STAR
High business performance

ATTO DI DESIGNAZIONE A RESPONSABILE DEL TRATTAMENTO

AI SENSI E PER GLI EFFETTI DELL'ART. 28 DEL REGOLAMENTO EUROPEO 27 APRILE 2016, N.679 ("GDPR")

Tra

Il **CLIENTE**, in qualità di Titolare del trattamento dati, ai sensi dell'art. 4 del Regolamento UE 2016/679 (GDPR) (di seguito, la "**Titolare del trattamento**" o "**Società**"),

e

STAR S.R.L. con sede legale in Piave 22, Cabiate (CO), nella persona del legale rappresentante (di seguito, il "Responsabile del trattamento", "Fornitore")
(collettivamente, definite le "**Parti**")

PREMESSO CHE

a) il Fornitore e la Società hanno stipulato, un contratto di seguito, "**Contratto**", avente ad oggetto l'erogazione, da parte del Fornitore stesso, del/dei servizio/i oggetto del contratto

Finalità del trattamento	Trattamento dei dati limitatamente alle finalità oggetto del contratto		
Tipo di dati personali	Dati personali	Dati particolari (Ex dati sensibili)	Dati giudiziari
	☑ nome ☑ cognome ☑ e-mail ☑ mansione ☑ data e luogo di nascita ☑ codice fiscale/partita iva ☑ il Responsabile può venire a conoscenza dei Nominativi degli interessati (attività /incarichi lavorativi da loro svolti) nelle fasi di vita del singolo prodotto chimico (proposta, accettazione/rifiuto disattivazione).	Non presenti	Non presenti
Categoria di interessati	Dipendenti, Consulenti del Titolare del trattamento, collaboratori (stagisti, interinali, apprendisti), Clienti		
Modalità di trattamento	Cartaceo ed automatizzato		
Natura del trattamento	☒ *la raccolta,* ☒ *la registrazione,* ☒ *l'organizzazione,* ☒ *la strutturazione,*		

	☒ *la conservazione, per la durata prevista dal contratto e/o la durata prevista dalla legge,* ☒ *l'adattamento o la modifica,* ☒ *l'estrazione,* ☒ *la consultazione,* ☒ *l'uso,* ☒ *la comunicazione mediante trasmissione,* ☐ *diffusione o qualsiasi altra forma di messa a disposizione,* ☒ *il raffronto o l'interconnessione,* ☒ *la limitazione,* ☒ *la cancellazione o la distruzione.*

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**");

c) il Consulente 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;

d) con il presente atto, le Parti intendono regolare i trattamenti dei Dati Personali da parte del Fornitore ai sensi dell'art. 28.3 del 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, entrato in vigore il 24 maggio 2016 e applicabile dal 25 maggio 2018 (di seguito, "**GDPR**" o "**Regolamento**");

Tutto ciò premesso (e costituendo le premesse parte integrante del presente atto di designazione), fra le Parti si conviene e si stipula quanto segue

OGGETTO: Con il presente atto, il Fornitore è nominato **Responsabile del trattamento dei Dati Personali** cin forza del rapporto contrattuale in essere tra le parti.

OBBLIGHI DEL RESPONSABILE: La sottoscrizione del presente atto vincola il Responsabile del trattamento al Titolare del trattamento e fa sorgere in capo al Responsabile una serie di obblighi specificamente individuati in apposita e separata clausola che segue il presente documento (**Allegato A**).

MISURE DI SICUREZZA E VIOLAZIONE DEI DATI: Il Responsabile è tenuto a mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio in merito al trattamento dei dati effettuato (art. 32 GDPR) meglio precisate nell'**Allegato B** del presente documento.

DECORRENZA – DURATA - CESSAZIONE DEL TRATTAMENTO
Il ruolo e le competenze assegnate al Responsabile del trattamento con il presente atto hanno la medesima durata ed efficacia del Contratto intercorrente tra le Parti e pertanto si intendono valide fino alla cessazione del Contratto stesso. In caso di rinnovo del Contratto o di un nuovo contratto tra le Parti per cui il Fornitore dovrà svolgere le medesime attività di trattamento di dati personali indicate in Premessa, il contenuto del presente atto deve intendersi automaticamente rinnovato.
In ogni caso, dopo il completamento del trattamento per conto del Titolare, il Responsabile deve, su istruzioni del Titolare del trattamento, restituire o cancellare i dati personali, e le relative copie esistenti, salvo che non siano previste specifiche e differenti politiche di conservazione dei dati (anche in relazione alle categorie di dati trattati) a norma del diritto dell'Unione o degli Stati membri cui è soggetto il Responsabile del trattamento. In entrambi i casi il Responsabile deve rilasciare contestualmente un'attestazione scritta che presso lo stesso non esiste alcuna copia dei dati personali trattati in nome e per conto del Titolare del trattamento.

Con l'occasione, Le ricordiamo l'importanza delle prescrizioni di legge in materia di trattamento dei dati personali, nonché il fatto che la violazione di dette normative può comportare responsabilità sia civili che penali per il Titolare e per il Responsabile, nonché l'applicazione di sanzioni amministrative e pecuniarie, ai sensi degli artt. 82,83 e 84 GDPR.

Resta, altresì, inteso che nessun ulteriore compenso o rimborso Le spetterà per l'assunzione della funzione di Responsabile per il trattamento dei dati personali di cui alla presente comunicazione.

Si prega, dunque, di voler cortesemente restituire copia della presente sottoscritta per accettazione.

Lì, _____, _____

Per il Titolare	**Per il Responsabile**
Azienda_____	**Star Srl**
Ruolo: _____	Ruolo: Legale Rappresentante pro-tempore
Nome: _____	Nome: Marta Penati
Firma: _____	Firma: _____

ALLEGATI:

- *Allegato A. Obblighi del Responsabile del trattamento designato.*
- *Allegato B.* Misure di Sicurezza e Violazione dei dati.

ALLEGATO A. Obblighi del Responsabile del trattamento designato.
(art. 28 e Considerando 81 e ss del Regolamento EU 2016/679)

In virtù dell'atto che vincola il Responsabile designato al Titolare del trattamento, sorgono in capo al Responsabile una serie di obblighi.

1. **Rispetto delle istruzioni impartite dal/i Titolare/i:** Il Responsabile deve assistere e coadiuvare il Titolare nella corretta gestione delle operazioni di trattamento che dovranno esser effettuate nel pieno rispetto degli obblighi previsti dal GDPR. A tale proposito, il Responsabile deve trattare i dati personali soltanto su istruzione documentata del Titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Responsabile del trattamento; in tal caso, il Responsabile deve informare il Titolare circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
2. **Riservatezza**: Il Responsabile deve assicurare per sé stesso e per le persone, da lui o dal Titolare del trattamento autorizzate al trattamento dei dati personali, piena riservatezza rispetto alle operazioni di trattamento effettuate.
   Sarà cura del Responsabile, qualora lo reputasse opportuno, vincolare le persone autorizzate al trattamento dei dati al segreto mediante un adeguato obbligo legale di riservatezza, anche per il periodo successivo all'estinzione del rapporto di lavoro intrattenuto con il Responsabile, in relazione alle operazioni di Trattamento da essi eseguite.
3. **Conformità a leggi e regolamenti applicabili:** Il Responsabile è tenuto ad uniformarsi alle disposizioni del GDPR e più in generale, di ogni altra disposizione normativa, nazionale e sovranazionale, in materia di trattamento dei dati personali attualmente in vigore o che in futuro vengano a modificare, integrare o sostituire l'attuale disciplina, nonché dei provvedimenti dell'Autorità Garante competente e delle linee guida adottate dall'European Data Protection Board.
4. **Misure di sicurezza:** Il Responsabile è tenuto a mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio in merito al trattamento dei dati effettuato (art. 32 GDPR). Si veda **Allegato B. Misure di sicurezza e Violazione dei dati**;
5. **Audit:** Il Responsabile del trattamento deve riferire al Titolare, ogni volta che riceve specifica richiesta per iscritto in tal senso, sui dettagli relativi all'adempimento di quanto disposto dal presente contratto nonché dalla normativa privacy, o attraverso relazioni scritte o attraverso compilazione di check list che verranno fornite. Previa notifica, e con un preavviso non inferiore a giorni 30, il Titolare può verificare l'adempimento del Fornitore accedendo ai locali aziendali del Fornitore coinvolti nel Trattamento dei Dati personali del Cliente durante il normale orario d'ufficio del Fornitore.
   Inoltre, il Responsabile deve contribuire alle attività di revisione, comprese le ispezioni, svolte dal Titolare con almeno 30 giorni di preavviso e ad informare prontamente il Titolare del trattamento di ogni questione rilevante ai fini del presente mandato, quali a titolo indicativo:
   - Istanze di interessati;
   - Richieste del Garante;
   - Esiti delle ispezioni;
   - Violazioni del GDPR o di altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati, o la messa in pericolo della riservatezza, della completezza o dell'integrità dei dati personali.
6. **Persone autorizzate al trattamento:** Il Responsabile si avvale di persone autorizzate al trattamento dei dati che operano sotto la sua responsabilità, in quanto deputati alle operazioni di Trattamento, e alle quali fornisce specifiche istruzioni scritte (salvo che il diritto

dell'Unione o degli Stati membri non richieda diversamente, art. 29 GDPR). È compito del Responsabile designato vigilare sulla corretta esecuzione delle istruzioni impartite (art.4.10 GDPR).

7. **Subresponsabile:** Il Titolare del trattamento autorizza il Responsabile del trattamento a ricorrere ad un altro Responsabile (di seguito "Subresponsabile") per l'esecuzione di specifiche attività di trattamento.
   Il Responsabile informa il Titolare di eventuali modifiche riguardanti l'aggiunta o la sostituzione di altri Responsabili, alle quali il Titolare del trattamento conserva il diritto di opporsi.
   Al "Subresponsabile" sono imposti gli stessi obblighi in materia di protezione dei dati contenuti nel contratto che lega il Titolare e il Responsabile del trattamento. Il "Subresponsabile" è tenuto ad: osservare, valutare e organizzare la gestione del trattamento dei dati personali e la loro protezione (mettendo in atto tutte le misure tecniche ed organizzative adeguate per assicurare un livello di sicurezza adeguato al rischio derivante dal trattamento dati effettuato) affinché questi siano trattati in modo lecito e pertinente e nel rispetto della normativa vigente. Qualora il "Subresponsabile" del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del "Subresponsabile" anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" *(*art. 82. 1 e 82. 3 GDPR).

Elenco dei Sub-Responsabili.

Per il trattamento dei dati personali il Fornitore utilizza i seguenti Sub-responsabili:

RAGIONE SOCIALE SUB-FORNITORE	SERVIZIO/TRATTAMENTO DI DATI PERSONALI	PAESI SEE o EXTRA SEE DI UBICAZIONE TRATTAMENTO DATI PERSONALI
1.Easynet	Data center e sviluppo software	NO
2.Sfelab	Sviluppo software	NO

8. **Rispetto del Provvedimento a carattere generale sugli Amministratori di Sistema dell'Autorità Garante Privacy del 27 Novembre 2008:** Il Responsabile garantirà al Titolare del trattamento che ciascun incaricato amministratore di sistema accederà con proprio utente e propria password. Con l'accettazione di questa nomina il Responsabile si impegna a nominare individualmente - ai sensi del Provvedimento a carattere generale dell'Autorità Garante Privacy del 27 Novembre 2008 (G.U. N. 300 Del 24 dicembre 2008) così come modificato dal Provvedimento a carattere generale dell'Autorità Garante Privacy del 25 giugno 2009 (G.U. N. 149 Del 30 giugno 2009) - gli incaricati della sua struttura che rivestono il ruolo di Amministratori del Sistema informativo. La designazione quale Amministratore di Sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Il Responsabile, su richiesta scritta del Titolare, fornirà al Titolare del trattamento l'elenco aggiornato degli Amministratori di sistema e provvederà a verificare l'attività dei soggetti individuati, come indicato dal Garante Privacy nel Provvedimento sugli Amministratori di Sistema sopra richiamato. Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.
   Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.
9. **Registro dei Trattamenti:** Ove applicabile, il Responsabile deve tenere un Registro delle attività di trattamento svolte sotto la propria responsabilità in nome e per conto del Titolare del trattamento (art. 30 GDPR).
   Il Registro, anche in formato elettronico, deve contenere tutta una serie di informazioni, che il Responsabile raccoglie anche interfacciandosi con i vari uffici o unità interne e/o esterne all'azienda, che trattano dati personali per conto del Titolare.
   In particolare:
   - il nome e i dati di contatto del Responsabile del trattamento;
   - le categorie dei trattamenti effettuati per conto di ogni Titolare;
   - i trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale;
   - una descrizione delle misure tecniche adottate.

   Il Responsabile del trattamento deve mettere il Registro a disposizione dell'Autorità di controllo, se questa ne fa richiesta, affinché possa fungere da strumento per il monitoraggio dei trattamenti effettuati (Considerando 82 GDPR)
10. **Esercizio dei diritti dell'interessato:** Il Responsabile, dovrà informare tempestivamente e per iscritto il Titolare del trattamento, della ricezione di eventuali richieste degli interessati, avanzate ai sensi degli artt. da 15 a 22 del GDPR, in merito, tra l'altro, alle finalità e alle modalità del trattamento, all'origine dei dati, all'aggiornamento, alla rettificazione, cancellazione, alla portabilità e limitazione dei dati od opposizione al trattamento (compresa la profilazione), o al fine di revocare il consenso prestato e/o proporre reclamo al Garante per la protezione dei dati personali.

In particolare, il Responsabile è tenuto a:

- coordinarsi a tal fine con le funzioni aziendali preposte dal Titolare alle relazioni con i soggetti interessati;
- darne tempestiva comunicazione scritta al Titolare allegando copia della richiesta;
- accertare l'identità del richiedente per verificare la legittimità della richiesta;
- attivare le dovute procedure atte a dare seguito alle richieste per l'esercizio dei diritti degli interessati, senza ingiustificato ritardo, e comunque, al più tardi entro 5 giorni dal ricevimento della richiesta stessa, ai sensi dell'art. 12 GDPR.

11. Altri adempimenti: il Responsabile del trattamento è tenuto altresì a:

- cooperare con l'Autorità di Controllo quando richiesto;
- supportare l'attività svolta dal DPO (Data Protection Officer – Responsabile della Protezione dei Dati) per conto del Titolare del trattamento, se nominato (artt. 37,38 GDPR);
- designare per iscritto un Rappresentante che lo rappresenti nell'Unione, se il Responsabile non è stabilito nell'UE e ricorrano i presupposti di cui all'art. 27 GDPR.

***

ALLEGATO B. Misure di Sicurezza e Violazione dei dati

(artt.32 e ss e Considerando 74-77, 83 e ss del Regolamento EU 2016/679 – GDPR)

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Responsabile del trattamento deve mettere in atto misure tecniche e organizzative adeguate per assicurare un livello di sicurezza adeguato al rischio, previste dall'art. 32 GDPR,
Tali misure devono assicurare un elevato livello di sicurezza. Nella valutazione del rischio per la sicurezza dei dati il Responsabile del trattamento deve tenere in considerazione i rischi presentati dal trattamento dei dati personali come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale. Il Responsabile del trattamento, se necessario e su richiesta, dovrà altresì assistere il Titolare del trattamento nella redazione del "DPIA" (*Data Protection Impact Assessment),* contenente la valutazione sulla particolare probabilità e gravità del rischio inerente alle operazioni di trattamento da effettuare (tenuto conto della natura, dell'ambito di applicazione, del contesto, delle finalità e delle fonti di rischio) e sulle misure tecniche ed organizzative da adottare al fine di attenuare tale rischio assicurando la protezione dei dati personali e la conformità al GDPR. Se del caso, il Responsabile dovrà richiedere in merito un parere al DPO (*Data Protection Officer*), se nominato (art.35 e C.90 GDPR).
Violazione dei dati. Se dovesse venire a conoscenza di una violazione dei dati personali (*Data Breach*), il Responsabile, senza ingiustificato ritardo e non oltre 48 ore deve informare per iscritto **il Titolare del Trattamento** affinché possa procedere, se del caso, a notificare la violazione all'autorità di controllo competente (art.33 GDPR) e, qualora la violazione dei dati personali in questione dovesse essere suscettibile di presentare un elevato rischio per i diritti e le libertà delle persone fisiche, il Titolare del trattamento provvederà a darne comunicazione all'interessato (art.34 GDPR).
Il Responsabile dovrà aiutare il Titolare del trattamento a documentare per iscritto qualsiasi violazione di dati subita, le circostanze ad essa relative, le conseguenze e i provvedimenti adottati per porvi rimedio.
Nello specifico dovranno essere documentati:

a) la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) il nome e i dati di contatto del DPO (se nominato) o di altro punto di contatto presso cui l'Autorità di controllo competente potrà ottenere maggiori informazioni;
c) la descrizione delle probabili conseguenze della violazione dei dati personali;
d) le descrizioni delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

Tale documentazione dovrà essere resa disponibile dal Titolare del trattamento all'Autorità di controllo competente attraverso la procedura di notifica della violazione dei dati (*Data breach)* prevista dall'art. 33 comma 3 del GDPR.