SUPPLHI

Adaptive SRM

SupplHi SRM SaaS - Standard T&C and DPA for Vendors

[Italiano]

PUBBLICO

www.supplhi.com

[ITA] Termini e Condizioni standard per l'utilizzo del SaaS SRM da parte dei "Vendor" 3
La nostra missione 3
Accordo 3
Protezione dei dati personali 3
Servizio 4
Costo del servizio 5
Account e obblighi dell'Utente 5
Informazioni fornite 6
Gestione delle informazioni e delle associazioni tra Vendor e SupplHi ID 7
Diritti sulle informazioni 8
Diritti sul software 8
Uso del logo di SupplHi 8
Sistemi di intelligenza artificiale 8
Miglioramenti e modifiche del servizio 9
Recesso 9
Legge applicabile e risoluzione delle controversie 9
Come contattarci 9
[ITA] Contratto di Nomina a Responsabile del Trattamento dei Dati - Data Protection Agreement (DPA) per "Vendor" 10
1. Oggetto 10
2. Ambito del Trattamento 11
3. Obblighi generali del Responsabile 11
4. Obblighi inerenti la Sicurezza 11
5. Soggetti Autorizzati al Trattamento 12
6. Violazioni di Dati Personali (cd. "*Data Breach*") 12
7. Valutazione d'impatto (cd. "Data Protecton Impact Assessment") 12
8. Amministratori di Sistema 12
9. Rapporti con le Autorità 13
10. Istanze degli Interessati 13
11. Reportistica e Verifiche 13
12. Sub-responsabili 13
13. Restituzione e cancellazione dei dati personali 14
14. Durata 14
15. Responsabile della protezione dei dati (c.d. "DPO") 14
ALLEGATO 1 - Misure Tecnico-Organizzative 15
ALLEGATO 2 - Ambito del Trattamento 19
ALLEGATO 3 - Elenco dei Sub-Responsabili 20

[ITA] Termini e Condizioni standard per l'utilizzo del SaaS SRM da parte dei "Vendor"

I seguenti Termini e Condizioni si applicano a tutti gli utenti registrati con un profilo "Vendor" (cioè le organizzazioni che possono fornire beni e/o servizi agli utenti delle organizzazioni "Buyer").

Il profilo "Buyer" (cioè le organizzazioni alle quali SupplHi fornisce l'accesso alla piattaforma per la gestione della propria base di fornitori) ha dei Termini e Condizioni dedicati.

La nostra missione

SupplHi è la piattaforma Software-as-a-Service (SaaS), in cloud, di Supplier Relationship Management (SRM) per le forniture di beni e servizi B2B. La nostra missione è quella di permettere ad ogni organizzazione di crescere tramite la propria filiera. SupplHi, infatti, permette alle organizzazioni Buyer di realizzare i propri processi di gestione della base fornitori in modo efficiente e compliant, nel rispetto delle normative di riferimento e alla luce delle migliori pratiche internazionali di mercato - portando ordine tramite processi di SRM sotto controllo e tramite facile accesso alle informazioni, non perdendo neanche un attimo del proprio tempo.

SupplHi mette a disposizione del mondo B2B la propria infrastruttura digitale con l'obiettivo di aumentare l'efficienza, ridurre i costi e creare maggiori opportunità per organizzazioni Buyer e Vendor, a livello globale.

Tutti i dati della piattaforma SupplHi (form, allegati, informazioni, e-mail) sono memorizzati in strutture ad alta affidabilità e su hosting situati nell'Unione Europea (attualmente in Irlanda) su Amazon Web Services (AWS).

È inoltre possibile utilizzare il nostro sito web di marketing navigando come Visitatore. In questo caso non è necessario effettuare il login, ma non è possibile accedere a tutti i contenuti e alle funzionalità della piattaforma. Quando usi i servizi che offriamo, entri a far parte del nostro network e prometti di usare il nostro sito responsabilmente e di rispettarne le regole di utilizzo.

Accordo

Registrandoti sul nostro sito concludi un contratto con SupplHi S.r.l. Società Unipersonale, Via A. Calabiana, 6 - 20139 Milano, Italia, registrata presso la C.C.I.A.A. di Milano con il numero 09721660968, R.E.A. MI 2110015, con Codice Fiscale e Partita IVA 09721660968, info@supplhi.com (di seguito semplicemente "SupplHi") e accetti tutte le seguenti condizioni in nome e per conto tuo o della società della quale fai le veci. Questo accordo disciplina anche l'uso delle applicazioni mobili.

Se la tua società ti ha autorizzato ad agire come rappresentante, stai stipulando questo accordo per conto della tua società. Entrambi siete soggetti alle regole stabilite nel presente accordo. Se non sei autorizzato, sei vincolato personalmente dal presente accordo. Utilizzando il nostro sito web, confermi di avere almeno 18 anni e di avere diritto a concludere il presente accordo.

Protezione dei dati personali

Ogni trattamento di dati personali è svolto da SupplHi per prestare il servizio richiesto in qualità di responsabile, così come definito all'art. 4, par. 1, n. 8 del Regolamento generale sulla protezione dei dati personali 2016/679, in ottemperanza alle indicazioni contenute nel Data Protection Agreement.

Servizio

Il ruolo di SupplHi è quello di fornire alle organizzazioni Buyer - attraverso la piattaforma SaaS - l'accesso ad informazioni strutturate e costantemente aggiornate sui Vendors al fine di poter gestire in autonomia i propri processi di Supplier Relationship Management (SRM). Ad esempio, SupplHi non decide se un determinato Vendor è qualificato o meno, né all'interno della rete delle organizzazioni Buyer che usano la piattaforma, né nei confronti di una specifica organizzazione Buyer e la decisione di qualifica di un Vendor resta sempre in capo alla singola organizzazione Buyer.

Nell'ambito dell'erogazione dei servizi alle organizzazioni Buyer e sulla base dei moduli e delle funzionalità selezionate e configurate per ogni specifica organizzazione Buyer, SupplHi offre i seguenti Servizi gratuiti ai Vendor:

- Gestire per ogni Vendor (sia essa una società o una persona fisica) - tramite codici identificativi definiti da SupplHi su base nazionale (VAT, TIN, numero di Registrazione), richiesti in fase di creazione di un nuovo Vendor in piattaforma - un codice "SupplHi ID" univoco;
- Permettere l'associazione di un utente Vendor ad un determinato "SupplHi ID". Tale associazione può essere svolta dall'Utente Vendor che si registra, dal Super Utente o da un'organizzazione Buyer. L'associazione effettuata dall'Utente ad un Vendor dove è già presente un Super Utente deve essere confermata dal Super Utente stesso. L'associazione comporta la possibilità per l'Utente di visualizzare e gestire le informazioni riguardanti il suo Vendor di riferimento. L'associazione avviene sotto l'esclusiva responsabilità di chi la compie e, quando necessario, di chi fornisce la conferma. SupplHi non effettua nessun controllo in merito, né può essere ritenuta responsabile in caso di errata associazione compiuta da un Utente, Super Utente o da un'organizzazione Buyer. Un Utente Vendor, come identificato da uno specifico indirizzo email, può essere associato solamente ad un unico SupplHi ID e, quindi, ad un univo Vendor.
- Avere uno o più Super Utente/i del Vendor in grado di gestire i diritti di visibilità e di gestione delle informazione per gli Utenti collegati allo stesso Vendor e di cedere o estendere, in piattaforma e in qualsiasi momento, il proprio ruolo di Super-Utente ad un collega specifico;
- Ospitare in piattaforma le informazioni fornite dal Vendor nelle varie fasi di registrazione e di compilazione, tramite Questionari dedicati, delle informazioni richieste dalle organizzazioni Buyer, siano esse "industry-shared" o "customer-specific". Si precisa infatti che le informazioni inserite dal Vendor in piattaforma in risposta ai Questionari possono essere di due tipologie, chiaramente evidenziate in piattaforma all'interno dei singoli Questionari:
    - "customer-specific": le informazioni saranno visibili solamente alla specifica organizzazione Buyer chiaramente riconoscibile al Vendor. Solo tale specifica organizzazione Buyer potrà visualizzarle, copiarle e utilizzarle.
    - "industry-shared": le informazioni saranno potenzialmente visibili a tutte le organizzazioni Buyer che hanno accesso alla piattaforma SupplHi. Questi potranno visualizzarle, copiarle e utilizzarle. La presenza di informazioni "industry-shared" permette di ridurre il tuo sforzo di compilazione delle tipiche informazioni ricomprese nei questionari di pre-qualifica e qualifica (e.g. presenza di certificazioni di qualità, numero di addetti, presenza di un codice etico, etc.) per più organizzazioni Buyer e per aumentare la visibilità presso le organizzazioni Buyer che utilizzano la piattaforma.
- Supportare il Vendor nelle fasi di compilazione ed aggiornamento delle informazioni richieste dalle organizzazioni Buyer all'interno dei Questionari, generando la lista di informazioni mancanti e realizzando - in modo automatico o manuale - l'attività di "Quality Assurance" volta

a garantire la coerenza delle informazioni fornite dal Vendor rispetto alla richiesta;

- Una volta che il Vendor raggiunge il 100% di completamento delle informazioni e dopo l'attività di "Quality Assurance", sulla base della loro tipologia ("industry-shared" o "customer-specific"), rendere visibili alle organizzazioni Buyer ai quali SupplHi fornisce accesso in piattaforma le informazioni fornite dal Vendor;
- Permettere al Vendor di ampliare i propri canali commerciali per la vendita di forniture B2B attraverso la visibilità che si acquisisce nei confronti delle organizzazioni Buyer che utilizzano la piattaforma. Teniamo infatti a sottolineare che, utilizzando il nostro sito, consenti a tutti gli utenti delle organizzazioni Buyer di visualizzare ed estrarre in modo semplice le informazioni "industry-shared" che carichi sulla nostra piattaforma, utilizzando gli strumenti da noi messi a disposizione, e che tali informazioni potrebbero dunque circolare nella rete anche fuori dal nostro controllo;
- Notificare al Vendor le informazioni in scadenza e consentire l'aggiornamento in piattaforma;
- Consentire al Vendor di candidarsi ai processi di Qualifica nei confronti di una specifica organizzazione Buyer;
- Consentire la possibilità di visualizzare uno o più risultati di classificazione e scoring del Vendor, sulla base della configurazione realizzata per la singola organizzazione Buyer;
- Tramite la funzionalità di "Vendor Actions", permettere di descrivere le azioni di miglioramento societario che il Vendor sta ponendo in essere;
- Consentire consentire al Vendor di ricevere RFx (richieste di informazioni, proposte, quotazioni) da parte dei dell'organizzazione Buyer attraverso i contatti forniti dal Vendor;
- Tramite il modulo di "Management of Contractual Documents" e la funzionalità di "Document Exchange", consentire lo scambio di documenti specifici;
- Tramite il modulo denominato "SupplAuth", permettere tecnicamente l'accesso ad altri sistemi applicativi configurati dall'organizzazione Buyer (ad es. sistemi di gestione ordini o di gara). Il sistema di autorizzazione è controllato dall'organizzazione Buyer in modo esclusivo e senza la possibilità, per SupplHi, di decidere in alcun modo i livelli di autorizzazione agli altri applicativi;
- Supportare il Vendor tramite la pubblicazione di manualistica e Frequently Asked Questions (FAQ) dedicate agli utenti Vendor e le attività di Help Desk tramite il sistema di ticketing presente all'interno della piattaforma.

Ulteriori eventuali Servizi e rapporti tra il Vendor e SupplHi sono regolati dai Termini e Condizioni del Servizio specifico.

SupplHi si impegna a mettere in atto misure di sicurezza informatiche adeguate agli *standard* di settore a tutela di tutti i dati e per la fornitura di un servizio quanto migliore possibile.

Costo del servizio

SupplHi fornisce gratuitamente ai Vendor i Servizi descritti nel presente contratto.

Account e obblighi dell'Utente

Utilizzando il nostro sito dichiari di non essere già soggetto a restrizioni da parte di SupplHi nell'utilizzo dei Servizi e ti impegni a:

1. attivare un solo account personale e a che la tua società abbia un solo account SupplHi come

Vendor;

2. fornire il tuo nome reale e il nome reale della tua società;
3. rispettare tutte le previsioni di legge applicabili e le policy interne come, ad esempio, la legge sulla protezione dei dati personali, sulla proprietà intellettuale, sullo spamming, etc.;
4. utilizzare i Servizi offerti da SupplHi solo a scopo professionale e non personale;
5. non agire in modo scorretto, pubblicando contenuti inappropriati o inesatti, non contattare gli altri utenti per ogni forma di comunicazione non desiderata, o porre in essere condotte non conformi alla legge, o che siano calunniose, offensivo, oscene, discriminatorie o in ogni caso discutibili;
6. non utilizzare o tentare di utilizzare l'account di altri;
7. non danneggiare un altro soggetto o qualsiasi altra società che utilizzi il nostro sito.

Ti impegni a scegliere una password sicura, a mantenerla segreta e a non condividere l'account con nessun altro. Tutti gli utenti che si registrano nella piattaforma SupplHi sono soggetti a una *password policy*.

Per creare il profilo della tua società, rispenderai alle domande in piattaforma e, quando necessario, aggiornerai le tue risposte. A questo scopo garantisci che le informazioni fornite a SupplHi:

- siano accurate;
- vengano prontamente aggiornate;
- non contengano nulla che violi il diritto di terzi, che la tua società non ti autorizzi a condividere o che sia altrimenti illecito. A titolo esemplificativo, ti impegni a non violare i diritti di proprietà intellettuale o industriale di terze parti, inclusi brevetti, marchi, segreti commerciali, diritti d'autore o altri diritti, non aggiungere contenuti che non siano destinati o che non siano esatti rispetto al campo da compilare (ad esempio, l'inserimento di un numero di telefono nella "email" o in qualsiasi altro campo);
- riflettano i beni ed i servizi effettivamente offerti come Vendor.

Informazioni fornite

Quando ci fornisci informazioni riguardanti la tua organizzazione, altri possono visualizzare, copiare e utilizzare tali informazioni. In particolare, le informazioni e i contenuti che ci fornisci saranno visualizzati dagli utenti delle organizzazioni Buyer.

Ti informiamo che, al fine di fornire a Vendor e organizzazioni Buyer il nostro servizio, e per motivi di *compliance*, tutte le interazioni o modifiche al tuo profilo come Vendor sulla piattaforma vengono registrate e memorizzate da SupplHi. Per tali motivi, tu e SupplHi sarete in grado di accedere a tali informazioni. Solo i dati aziendali e nessun dato personale - fatta eccezione per l'email dell'utente - saranno memorizzati a questo scopo.

Al fine di fornire il nostro servizio a Vendor e organizzazioni Buyer, tutte le interazioni o le modifiche al profilo del vostro Vendor sulla piattaforma vengono registrate e rese visibili alle organizzazioni Buyer. I dati personali eventualmente trattati da SupplHi a tale scopo saranno gestiti in ottemperanza al principio di minimizzazione di cui all'art. 25 del GDPR e con tutte le misure di sicurezza previste nel Data Protection Agreement.

Al fine di fornire agli utenti un servizio più completo, le informazioni che ci fornisci potrebbero essere visualizzate insieme ad altre informazioni che le organizzazioni Buyer che utilizzano

SupplHi possono legittimamente utilizzare in riferimento alla tua società e ai servizi che fornisce (ad esempio: punteggi di solidità finanziaria forniti dalle agenzie di rating finanziario).

Le informazioni che carichi sul nostro sito secondo una delle due modalità – "industry-shared" e "customer-specific" sopra definite potranno essere visualizzate ed estratte dalle organizzazioni Buyer secondo le seguenti regole.

- Le informazioni "customer-specific" non saranno accessibili ad altre organizzazioni Buyer di SupplHi e lo scambio di informazioni può anche essere soggetto agli accordi specifici - quando presenti - tra la tua organizzazione e la singola organizzazione Buyer.
- SupplHi è costruito per non consentire ai tuoi concorrenti di visualizzare le informazioni "industry-shared" che ci fornisci direttamente tramite il nostro sito. A tal fine, la nostra piattaforma è progettata in modo da gestire i diritti di visibilità a seconda della specifica organizzazione Buyer. Infatti, organizzazioni Buyer specifiche hanno accesso a informazioni "industry-shared" specifiche secondo criteri prestabiliti e, in particolare, in base alle categorie di fornitura della Categorizzazione Standard SupplHi e alle aree geografiche di utilizzo. Tale accesso controllato viene realizzato per impedire ai Vendor e alle organizzazioni Buyer verticalmente integrati di avere accesso a informazioni che possano permettere di confrontarsi con i concorrenti su base individuale. Nel caso di società che agiscono sia come organizzazioni Buyer, sia come Vendor, vengono forniti due profili separati, in modo che il profilo dell' organizzazione Buyer non abbia accesso alle informazioni delle società attive nelle stesse famiglie di fornitura in cui il Vendor è registrato. Tuttavia, con l'utilizzo di questo servizio si consente che le informazioni siano disponibili su Internet e, pertanto teniamo a sottolineare nuovamente che queste non resteranno segrete.

Nessuna delle attività connesse a terze parti è imposta da SupplHi, che fornisce solo la possibilità tecnica di rendere disponibili le informazioni alle organizzioni Buyer. Per tale ragione, SupplHi non può essere ritenuta responsabile per danni, perdite dirette o indirette o altri problemi derivanti dallo sviluppo autonomo di tali relazioni con i terzi.

Gestione delle informazioni e delle associazioni tra Vendor e SupplHi ID

Ciascuno è responsabile di tutto ciò che accade nel proprio account. SupplHi non modificherà il contenuto delle informazioni che ci fornisci, che saranno pubblicate sotto la tua responsabilità sulla nostra piattaforma. Tuttavia, potremo modificare il layout delle informazioni nel caso in cui ciò fosse necessario per renderle meglio leggibili ad altri.

Quando vedi o utilizzi i contenuti e le informazioni di altri pubblicati sul nostro sito, lo fai a tuo rischio. SupplHi non controlla le informazioni fornite dalle organizzazioni Buyer o di altri soggetti e non può garantirne l'accuratezza.

SupplHi non risponde dei contenuti o delle informazioni forniti da te, da altri utenti o da terzi e per gli eventuali danni derivanti dalla loro pubblicazione, dal loro uso o dall'affidamento su questi fatto dagli utenti o da terzi.

Utilizzando il nostro sito dichiari anche di comprendere che le informazioni che carichi su SupplHi non sono segrete, ma saranno conoscibili agli utenti di SupplHi secondo le regole sopra specificate, potendo altresì divenire conoscibili in via generale a seguito di azioni intraprese da terzi o Utenti per le quali SupplHi non potrà essere considerata in alcun modo responsabile. SupplHi non è inoltre in alcun modo responsabile per ogni conseguenza pregiudizievole o danno possa derivare a te o a terzi dalla diffusione di tali informazioni.

L'associazione di un utente Vendor ad un determinato "SupplHi ID" come sopra descritta avviene sotto l'esclusiva responsabilità di chi la compie e di chi fornisce la conferma. SupplHi non effettua

nessun controllo in merito, né può essere ritenuta responsabile in caso di errata associazione compiuta da un Utente, Super Utente o da un'organizzazione Buyer.

Nel caso in cui SupplHi venisse informata di una condivisione di informazioni illecite, non corrette o inappropriate, potrebbe essere tenuta per legge a rimuovere tali informazioni o contenuti.

Diritti sulle informazioni

L'utente mantiene la titolarità dei diritti sui dati caricati e concede a SupplHi una licenza irrevocabile, non esclusiva, mondiale, comprendente i diritti di riproduzione, elaborazione, adattamento tecnico, archiviazione, comunicazione e ogni altro utilizzo necessario al funzionamento, alla sicurezza, al miglioramento e allo sviluppo della piattaforma. SupplHi si riserva il diritto di utilizzare (e.g. analizzare, elaborare e pubblicare), in forma aggregata e anche per finalità commerciali, i dati non personali "industry-shared" resi disponibili dagli Utenti. In ogni caso, i dati personali caricati dagli utenti non saranno utilizzati da SupplHi per altro scopo oltre a quello della fornitura del servizio.

Diritti sul software

SupplHi si riserva tutti i diritti di proprietà intellettuale e industriale sui Servizi prestati e sul software messo a disposizione, nonché sulle informazioni e sui database generati tramite l'utilizzo del sito o tramite il software.

Usando il nostro Servizio, ti impegni inoltre a non modificare, copiare o creare opere derivate di SupplHi, dei Servizi o di qualsiasi tecnologia correlata (ad eccezione di quanto espressamente autorizzato da SupplHi), non copiare o utilizzare le informazioni, il contenuto o i dati su SupplHi a scopo di system integration o in relazione ad un servizio concorrente, non decodificare, disassemblare, decompilare, decifrare o tentare in altro modo di derivare il codice sorgente per i Servizi o qualsiasi tecnologia correlata o parte di essi e a non monitorare il Servizio, le prestazioni o le funzionalità di SupplHi per qualsiasi scopo competitivo.

Uso del logo di SupplHi

SupplHi autorizza la tua società ad utilizzare il logo e il marchio di SupplHi nel materiale di marketing (sito Web, e-mail, brochure, presentazioni, etc.) al solo scopo di identificare la tua azienda come organizzazione di Vendor attiva su SupplHi. Il logo di SupplHi non può essere modificato in alcun modo e può essere utilizzato solo per lo scopo dichiarato. Il logo non deve essere utilizzato in alcun modo che possa essere considerato denigratorio o negativo.

Ti impegni inoltre a non utilizzare la parola "SupplHi" in qualsiasi nome commerciale, email o URL se non con il consenso di SupplHi.

Sistemi di intelligenza artificiale

SupplHi utilizza sistemi di intelligenza artificiale supervisionati per svolgere l'attività di "Quality Assurance" volta a garantire la coerenza delle informazioni fornite dal Vendor rispetto alla richiesta all'interno dei Questionari.

SupplHi consente ai propri utenti di utilizzare sistemi di intelligenza artificiale allo scopo di:

- per gli utenti Vendor (tramite la funzionalità di "self-checkout"), per SupplHi e per le organizzazioni Buyer, realizzare "Quality Assurance" delle informazioni fornite dai Vendors;

- per le organizzazioni Buyer, realizzare attività di “Vendor Scouting”.

I risultati generati dall’intelligenza artificiale si basano su dati e informazioni che includono anche i dati specificatamente messi a disposizione dagli Utenti Vendor stessi durante l’utilizzo della piattaforma. SupplHi non presta alcuna garanzia né si assume alcuna responsabilità, implicita o esplicita, rispetto al funzionamento e ai risultati ottenuti attraverso l’utilizzo di strumenti di intelligenza artificiale.

Miglioramenti e modifiche del servizio

SupplHi può aggiungere, modificare o eliminare qualsiasi categoria della Categorizzazione Standard di beni e servizi, nonché qualsiasi domanda rivolta al Vendor al fine di migliorare il servizio offerto.

Potremmo cambiare o modificarne i prezzi del servizio o alcune delle presenti condizioni contrattuali. Nella misura consentita dalla legge, tali modifiche saranno efficaci salvo recesso esercitato dall’utente a seguito di idonea notifica da parte di SupplHi.

Recesso

Puoi recedere dal presente accordo in qualsiasi momento. Una volta effettuato il recesso, perderai il diritto di accedere o utilizzare il Servizio. Nonostante l’eventuale intervenuto recesso, gli utenti di SupplHi conserveranno il diritto di condividere nuovamente i contenuti e le informazioni forniti tramite il Servizio nella misura in cui questi sono stati copiati o ricondivisi prima del recesso.

Se desideri chiudere il tuo account, contatta il nostro team all'indirizzo info@supplhi.com.

SupplHi si riserva il diritto di sospendere l’utilizzo del suo account qualora gli sia richiesto dalle competenti autorità o qualora vi sia un legittimo sospetto di illecito utilizzo. In caso tale illecito utilizzo sia confermato, SupplHi si riserva il diritto di terminare il presente accordo.

In caso di recesso, tutti i dati personali presenti sono trattati conformemente al GDPR, come descritto nel Data Protection Agreement.

Legge applicabile e risoluzione delle controversie

Nella malaugurata ipotesi di lite, le parti scelgono quale foro di competenza elettivo quello di Milano (Italia). La legge applicabile è quella italiana.

Come contattarci

Online all'indirizzo: www.supplhi.com

Via email a: info@supplhi.com

[ITA] Contratto di Nomina a Responsabile del Trattamento dei Dati - Data Protection Agreement (DPA) per "Vendor"

SupplHi S.r.l. Società Unipersonale, la cui Sede Legale è sita in Via A. Calabiana, 6 - 20139 Milano (MI), Italia - Codice Fiscale e Partita IVA 09721660968 - PEC: postmaster@pec.supplhi.com (di seguito: "Fornitore");

e

il soggetto che accetta i Termini e Condizioni standard per l'utilizzo del SaaS SRM come utente "Vendor" (di seguito: "Cliente"),

(di seguito, collettivamente definite le "Parti").

Premesso che:

a) il Cliente - tramite l'accettazione dei Termini e Condizioni standard per l'utilizzo del SaaS SRM da parte dei "Vendor" - ha stipulato con il Fornitore un contratto (di seguito: "Contratto") avente ad oggetto l'erogazione, da parte del Fornitore stesso, del servizio di SupplHi SRM SaaS per Vendor (di seguito: "Servizi");

b) lo svolgimento dei suddetti Servizi da parte del Fornitore comporta il trattamento, da parte di quest'ultimo, per conto della Società, dei dati personali di interessati di cui la Società stessa è Titolare (di seguito: "Dati Personali"), meglio indicati in ALLEGATO 2: Ambito del trattamento;

c) il Fornitore dichiara di possedere esperienza, competenze tecniche e risorse che gli consentono di mettere in atto misure tecniche e organizzative adeguate atte a garantire la conformità alla normativa in materia di tutela dei dati personali e la tutela degli interessati;

d) con il presente Contratto di Nomina, le Parti intendono disciplinare il trattamento e la protezione dei Dati Personali in conformità alle norme di legge e di regolamento applicabili, ivi incluso il Regolamento (UE) 2016/679 del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali - Regolamento Generale sulla Protezione dei Dati Personali (di seguito: "GDPR" o "Regolamento");

e) il Cliente ed il Fornitore sono qualificati anche, nel prosieguo, rispettivamente, quali Titolare e Responsabile;

f) ai fini del presente Contratto di Nomina, i termini "Titolare", "Responsabile", "interessato", "trattamento", "Autorità di Controllo" avranno il significato ad essi rispettivamente attribuito dal GDPR.

Tutto ciò premesso (e costituendo le premesse parte integrante e sostanziale del presente Contratto di Nomina a Responsabile del Trattamento dei Dati), fra le Parti si conviene e si stipula quanto segue

1. Oggetto

1.1 Le Parti espressamente riconoscono ed accettano che, con riferimento al trattamento dei Dati Personali, la Società riveste il ruolo di Titolare del trattamento. In quanto tale, essa è l'unica responsabile della correttezza e della legittimità dei Dati Personali, del loro utilizzo ai sensi del Contratto e della legittimità delle modalità con cui essi sono stati acquisiti.

1.2 La Società nomina il Fornitore, ai sensi dell'articolo 28 del GDPR, Responsabile del trattamento dei Dati Personali connesso all'erogazione dei Servizi.

2. Ambito del Trattamento

2.1 La finalità del trattamento dei Dati Personali da parte del Fornitore è la prestazione dei Servizi ai sensi del Contratto. La natura del trattamento, la tipologia di Dati Personali trattati e le categorie di interessati sono meglio specificate nell'ALLEGATO 2: Ambito del trattamento.

3. Obblighi generali del Responsabile

3.1 I Dati Personali saranno trattati dal Responsabile in conformità alle norme applicabili in materia di trattamento dei dati personali, al presente atto di designazione, alle eventuali ragionevoli istruzioni ricevute per iscritto dalla Società, a condizione che tali istruzioni siano coerenti con i termini del presente atto di designazione, e solo ed esclusivamente negli stretti limiti in cui ciò risulti necessario per l'esecuzione dei Servizi oggetto del Contratto, restando espressamente escluso ogni altro e diverso utilizzo.

3.2 L'unica deroga possibile rispetto a quanto previsto al comma 3.1 che precede è l'esistenza di un obbligo di legge o la richiesta motivata da parte di un'Autorità amministrativa o giurisdizionale, ivi incluse le Autorità di Controllo (di seguito: "Autorità"), nel qual caso il Responsabile, nei limiti consentiti dalla legge o dai provvedimenti dell'Autorità, provvederà ad informare la Società dei trattamenti di Dati Personali diversi o eccedenti rispetto a quanto previsto dal presente atto di designazione.

3.3 Il Responsabile si obbliga a istituire e tenere aggiornato il registro delle attività di trattamento svolte dal Responsabile per conto della Società medesima.

4. Obblighi inerenti la Sicurezza

4.1 Il Responsabile, tenendo conto dei rischi che derivano dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale ai Dati Personali trasmessi, conservati o comunque trattati provvederà ad adottare e a mantenere misure tecniche ed organizzative adeguate per proteggere la sicurezza, la riservatezza e l'integrità dei Dati Personali, tenendo conto, fra l'altro, della tipologia di trattamento, delle finalità perseguite, del contesto e delle specifiche circostanze in cui avviene il trattamento, nonché della tecnologia applicabile e dei costi di attuazione.

4.2 Il Responsabile si obbliga ad adottare le misure di sicurezza fisiche, logiche e organizzative previste dalla ISO 27018. Tali misure potranno essere modificate solo a condizione che venga mantenuto un livello di sicurezza almeno pari a quello esistente al momento della sottoscrizione del presente atto di designazione.

4.3 Eventuali evoluzioni e/o modifiche delle misure di sicurezza richieste dal Titolare saranno oggetto di specifica quotazione economica da parte del Fornitore e dovranno essere approvate per iscritto da entrambe.

4.4 Il Responsabile si impegna, altresì, a fornire alla Società collaborazione in relazione all'obbligo del Titolare di mettere in atto misure tecniche ed organizzative adeguate, secondo quanto disposto dall'articolo 32 del GDPR.

5. Soggetti Autorizzati al Trattamento

5.1 Fatto salvo quanto previsto all'articolo 12 che segue, il Responsabile garantisce che l'accesso ai Dati Personali sarà limitato ai propri dipendenti e collaboratori nei limiti di quanto necessario per l'esecuzione dei Servizi e a condizione che gli stessi siano istruiti in maniera appropriata, ai sensi del comma 5.2 che segue, in relazione alle modalità di trattamento dei Dati Personali e alle misure di sicurezza tecniche ed organizzative poste a tutela dei Dati Personali.

5.2 Il Responsabile si impegna a designare per iscritto i propri dipendenti e collaboratori deputati a trattare i Dati Personali di titolarità della Società tramite apposite lettere di incarico, individuando l'ambito di trattamento consentito e fornendo loro le istruzioni idonee allo scopo, in particolare vincolandoli alla riservatezza su tutte le informazioni acquisite nello svolgimento della loro attività, anche per il periodo successivo alla cessazione del rapporto di lavoro.

6. Violazioni di Dati Personali (cd. "*Data Breach*")

6.1 Il Fornitore si impegna a comunicare alla Società, per iscritto e senza ingiustificato ritardo, ogni Violazione dei Dati Personali subita da sé o notificatagli da qualsivoglia Sub-responsabile. In particolare, il Fornitore si impegna ad informare il Titolare di ogni violazione della sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque trattati, ed a prestare ogni necessaria collaborazione al Titolare in relazione all'adempimento degli obblighi sullo stesso gravanti di notifica delle suddette violazioni all'Autorità ai sensi dell'art. 33 del GDPR o di comunicazione della stessa agli interessati ai sensi dell'art. 34 del GDPR.

6.2 Il Titolare avrà diritto di effettuare ogni verifica, anche presso le sedi del Responsabile, utile al fine di verificare il rispetto da parte del Responsabile delle prescrizioni del presente articolo, anche tramite la compilazione di questionari di self *assessment*.

7. Valutazione d'impatto (cd. "Data Protecton Impact Assessment")

7.1 Il Responsabile s'impegna a fornire al Titolare ogni elemento utile all'effettuazione, da parte di quest'ultimo, della valutazione di impatto sulla protezione dei dati, qualora lo stesso sia tenuto ad effettuarla ai sensi dell'art. 35 del Regolamento, nonché ogni collaborazione nell'effettuazione della eventuale consultazione preventiva al Garante ai sensi dell'art. 36 del Regolamento stesso.

8. Amministratori di Sistema

8.1 Il Responsabile del trattamento dovrà rispettare le leggi applicabili in materia di protezione dei dati, incluso il GDPR, e tutte le linee guida pertinenti emanate dall'Autorità di controllo in merito al ruolo e ai doveri degli amministratori di sistema.

8.2 Il Fornitore si impegna, in particolare, a:

i) designare quali amministratori di sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di Dati personali;

ii) predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali amministratori di sistema e le funzioni ad essi attribuite.

9. Rapporti con le Autorità

9.1 Il Responsabile, su richiesta del Titolare, si impegna a coadiuvare quest'ultimo in caso di procedimenti dinanzi all'autorità di controllo o all'autorità giudiziaria, anche consentendogli la tempestiva esibizione della modulistica privacy e dei documenti probatori rientranti nella competenza del Responsabile stesso.

10. Istanze degli Interessati

10.1 Nel caso in cui l'interessato si rivolga direttamente al Responsabile nell'esercizio dei suoi diritti, il Responsabile deve evadere la richiesta e rispondere all'interessato entro un mese. Qualora ciò non sia possibile, il Responsabile, nei limiti consentiti dalla legge, provvederà a dare comunicazione al Titolare della richiesta.

10.2 Tenuto conto della natura del trattamento, il Responsabile assisterà la Società con misure tecniche ed organizzative adeguate, nella misura in cui ciò sia possibile, nell'adempimento dell'obbligo della Società di dar seguito alle richieste degli interessati ai sensi delle norme applicabili in materia.

11. Reportistica e Verifiche

11.1 Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla suddetta normativa e/o delle istruzioni del Titolare di cui al presente atto di designazione e consente al Titolare del trattamento l'esercizio del potere di controllo e ispezione, prestando ogni ragionevole collaborazione alle attività di *audit* effettuate dal Titolare, con lo scopo di controllare l'adempimento degli obblighi e delle istruzioni di cui al presente atto di designazione. Resta inteso che qualsiasi verifica condotta ai sensi del presente articolo dovrà essere eseguita in maniera tale da non interferire con il normale corso delle attività del Responsabile e fornendo a quest'ultimo un ragionevole preavviso.

12. Sub-responsabili

12.1 Il Fornitore potrà avvalersi di ulteriori responsabili per trattare i Dati Personali di titolarità della Società (di seguito: "Sub-Responsabili"). Con il presente contratto, si intende prestata l'autorizzazione generale di cui all'art. 28, comma 2 del GDPR, al ricorso ai Sub-Responsabili attualmente utilizzati dal Fornitore. L'elenco degli attuali Sub-Responsabili è riportato nell'ALLEGATO 3 - Elenco dei Sub-Responsabili.

12.2 Il Responsabile si obbliga ad imporre per iscritto ai propri Sub-Responsabili, attraverso appositi accordi vincolanti, i medesimi obblighi in materia di protezione dei Dati Personali cui è soggetto il Responsabile in virtù del presente atto di designazione, in particolare sotto il profilo degli obblighi in materia di scurezza.

12.3 Il Responsabile si impegna espressamente ad informare la Società di eventuali modifiche riguardanti l'aggiunta o la sostituzione degli ulteriori Sub-responsabili. La Società avrà il diritto di opporsi a tali modifiche, comunicando la sua opposizione per iscritto entro 3 giorni di calendario dalla notifica da parte del Responsabile. In mancanza di opposizione, la modifica si intenderà accettata.

12.4 Resta espressamente inteso che il Responsabile rimarrà direttamente responsabile nei confronti della Società in ordine alle azioni e alle omissioni dei propri Sub-responsabili.

13. Restituzione e cancellazione dei dati personali

13.1 Il Responsabile, all'atto della scadenza del Contratto e/o della cessazione dei Servizi o, comunque, in caso di cessazione – per qualunque causa – dell'efficacia del presente atto di designazione, salvo la sussistenza di un obbligo di legge o di regolamento nazionale e/o comunitario che preveda la conservazione dei Dati Personali, dovrà interrompere ogni operazione di trattamento degli stessi e dovrà provvedere all'immediata restituzione allo stesso dei Dati Personali.

14. Durata

14.1 La presente nomina decorre dalla data in cui viene sottoscritta dalle Parti ed è valida fino alla cessazione per qualunque motivo del Contratto e/o, comunque, dei Servizi ovvero fino alla revoca anticipata per qualsiasi motivo da parte del Titolare.

15. Responsabile della protezione dei dati (c.d. "DPO")

15.1 Il Responsabile della protezione dei dati designato dal Responsabile del Trattamento, ai sensi dell'articolo 37 del GDPR, è Francesco Garrassino (privacy@supplhi.com).

ALLEGATO 1 - Misure Tecnico-Organizzative

In aggiunta alle misure di sicurezza previste nel Contratto e nel DPA, il Responsabile del Trattamento applica le seguenti *misure di sicurezza organizzative:*

Riservatezza, integrità, disponibilità e resilienza dei sistemi

Categoria	*Misura adottata*
Infrastruttura	I server SupplHi sono ospitati sul cloud nei data center di Amazon Web Service nella regione Europea (attualmente con sede nella regione "eu-west-1" in Irlanda), garantendo il pieno rispetto dei requisiti GDPR.
Controllo accessi	Gestione basata su ruoli (RBAC), secondo il principio del minimo privilegio.
Autenticazione	Autenticazione a più fattori (MFA) disponibili per l'accesso alla piattaforma degli utenti "Vendor". La password policy prevede le seguenti regole: • avere una lunghezza minima di 8 caratteri; • contenere almeno un carattere maiuscolo; • contenere almeno un carattere minuscolo; • contenere almeno un carattere numerico; • contenere almeno un carattere non alfa-numerico; • non essere uguale alle precedenti 5 password; • essere modificata con cadenza almeno trimestrale; • essere modificata dopo il primo accesso; • non deve essere riconducibile a dati personali dell'utente, quali nome o la data di nascita, né a famigliari o animali domestici. Inoltre, possibilità di e Single Sign-On (SSO/SAML) per gli utenti "Buyer".
Segregazione ambienti	Separazione logica tra ambienti di sviluppo, test e produzione.
Segregazione dati	I clienti hanno accesso ai propri dati sulla piattaforma secondo un approccio multi-tenant: il database è condiviso, e ogni record all'interno della struttura multi-tenant è assegnato a un record specifico per il tenant. Attraverso l'uso di filtri specifici e meccanismi di autorizzazione, solo gli utenti appartenenti allo stesso tenant possono accedere / visualizzare il record specifico.
Logging e monitoraggio	Registrazione e monitoraggio continuo degli accessi e delle attività di sistema.

Categoria	*Misura adottata*
Protezioni perimetrali	Firewall e sistemi di rilevamento delle intrusioni, incluso l'utilizzo di WAF (Web Application Firewall).
Gestione vulnerabilità	Processo strutturato di vulnerability management e patching regolare dei sistemi.

Cifratura e pseudonimizzazione

Categoria	*Misura adottata*
Dati in transito	Cifratura tramite protocollo TLS 1.2 o superiore per tutte le comunicazioni client-server e tra servizi interni.
Dati a riposo (at-rest)	Cifratura dei database e degli storage tramite gli strumenti nativi del cloud provider AWS.
Gestione delle chiavi	Gestione delle chiavi di cifratura tramite servizio dedicato del cloud provider AWS.

Capacità di ripristino della disponibilità e dell'accesso ai dati

Categoria	*Misura adottata*
Backup	Esecuzione di backup con frequenza giornaliera e retention di 18 mesi.
Test di restore	Verifica periodica dell'integrità dei backup tramite test di ripristino.
Disaster Recovery	Piano di Disaster Recovery e Business Continuity con obiettivi di RPO (Recovery Point Objective) di 36 ore e di RTO (Recovery Time Objective) di 48 ore.
Ridondanza	Ridondanza infrastrutturale grazie al fatto che tutte le risorse AWS utilizzate da SupplHi sono distribuite in tutta Europa, nello specifico sono distribuite in tre zone di disponibilità (per garantire il recupero in caso di disastri) nel data center AWS irlandese.

Test e verifica periodica dell'efficacia delle misure

Categoria	*Misura adottata*
Certificazioni	SupplHi è certificata da Bureau Veritas in accordo alla ISO/IEC 27001:2022 per la "*Gestione di piattaforma SaaS per raccolta e gestione di informazioni di Vendor Management*" in accordo con la Dichiarazione di Applicabilità Rev. 7.01 del 01/04/2025 integrata dai controlli previsti dalle linee guida ISO/IEC 27017:2015 e ISO/IEC 27018:2019. Presenza, inoltre, di SOC 2 Type II – elaborato da EY – sulla base dei controlli descritti nel Report stesso.
Penetration test	Esecuzione di penetration test e vulnerability assessment (VA/PT) con frequenza annuale, a cura di primaria società di Cyber Security.
Gestione incidenti	Incident Response Plan formalizzato, con notifica al Titolare del trattamento entro 72 ore dalla rilevazione.

Misure organizzative

Categoria	*Misura adottata*
Politiche di sicurezza	Sistema di Gestione della Sicurezza delle Informazioni (SGSI/ISMS) conforme a ISO 27001, ISO 27017 e ISO 27018 con politiche interne documentate e manutenute nei cicli di aggiornamento. Presenza, inoltre, di politiche di sicurezza in accordo ai controlli definiti nel SOC 1 Type II Report annuale.
Formazione	Formazione periodica del personale su data protection e sicurezza delle informazioni.
Riservatezza del personale	Accordi di riservatezza (NDA) sottoscritti da dipendenti e collaboratori con accesso ai dati.
Gestione sub-responsabili	Due diligence e qualificazione dei sub-processor, con imposizione contrattuale di obblighi equivalenti tramite accordi di trattamento dati a cascata.
Data retention	Politiche di conservazione e procedure di cancellazione sicura dei dati al termine del rapporto contrattuale o su richiesta del Titolare.
Privacy by design	Approccio "privacy by design and by default" nello sviluppo di nuove funzionalità della piattaforma.

Sicurezza fisica

Categoria	*Misura adottata*
Sicurezza fisica	Demandata al cloud provider AWS, certificato 27001/27017/27018 (sicurezza e privacy cloud), SOC 1, 2 e 3 per i propri data center, che includono controlli di accesso fisico, videosorveglianza, alimentazione ridondata e protezione antincendio.

ALLEGATO 2 - Ambito del Trattamento

Il presente allegato costituisce parte integrante del Contratto di Nomina a Responsabile. I Dati Personali gestiti sono esclusivamente quelli di seguito indicati.

Categorie di interessati	• Utenti fornitori che si registrano alla piattaforma SupplHi e loro colleghi referenziati nelle risposte ai questionari.
Tipo di Dati Personali oggetto di trattamento	• Nome, cognome e indirizzo e-mail. • I file di log non applicativi (ad esempio: l'accesso in piattaforma, la traccia delle richieste effettuate a back-end, …) generati dagli utenti fornitori durante l'utilizzo della piattaforma SupplHi. • In alcuni casi potrebbe anche essere richiesto il numero di telefono aziendale • Nel caso di utenti fornitori definiti come "Persone Fisiche", dati fiscali e IBAN o altri dati relativi al conto corrente
Natura e finalità del trattamento	Accesso a SaaS su piattaforma SupplHi.
Durata del trattamento	Fino al perseguimento delle finalità e secondo i termini di conservazione previsti dalla legge.

ALLEGATO 3 - Elenco dei Sub-Responsabili

I seguenti Sub-Responsabili sono utilizzati da SupplHi:

Name	*Indirizzo di fatturazione*	*Descrizione del trattamento*	*Certificazione*	*Location del trattamento*
Amazon Web Services EMEA SARL	38 avenue John F. Kennedy L-1855 Luxembourg	• Hosting • Data storage • Backup	• ISO/IEC 27001:2022 • ISO/IEC 27017:2015 • ISO/IEC 27018:2019 • ISO/IEC 27701:2019 • ISO/IEC 22301:2019 • ISO/IEC 9001:2015	Europe
Microsoft S.r.l.	Microsoft House Viale Pasubio 21 20154 Milano (MI), Italy	• Azure Active Directory • OneDrive	• ISO/IEC 27001:2022 • ISO/IEC 27017:2015 • ISO/IEC 27018:2019	Europe
Google Cloud Italy S.r.l.	Via Federico Confalonieri 4 20124 Milano, Italy	• Google Cloud • Gemini	• ISO/IEC 27001:2022 • ISO/IEC 27017:2015 • ISO/IEC 27018:2019	Europe
Aruba S.P.A.	Via S. Clemente, 53 - 24036 Ponte San Pietro (Bergamo), Italy	• Email management	• ISO/IEC 27001:2022 • ISO/IEC 27017:2015 • ISO/IEC 27018:2019	Europe
Atlassian Pty Ltd	Level 6, 341 George St, - Sydney NSW 2000, Australia	• Internal Ticket Management	• ISO/IEC 27001:2022 • ISO/IEC 27018:2019	Europe