadas, poderá ser obrigada por lei a remover tais informações ou conteúdos.

## Direitos sobre as informações

O usuário mantém a titularidade dos direitos sobre os dados carregados e concede à SupplHi uma licença irrevogável, não exclusiva, mundial, que compreende os direitos de reprodução, processamento, adaptação técnica, armazenamento, comunicação e qualquer outro uso necessário ao funcionamento, à segurança, à melhoria e ao desenvolvimento da plataforma. A SupplHi reserva-se o direito de utilizar (por exemplo, analisar, processar e publicar), de forma agregada e também para fins comerciais, os dados não pessoais "industry-shared" disponibilizados pelos Usuários. Em qualquer caso, os dados pessoais carregados pelos usuários não serão utilizados pela SupplHi para qualquer outra finalidade além da prestação do serviço.

## Direitos sobre o software

A SupplHi reserva todos os direitos de propriedade intelectual e industrial sobre os Serviços prestados e sobre o software disponibilizado, bem como sobre as informações e os bancos de dados gerados por meio da utilização do site ou do software.

Ao usar o nosso Serviço, você também se compromete a não modificar, copiar ou criar obras derivadas da SupplHi, dos Serviços ou de qualquer tecnologia relacionada (exceto quando expressamente autorizado pela SupplHi), a não copiar ou utilizar as informações, o conteúdo ou os dados da SupplHi para fins de integração de sistemas ou em relação a um serviço concorrente, a não decodificar, desmontar, descompilar, decifrar ou de qualquer outra forma tentar obter o código-fonte dos Serviços ou de qualquer tecnologia relacionada ou parte deles, e a não monitorar o Serviço, o desempenho ou as funcionalidades da SupplHi para qualquer finalidade competitiva.

## Uso do logotipo da SupplHi

A SupplHi autoriza a sua empresa a utilizar o logotipo e a marca da SupplHi em materiais de marketing (site, e-mail, brochuras, apresentações, etc.) com o único objetivo de identificar a sua empresa como uma organização Vendor ativa na SupplHi. O logotipo da SupplHi não pode ser modificado de forma alguma e só pode ser utilizado para o fim declarado. O logotipo não deve ser utilizado de qualquer forma que possa ser considerada depreciativa ou negativa.

Você também se compromete a não utilizar a palavra "SupplHi" em qualquer nome comercial, e-mail ou URL sem o consentimento da SupplHi.

## Sistemas de inteligência artificial

A SupplHi utiliza sistemas de inteligência artificial supervisionados para realizar a atividade de "Quality Assurance" destinada a garantir a coerência das informações fornecidas pelo Vendor em relação ao solicitado dentro dos Questionários.

A SupplHi permite que os seus usuários utilizem sistemas de inteligência artificial com o objetivo de:

- para os usuários Vendor (por meio da funcionalidade "self-checkout"), para a SupplHi e para as organizações Buyer, realizar a "Quality Assurance" das informações fornecidas pelos Vendors;
- para as organizações Buyer, realizar atividades de "Vendor Scouting".

Os resultados gerados pela inteligência artificial baseiam-se em dados e informações que incluem também os dados especificamente disponibilizados pelos próprios Usuários Vendor durante a utilização da plataforma. A SupplHi não presta nenhuma garantia nem assume qualquer responsabilidade, implícita ou explícita, em relação ao funcionamento e aos resultados obtidos por meio da utilização de ferramentas de inteligência artificial.

## Melhorias e alterações do serviço

A SupplHi pode adicionar, modificar ou excluir qualquer categoria da Categorização Padrão de bens e serviços, bem como qualquer pergunta dirigida ao Vendor, a fim de melhorar o serviço oferecido.

Poderemos alterar ou modificar os preços do serviço ou algumas das presentes condições contratuais. Na medida permitida por lei, tais alterações entrarão em vigor, salvo rescisão exercida pelo usuário mediante notificação adequada por parte da SupplHi.

## Rescisão

Você pode rescindir este acordo a qualquer momento. Uma vez efetuada a rescisão, você perderá o direito de acessar ou utilizar o Serviço. Não obstante a eventual rescisão, os usuários da SupplHi conservarão o direito de compartilhar novamente os conteúdos e as informações fornecidos por meio do Serviço, na medida em que tenham sido copiados ou recompartilhados antes da rescisão.

Se desejar encerrar a sua conta, entre em contato com a nossa equipe pelo endereço info@supplhi.com.

A SupplHi reserva-se o direito de suspender a utilização da sua conta caso isso seja exigido pelas autoridades competentes ou caso haja suspeita legítima de uso ilícito. Caso tal uso ilícito seja confirmado, a SupplHi reserva-se o direito de rescindir o presente acordo.

Em caso de rescisão, todos os dados pessoais presentes são tratados em conformidade com o GDPR, conforme descrito no Data Protection Agreement.

## Lei aplicável e resolução de controvérsias

Na infeliz hipótese de litígio, as partes elegem como foro de competência exclusivo o de Milão (Itália). A lei aplicável é a lei italiana.

## Como entrar em contato conosco

Online no endereço: www.supplhi.com

Por e-mail em: info@supplhi.com

# [POR] Contrato de Nomeação como Operador do Tratamento de Dados - Data Protection Agreement (DPA) para "Vendor"

SupplHi S.r.l. Società Unipersonale, com Sede Legal em Via A. Calabiana, 6 - 20139 Milão (MI), Itália - Código Fiscal e Número de Identificação de IVA 09721660968 - PEC: postmaster@pec.supplhi.com (doravante: "Fornecedor");

e

o sujeito que aceita os Termos e Condições padrão para a utilização do SaaS SRM como usuário "Vendor" (doravante: "Cliente"),

(doravante, designados em conjunto como as "Partes").

Considerando que:

a) o Cliente - por meio da aceitação dos Termos e Condições padrão para a utilização do SaaS SRM por parte dos "Vendors" - celebrou com o Fornecedor um contrato (doravante: "Contrato") que tem por objeto a prestação, por parte do próprio Fornecedor, do serviço SupplHi SRM SaaS para Vendor (doravante: "Serviços");

b) a execução dos referidos Serviços pelo Fornecedor implica o tratamento, por parte deste último, em nome da Sociedade, dos dados pessoais de titulares dos quais a própria Sociedade é Controladora (doravante: "Dados Pessoais"), melhor indicados no ANEXO 2: Âmbito do Tratamento;

*c)* o Fornecedor declara possuir experiência, competências técnicas e recursos que lhe permitem implementar medidas técnicas e organizacionais adequadas, aptas a garantir a conformidade com a legislação em matéria de proteção de dados pessoais e a tutela dos titulares dos dados;

*d)* com o presente Contrato de Nomeação, as Partes pretendem disciplinar o tratamento e a proteção dos Dados Pessoais em conformidade com as normas legais e regulamentares aplicáveis, incluindo o Regulamento (UE) 2016/679, de 27 de abril de 2016, relativo à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais - Regulamento Geral sobre a Proteção de Dados (doravante: "GDPR" ou "Regulamento");

*e)* o Cliente e o Fornecedor também são qualificados, a seguir, respectivamente, como Controlador e Operador;

*f)* para os fins do presente Contrato de Nomeação, os termos "Controlador", "Operador", "titular dos dados", "tratamento", "Autoridade de Controle" terão o significado a eles respectivamente atribuído pelo GDPR.

Diante do exposto (e constituindo as premissas parte integrante e substancial do presente Contrato de Nomeação como Operador do Tratamento de Dados), entre as Partes, acorda-se e estipula-se o seguinte

## 1. Objeto

1.1 As Partes reconhecem e aceitam expressamente que, com referência ao tratamento dos Dados Pessoais, a Sociedade assume o papel de Controladora do tratamento. Como tal, ela é

a única responsável pela correção e legitimidade dos Dados Pessoais, pelo seu uso nos termos do Contrato e pela legitimidade das formas pelas quais foram obtidos.

1.2 A Sociedade nomeia o Fornecedor, nos termos do artigo 28 do GDPR, Operador do tratamento dos Dados Pessoais relacionado à prestação dos Serviços.

## 2. Âmbito do Tratamento

2.1 A finalidade do tratamento dos Dados Pessoais pelo Fornecedor é a prestação dos Serviços nos termos do Contrato. A natureza do tratamento, o tipo de Dados Pessoais tratados e as categorias de titulares estão melhor especificados no ANEXO 2: Âmbito do tratamento.

## 3. Obrigações gerais do Operador

3.1 Os Dados Pessoais serão tratados pelo Operador em conformidade com as normas aplicáveis em matéria de tratamento de dados pessoais, com o presente ato de designação, com eventuais instruções razoáveis recebidas por escrito da Sociedade, desde que tais instruções sejam coerentes com os termos do presente ato de designação, e exclusivamente nos estritos limites em que isso seja necessário para a execução dos Serviços objeto do Contrato, ficando expressamente excluído qualquer outro uso diverso.

3.2 A única exceção possível ao previsto no item 3.1 anterior é a existência de uma obrigação legal ou a solicitação motivada por parte de uma Autoridade administrativa ou judicial, incluindo as Autoridades de Controle (doravante: "Autoridade"), caso em que o Operador, nos limites permitidos pela lei ou pelas determinações da Autoridade, informará a Sociedade sobre os tratamentos de Dados Pessoais diversos ou que excedam o previsto neste ato de designação.

3.3 O Operador compromete-se a instituir e manter atualizado o registro das atividades de tratamento realizadas pelo Operador em nome da própria Sociedade.

## 4. Obrigações relativas à Segurança

4.1 O Operador, levando em consideração os riscos decorrentes da destruição, perda, alteração, divulgação não autorizada ou acesso, de forma acidental ou ilegal, aos Dados Pessoais transmitidos, armazenados ou de qualquer forma tratados, deverá adotar e manter medidas técnicas e organizacionais adequadas para proteger a segurança, a confidencialidade e a integridade dos Dados Pessoais, levando em conta, entre outros aspectos, o tipo de tratamento, as finalidades perseguidas, o contexto e as circunstâncias específicas em que ocorre o tratamento, bem como a tecnologia aplicável e os custos de implementação.

4.2 O Operador compromete-se a adotar as medidas de segurança físicas, lógicas e organizacionais previstas na ISO 27018. Tais medidas só poderão ser alteradas desde que seja mantido um nível de segurança pelo menos igual ao existente no momento da assinatura do presente ato de designação.

4.3 Eventuais evoluções e/ou alterações das medidas de segurança solicitadas pela Controladora serão objeto de cotação econômica específica por parte do Fornecedor e deverão ser aprovadas por escrito por ambas as partes.

4.4 O Operador compromete-se, ainda, a fornecer à Sociedade colaboração em relação à obrigação da Controladora de implementar medidas técnicas e organizacionais adequadas, conforme disposto no artigo 32 do GDPR.

## 5. Sujeitos Autorizados ao Tratamento

5.1 Ressalvado o previsto no artigo 12 a seguir, o Operador garante que o acesso aos Dados Pessoais será limitado aos seus próprios funcionários e colaboradores, nos limites do necessário para a execução dos Serviços e desde que estes sejam devidamente instruídos, nos termos do item 5.2 a seguir, em relação às modalidades de tratamento dos Dados Pessoais e às medidas de segurança técnicas e organizacionais adotadas para a proteção dos Dados Pessoais.

5.2 O Operador compromete-se a designar por escrito os seus funcionários e colaboradores responsáveis por tratar os Dados Pessoais de titularidade da Sociedade por meio de cartas de incumbência específicas, identificando o âmbito de tratamento permitido e fornecendo-lhes as instruções adequadas para esse fim, em particular vinculando-os à confidencialidade sobre todas as informações obtidas no desempenho de suas atividades, inclusive pelo período posterior ao término da relação de trabalho.

## 6. Violações de Dados Pessoais (também denominadas "*Data Breach*")

6.1 O Fornecedor compromete-se a comunicar à Sociedade, por escrito e sem atraso injustificado, toda Violação de Dados Pessoais por ele sofrida ou que lhe tenha sido notificada por qualquer Sub-operador. Em particular, o Fornecedor compromete-se a informar a Controladora sobre toda violação de segurança que acarrete, de forma acidental ou ilícita, a destruição, a perda, a alteração, a divulgação não autorizada ou o acesso aos Dados Pessoais transmitidos, armazenados ou de qualquer forma tratados, e a prestar toda a colaboração necessária à Controladora em relação ao cumprimento das obrigações desta última de notificar tais violações à Autoridade nos termos do art. 33 do GDPR ou de comunicá-las aos titulares dos dados nos termos do art. 34 do GDPR.

6.2 A Controladora terá o direito de realizar toda verificação, inclusive nas instalações do Operador, útil para verificar o cumprimento por parte do Operador das disposições deste artigo, inclusive por meio do preenchimento de questionários de self *assessment*.

## 7. Avaliação de impacto (também denominada "Data Protection Impact Assessment")

7.1 O Operador compromete-se a fornecer à Controladora todos os elementos úteis para a realização, por parte desta última, da avaliação de impacto sobre a proteção de dados, caso esta seja obrigada a realizá-la nos termos do art. 35 do Regulamento, bem como toda colaboração na realização de eventual consulta prévia à Autoridade nos termos do art. 36 do próprio Regulamento.

## 8. Administradores de Sistema

8.1 O Operador do tratamento deverá respeitar as leis aplicáveis em matéria de proteção de dados, incluindo o GDPR, e todas as diretrizes pertinentes emitidas pela Autoridade de controle a respeito do papel e dos deveres dos administradores de sistema.

8.2 O Fornecedor compromete-se, em particular, a:

i) designar como administradores de sistema os profissionais dedicados à gestão e à manutenção de equipamentos de processamento ou de seus componentes, por meio dos quais são realizados tratamentos de Dados Pessoais;

ii) elaborar e manter a lista contendo os dados identificativos das pessoas físicas qualificadas

como administradores de sistema e as funções a elas atribuídas.

## 9. Relações com as Autoridades

9.1 O Operador, mediante solicitação da Controladora, compromete-se a auxiliá-la em caso de procedimentos perante a autoridade de controle ou a autoridade judicial, inclusive permitindo a apresentação tempestiva da documentação de privacidade e dos documentos comprobatórios sob a competência do próprio Operador.

## 10. Solicitações dos Titulares dos Dados

10.1 Caso o titular dos dados se dirija diretamente ao Operador no exercício de seus direitos, o Operador deve atender à solicitação e responder ao titular dos dados em até um mês. Caso isso não seja possível, o Operador, nos limites permitidos por lei, comunicará a solicitação à Controladora.

10.2 Levando em consideração a natureza do tratamento, o Operador auxiliará a Sociedade com medidas técnicas e organizacionais adequadas, na medida em que isso seja possível, no cumprimento da obrigação da Sociedade de atender às solicitações dos titulares dos dados nos termos das normas aplicáveis em matéria.

## 11. Relatórios e Verificações

11.1 O Operador disponibiliza à Controladora todas as informações necessárias para demonstrar o cumprimento das obrigações previstas na referida legislação e/ou das instruções da Controladora constantes do presente ato de designação, e permite à Controladora do tratamento o exercício do poder de controle e inspeção, prestando toda colaboração razoável às atividades de *auditoria* realizadas pela Controladora, com o objetivo de verificar o cumprimento das obrigações e instruções previstas no presente ato de designação. Fica entendido que qualquer verificação realizada nos termos deste artigo deverá ser executada de modo a não interferir no curso normal das atividades do Operador, mediante aviso prévio razoável a este último.

## 12. Sub-operadores

12.1 O Fornecedor poderá se valer de operadores adicionais para tratar os Dados Pessoais de titularidade da Sociedade (doravante: "Sub-operadores"). Com o presente contrato, considera-se concedida a autorização geral prevista no art. 28, item 2, do GDPR, para o recurso aos Sub-operadores atualmente utilizados pelo Fornecedor. A lista dos atuais Sub-operadores consta do ANEXO 3 - Lista dos Sub-operadores.

12.2 O Operador compromete-se a impor por escrito aos seus Sub-operadores, por meio de acordos vinculantes específicos, as mesmas obrigações em matéria de proteção dos Dados Pessoais às quais o Operador está sujeito em virtude do presente ato de designação, em particular no que diz respeito às obrigações em matéria de segurança.

12.3 O Operador compromete-se expressamente a informar a Sociedade sobre eventuais alterações relativas à adição ou substituição de outros Sub-operadores. A Sociedade terá o direito de se opor a tais alterações, comunicando a sua oposição por escrito no prazo de 3 dias corridos a partir da notificação por parte do Operador. Na ausência de oposição, a alteração será considerada aceita.

12.4 Fica expressamente entendido que o Operador permanecerá diretamente responsável perante a Sociedade pelas ações e omissões de seus Sub-operadores.

## 13. Devolução e exclusão dos dados pessoais

13.1 O Operador, no momento do vencimento do Contrato e/ou do encerramento dos Serviços ou, em qualquer caso, de cessação - por qualquer motivo - da eficácia do presente ato de designação, salvo a existência de uma obrigação legal ou regulamentar nacional e/ou comunitária que preveja a conservação dos Dados Pessoais, deverá interromper toda operação de tratamento dos mesmos e deverá providenciar a imediata devolução à mesma dos Dados Pessoais.

## 14. Vigência

14.1 A presente nomeação tem início na data em que é assinada pelas Partes e é válida até o encerramento, por qualquer motivo, do Contrato e/ou, em qualquer caso, dos Serviços, ou até a revogação antecipada por qualquer motivo por parte da Controladora.

## 15. Encarregado de proteção de dados (também denominado “DPO”)

15.1 O Encarregado de proteção de dados designado pelo Operador do Tratamento, nos termos do artigo 37 do GDPR, é Francesco Garrassino (privacy@supplhi.com).

## ANEXO 1 - Medidas Técnico-Organizacionais

Além das medidas de segurança previstas no Contrato e no DPA, o Operador de Tratamento aplica as seguintes medidas de segurança organizacionais.

### Confidencialidade, integridade, disponibilidade e resiliência dos sistemas

**Infraestrutura.** Servidores da SupplHi hospedados em nuvem nos data centers da Amazon Web Services na região europeia (atualmente "eu-west-1", Irlanda), em conformidade com os requisitos de residência de dados previstos pelo GDPR.

**Controle de acessos.** Gestão baseada em papéis (RBAC), segundo o princípio do menor privilégio.

**Autenticação.** Autenticação multifator (MFA) obrigatória para o acesso à plataforma pelos usuários "Vendor". Possibilidade de os Clientes "Buyer" integrarem seu próprio Single Sign-On, tanto para autenticação (SAML) quanto para de/provisionamento (SCIM).

**Segregação de ambientes.** Separação lógica entre os ambientes de desenvolvimento, teste e produção.

**Segregação de dados.** Isolamento lógico dos dados em arquitetura multi-tenant: cada registro é associado a um tenant específico e acessível, por meio de mecanismos de autorização e filtragem aplicativa, apenas aos usuários do mesmo tenant; a eficácia dos controles de isolamento é verificada no âmbito dos processos de teste e segurança aplicativa.

**Registro e monitoramento.** Registro e monitoramento contínuo dos acessos e das atividades do sistema.

**Proteções perimetrais.** Firewalls e sistemas de detecção de intrusões, incluindo o uso de WAF (Web Application Firewall).

**Gestão de vulnerabilidades.** Processo estruturado de vulnerability management e aplicação regular de patches nos sistemas.

### Criptografia e pseudonimização

**Dados em trânsito.** Criptografia por meio do protocolo TLS 1.2 ou superior para todas as comunicações cliente-servidor e entre serviços internos.

**Dados em repouso (at-rest).** Criptografia dos bancos de dados e dos storages por meio das ferramentas nativas do provedor de nuvem AWS.

**Gestão de chaves.** Gestão das chaves de criptografia por meio de serviço dedicado do provedor de nuvem AWS.

### Capacidade de restabelecimento da disponibilidade e do acesso aos dados

**Backup.** Execução de backups com frequência diária, com monitoramento do resultado e retenção de 18 meses.

**Teste de restauração.** Verificação trimestral da integridade dos backups por meio de testes de restauração.

**Disaster Recovery.** Plano de Disaster Recovery e Continuidade de Negócios com objetivos de RPO (Recovery Point Objective) de 36 horas e de RTO (Recovery Time Objective) de 48 horas.

**Redundância.** Redundância de infraestrutura em múltiplas zonas de disponibilidade (Availability Zones) da região AWS eu-west-1 (Irlanda) – data centers fisicamente separados na mesma região – para garantir alta disponibilidade e resiliência em caso de desastre; capacidade de realocação de toda a infraestrutura para outra região AWS europeia (ex.: eu-central-1, Frankfurt), mantendo a residência dos dados na UE, verificada no âmbito dos testes periódicos de Disaster Recovery.

### Testes e verificação periódica da eficácia das medidas

**Certificações.** Certificação ISO/IEC 27001:2022 emitida pela Bureau Veritas para a "Gestão de plataforma SaaS para coleta e gestão de informações de Vendor Management", de acordo com a Declaração de Aplicabilidade, complementada pelos controles das diretrizes ISO/IEC 27017:2015 e ISO/IEC 27018:2019. Disponibilidade de relatórios SOC 1 Type II (auditoria EY) sobre os controles gerais de TI relevantes para os relatórios financeiros dos Clientes, cobrindo os processos de gestão de mudanças, acessos, operações e infraestrutura que alimentam, por meio de integrações aplicativas, os sistemas de gestão/ERP dos Clientes.

**Teste de penetração.** Execução de avaliação de vulnerabilidades e teste de penetração (VA/PT) com frequência ao menos anual e mediante lançamentos significativos, realizada por empresa líder em Cyber Security, com posterior gestão e correção das eventuais vulnerabilidades identificadas.

**Gestão de incidentes.** Procedimento específico destinado à gestão de eventos e incidentes com potencial impacto sobre os dados pessoais, que define papéis e responsabilidades, o processo de detecção (suspeita ou confirmada), a aplicação de medidas de contenção, a resposta e a contenção do incidente/violação, bem como as modalidades por meio das quais realizar as comunicações de violações de dados pessoais ao Cliente.

### Medidas organizacionais

**Políticas de segurança.** Sistema de Gestão de Segurança da Informação (SGSI/ISMS) em conformidade com ISO 27001, ISO 27017 e ISO 27018, com políticas internas documentadas e mantidas nos ciclos de atualização.

**Treinamento.** Treinamento periódico do pessoal sobre proteção de dados e segurança da informação.

**Confidencialidade do pessoal.** Acordos de confidencialidade (NDA) firmados por funcionários e colaboradores com acesso aos dados.

**Gestão de sub-operadores.** Due diligence e qualificação dos sub-processadores, com imposição contratual de obrigações equivalentes por meio de acordos de tratamento de dados em cascata.

**Retenção de dados.** Políticas de retenção e procedimentos de exclusão segura dos dados ao término da relação contratual ou mediante solicitação do Controlador.

**Privacy by design.** Abordagem de "privacy by design and by default" no desenvolvimento de novas funcionalidades da plataforma.

## Segurança física

**Segurança física.** Delegada ao provedor de nuvem AWS, certificado 27001/27017/27018 (segurança e privacidade em nuvem), SOC 1, 2 e 3 para seus data centers, que incluem controles de acesso físico, videovigilância, alimentação elétrica redundante e proteção contra incêndio.

## ANEXO 2 - Âmbito do Tratamento

O presente anexo constitui parte integrante do Contrato de Nomeação como Operador.

**Categorias de titulares dos dados:** usuários fornecedores que se registram na plataforma SupplHi e seus colegas referenciados nas respostas aos questionários.

**Tipo de Dados Pessoais objeto de tratamento.** Os Dados Pessoais tratados são exclusivamente os indicados a seguir:

- Nome, sobrenome e endereço de e-mail corporativo.
- Arquivos de log não aplicativos (por exemplo: o acesso à plataforma, o rastro das solicitações efetuadas ao back-end, etc.) gerados pelos usuários fornecedores durante a utilização da plataforma SupplHi.
- No caso de usuários fornecedores definidos como “Pessoas Físicas”, dados fiscais e IBAN ou outros dados relativos à conta corrente.
- Em alguns casos, também pode ser solicitado o número de telefone corporativo.

**Natureza e finalidade do tratamento:** acesso na plataforma SaaS SupplHi.

**Duração do tratamento:** até o alcance das finalidades e de acordo com os termos de conservação previstos por lei.

## ANEXO 3 - Lista dos Sub-operadores

Os seguintes Sub-operadores são utilizados pela SupplHi:

| *Nome* | *Endereço de faturamento* | *Descrição do tratamento* | *Certificação* | *Local do tratamento* |
|---|---|---|---|---|
| Amazon Web Services EMEA SARL | 38 avenue John F. Kennedy L-1855 Luxemburgo | • Hospedagem<br>• Armazenamento de dados<br>• Backup | • ISO/IEC 27001:2022<br>• ISO/IEC 27017:2015<br>• ISO/IEC 27018:2019<br>• ISO/IEC 27701:2019<br>• ISO/IEC 22301:2019<br>• ISO/IEC 9001:2015 | Europa |
| Microsoft S.r.l. | Microsoft House Viale Pasubio 21 20154 Milão (MI), Itália | • Azure Active Directory<br>• OneDrive | • ISO/IEC 27001:2022<br>• ISO/IEC 27017:2015<br>• ISO/IEC 27018:2019 | Europa |
| Google Cloud Italy S.r.l. | Via Federico Confalonieri 4 20124 Milão, Itália | • Google Cloud<br>• Gemini | • ISO/IEC 27001:2022<br>• ISO/IEC 27017:2015<br>• ISO/IEC 27018:2019 | Europa |
| Aruba S.P.A. | Via S. Clemente, 53 - 24036 Ponte San Pietro (Bergamo), Itália | • Gestão de e-mail | • ISO/IEC 27001:2022<br>• ISO/IEC 27017:2015<br>• ISO/IEC 27018:2019 | Europa |
| Atlassian Pty Ltd | Level 6, 341 George St, - Sydney NSW 2000, Austrália | • Gestão Interna de Tickets | • ISO/IEC 27001:2022<br>• ISO/IEC 27018:2019 | Europa |