

**ACCORDO SUL TRATTAMENTO DEI DATI PERSONALI
(ai sensi e per gli effetti dell'art. 28 del Regolamento UE 679/2016)**

TRA

La Camera di Commercio di Foggia (partita IVA 00837390715 - codice fiscale 80002570713) con sede legale in Foggia - Via Michele Protano n.7, pec cciaa@fg.legalmail.camcom.it (di seguito "**CCIAA**" o "**Titolare**") in persona del proprio Segretario Generale dott.ssa Lorella Palladino

E

Unioncamere, con sede legale in Piazza Sallustio, 21, 00187 - Roma ("**Fornitore**" o "**Responsabile**") in persona del proprio Segretario Generale dott. Giuseppe Tripoli

(di seguito, singolarmente la "**Parte**" e collettivamente le "**Parti**").

PREMESSO CHE

- a) in esecuzione delle attività connesse e afferenti al CRM di sistema in relazione al rapporto giuridico intrattenuto con il Titolare (i "**Servizi**"), con particolare riferimento alle operazioni di trattamento relative alle attività meglio dettagliate all'Annex I (le "**Attività**"), il Fornitore tratterà dati personali per conto di CCIAA;
- b) la CCIAA, prima di affidare al Fornitore lo svolgimento delle Attività ha valutato che il Fornitore abbia adottato presidi idonei a garantire la tutela e la protezione dei dati personali trattati per conto del Titolare;
- c) con il presente accordo (di seguito "**Accordo**") il Titolare intende nominare il Fornitore quale Responsabile del trattamento dei dati personali ai sensi dell'art. 28 del Regolamento (UE) 2016/679, nonché fornirgli le istruzioni necessarie per le operazioni di trattamento;

Tutto ciò premesso, le Parti concordano e stipulano quanto segue.

1. Definizioni

1.1. Ai fini del presente Accordo, valgono le seguenti definizioni:

- per **“Dati personali”** si intendono tutte le informazioni relative ad una persona fisica, identificata o identificabile (l’**“Interessato”**) che il Responsabile tratta per conto del Titolare allo scopo di fornire i Servizi;
- per **“Legge applicabile”** si intende il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati* (il **“Regolamento”** o **“GDPR”**), nonché qualsiasi altra normativa o atto avente forza normativa in materia di protezione dei dati personali applicabile in Italia, ivi compresi i provvedimenti del Garante;
- per **“Garante”** si intende l’Autorità di cui all’art. 51 del Regolamento, che svolge le funzioni indicate nel successivo art. 57, GDPR;
- per **“Misure di sicurezza”** si intendono le misure di sicurezza indicate dall’art. 32, GDPR e nei provvedimenti del Garante.

2. Nomina

- 2.1. Con la sottoscrizione del presente Accordo, il Titolare nomina il Fornitore, che accetta, Responsabile ai sensi dell’art. 28 del Regolamento.

3. Operazioni di trattamento, tipologia di dati personali e categorie di interessati

- 3.1. Come meglio dettagliato nell’Annex A, il presente Accordo si riferisce a tutte le operazioni di trattamento connesse e funzionali all’esecuzione delle Attività (le **“Operazioni di trattamento”**).
- 3.2. Le Operazioni di trattamento avranno ad oggetto le seguenti categorie di dati personali: dati identificativi, di contatto (a titolo esemplificativo, nome, cognome, e-mail, nome utente, codice fiscale, data di nascita, nazionalità, Regione, Provincia, nonché denominazioni sociali e ragione sociale, e credenziali di accesso) (**“Dati Personali”**).
- 3.3. Il Responsabile tratterà i Dati personali riferiti alle seguenti categorie di interessati: legali rappresentanti delle imprese iscritte presso il Titolare, imprese, società, singoli imprenditori, professionisti, aspiranti imprenditori, studenti, utenti (gli **“Interessati”**).

4. Rapporti con Sub-responsabili

- 4.1. Il Responsabile può sub-appaltare i Servizi che implicino il trattamento di Dati personali per conto del Titolare, informandolo tempestivamente.
- 4.2. Il Titolare autorizza il Responsabile ad avvalersi di Sub-responsabili esclusivamente localizzati sul territorio europeo ovvero, solo previa autorizzazione del Titolare e applicazione di idonee garanzie ai sensi del

GDPR, anche di Sub-responsabili localizzati al di fuori del territorio europeo. Si rinvia all'Annex B per l'elenco dei Sub-responsabili autorizzati.

- 4.3. Il Responsabile si impegna espressamente a selezionare i propri Sub-responsabili con riferimento ai profili di rischio del trattamento dei dati oggetto del presente Accordo e, solo in caso di esito positivo della valutazione, a vincolarli alle medesime obbligazioni cui il Responsabile stesso è tenuto in virtù del presente Accordo, nonché a vigilare, anche per mezzo di specifiche attività di audit, che gli stessi rispettino le istruzioni fornite.
- 4.4. Il Responsabile si impegna a fornire una lista aggiornata dei Sub-responsabili e/o le risultanze della selezione e/o delle attività di audit entro 15 gg lavorativi dalla richiesta del Titolare.
- 4.5. Fermo restando quanto sopra, resta inteso tra le Parti che il Fornitore è responsabile nei confronti dell'interessato e del Titolare con riferimento al rispetto da parte di ciascun Sub-responsabile della Normativa applicabile. Il Titolare, ad ogni modo, si riserva di vietare al Responsabile di avvalersi di Sub-responsabili che a proprio insindacabile giudizio non offrano idonee garanzie di affidabilità e rispetto della Normativa Applicabile e/o del presente Accordo. In tal caso il Responsabile si impegna a non interrompere le Attività e a sostituire il Sub-responsabile con altro che offra idonee garanzie di affidabilità e rispetto della Normativa Applicabile e/o del presente Accordo.

5. Obblighi del Responsabile

- 5.1. Fermo restando ogni altro obbligo previsto dalla Normativa applicabile, il Responsabile si impegna a:
 - a. trattare i Dati personali esclusivamente per le finalità indicate nel presente Accordo, nonché per le finalità ulteriori che il Titolare dovesse eventualmente e successivamente indicare;
 - b. trattare i Dati personali in piena conformità alla Legge applicabile, alla *best practice* in materia di protezione dei dati personali in ragione delle Operazioni di trattamento svolte, nonché alle istruzioni qui fornite da parte del Titolare ovvero, di quelle ulteriori che lo stesso dovesse, in futuro, ritenere opportuno fornire per la migliore e più efficiente esecuzione delle attività; le ulteriori istruzioni che dovessero essere fornite dal Titolare, saranno rese al Responsabile per iscritto;
 - c. garantire che tutte le persone agenti sotto la propria autorità alle quali sia consentito di accedere o anche trattare i Dati personali abbiano sottoscritto idoneo impegno, o siano altrimenti comunque adeguatamente vincolate, a mantenere totale riservatezza rispetto a tali dati e che, a tal fine, gli stessi

agiscano sotto il costante controllo del Responsabile ed in conformità alle istruzioni da quest'ultimo fornite. Qualora applicabile in relazione alle Operazioni di Trattamento, nominare con atto scritto i propri autorizzati quali Amministratori di Sistema, effettuare le attività di verifica previste dal Provvedimento *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008)* smi e fornire a richiesta del Titolare l'elenco aggiornato degli Amministratori di Sistema nominati;

- d. non consentire a terzi l'accesso ai Dati personali, se non in presenza di adeguati presupposti di liceità per tali ulteriori trattamenti;
- e. tenere i Dati personali separati dai dati detenuti per proprie finalità e/o conto di altri soggetti;
- f. adottare idonea procedura di gestione delle violazioni della sicurezza da cui derivino, accidentalmente o in modo illecito, la distruzione, la perdita, la divulgazione non autorizzata o l'accesso ai Dati personali (c.d. *data breach*) o, in alternativa, conformarsi e dare adeguata attuazione alla corrispondente *policy* che dovesse essere trasmessa da parte del Titolare, prestando in ogni caso la massima collaborazione nei confronti dello stesso al fine di eliminare o quantomeno ridurre al minimo gli impatti derivanti da eventi di questo tipo;
- g. notificare senza ingiustificato ritardo al Titolare e, comunque, entro un tempo ragionevole dalla scoperta degli eventi (24 ore) che rientrino nella fattispecie del c.d. *data breach*, nonché informare prontamente il Titolare riguardo a qualsiasi ulteriore evento, fatto o circostanza, prevedibile o meno, da cui possa derivare un rischio elevato per i diritti e le libertà fondamentali degli interessati coinvolti nelle Operazioni di trattamento;
- h. collaborare con il Titolare, limitatamente ai trattamenti relativi ai Dati personali, nell'assolvimento degli obblighi di:
 - i) notifica delle violazioni di dati al Garante o ad altre autorità di controllo competenti e, laddove richiesto in ragione dell'elevato livello di rischio per i diritti e le libertà degli interessati, anche a questi ultimi;
 - ii) esecuzione, qualora ritenuto necessario dal e su richiesta del Titolare, di idonea valutazione di impatto sulla protezione dei dati, oltre che nello svolgimento delle procedure di consultazione preventiva con il Garante o le altre autorità competenti;
- i. nell'ambito dello svolgimento delle Operazioni di trattamento, mettere il Titolare al corrente – senza ingiustificato ritardo e comunque entro e non oltre

3 giorni lavorativi dalla ricezione - riguardo a qualsiasi richiesta di esercizio di diritti che il Responsabile dovesse ricevere da parte degli Interessati;

- j. segnalare senza indugio al Titolare eventuali istruzioni che il Responsabile ritiene in violazione della Legge applicabile (“Istruzione Contestata”); a seguito di tale comunicazione il Responsabile non sarà tenuto ad osservare l’Istruzione Contestata. Se a seguito delle informazioni fornite dal Responsabile, il Titolare conferma l’Istruzione Contestata assumendosene la responsabilità, il Responsabile dovrà osservare l’Istruzione Contestata a meno che questa sia collegata (i) all’adozione di misure tecniche e organizzative; (ii) alla nomina di Sub-responsabili;
- k. prestare al Titolare ogni necessaria collaborazione nell’assolvimento di richieste che dovessero pervenire dal Garante o da altre autorità competenti o in relazione a procedure o ispezioni che dovessero essere avviate nei confronti del Titolare, dando altresì immediata esecuzione alle istruzioni ricevute e fornendo copia di ogni documento richiesto.
- l. mantenere e aggiornare il registro dei trattamenti ai sensi dell’art. 30 del GDPR;
- m. ove applicabile, mantenere e aggiornare la lista dei trasferimenti di dati personali verso paesi terzi (extra SEE) compresa l’identificazione del paese terzo e, per i trasferimenti di cui al secondo comma dell’articolo 49 del GDPR, la documentazione delle garanzie adeguate;
- n. ove applicabile, eseguire le Attività in conformità al principio di minimizzazione e privacy by design e by default di cui all’art. 25 del GDPR.

6. Restituzione e distruzione dei dati personali

- 6.1. È espressamente convenuto tra le Parti che alla data di cessazione del presente Accordo il Responsabile procederà alla restituzione e/o alla cancellazione/distruzione dei Dati personali trattati nell’ambito del presente Accordo, dandone tempestiva conferma al Titolare, nonché ogni copia degli stessi sia digitale sia cartacea. In caso di cancellazione, il Titolare si riserva di chiedere una certificazione di cancellazione al Responsabile.
- 6.2. Il Responsabile, inoltre, si impegna ad imporre ai propri Sub-responsabili autorizzati l’obbligo di cancellare e/o distruggere qualsiasi Dato personale trattato in considerazione dell’Attività prestata a favore del Titolare stesso.

7. Sicurezza dei dati

7.1. Il Titolare, con l'assistenza del Responsabile, ha individuato la lista di misure di sicurezza tecniche e organizzative adeguate descritta nell'Annex C del presente Accordo, che il Responsabile si impegna a mantenere in essere per tutta la durata dello stesso Accordo, al fine di prevenire, o quantomeno minimizzare, ogni rischio ragionevolmente prevedibile connesso alla distruzione, alla perdita, alla modifica, alla divulgazione non autorizzata o all'accesso, in modo accidentale o illegale, ai dati ricevuti. Il Responsabile si impegna quindi ad adottare misure di sicurezza conformi a quanto disposto all'art. 32 del Regolamento e, più in generale, dalla Legge applicabile, dalla disciplina di settore e dalla *best practice* in materia.

In ogni caso, le misure di sicurezza includono almeno le seguenti:

- la capacità di assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi utilizzati per il trattamento dei Dati personali;
- la capacità di ripristinare la disponibilità e l'accesso ai Dati personali qualora si verifici un incidente tecnico oppure fisico, come a titolo esemplificativo ma non esaustivo, in caso di *Data Breach*;
- un processo per condurre un test regolare di valutazione circa l'effettività delle misure tecniche e organizzative per assicurare la sicurezza del trattamento dei Dati personali;
- la garanzia in riferimento alle qualità e gli obblighi delle persone autorizzate, da parte del Responsabile, al trattamento dei Dati personali, in particolare:
 - sono vincolati agli obblighi di riservatezza e non permettono ad alcun soggetto che non sia vincolato ai medesimi obblighi di trattare i Dati personali;
 - abbiano ricevuto una formazione specifica in merito alla protezione, alla tutela e alla custodia dei Dati personali.

7.2. Restano ferme in ogni caso le eventuali ulteriori misure di sicurezza che il Titolare con l'assistenza del Responsabile dovesse ritenere adeguate ovvero chiedesse di adottare in relazione a specifiche Operazioni del trattamento.

8. Audit

8.1. Il Responsabile si impegna a fornire al Titolare, su richiesta, relazioni e report che attestino l'adempimento degli obblighi gravanti sul Responsabile stesso ai sensi del presente Accordo, tra cui, a titolo esemplificativo, riguardo alle misure di sicurezza adottate.

8.2. Il Responsabile si impegna a consentire al Titolare o a soggetti terzi da questo delegati, con modalità e tempi da concordarsi, l'accesso ad uffici, dispositivi, sistemi e documenti informatici propri e dei propri subappaltatori, qualora risulti necessario per verificare l'osservanza, da parte del Responsabile, degli obblighi pattuiti.

9. Riservatezza

- 9.1. Senza recare alcun pregiudizio a qualsivoglia rapporto esistente tra le Parti, ulteriore rispetto il presente Accordo, il Responsabile tratta i Dati Personali in modo strettamente confidenziale e si impegna a informare i propri dipendenti, agenti e/o sub-fornitori coinvolti nelle attività di trattamento dei Dati personali circa la natura riservata di detti dati. Il Responsabile assicura altresì che i soggetti suindicati abbiano appositamente firmato un accordo di riservatezza, siano tenuti all'osservanza di obblighi di riservatezza, ovvero siano assoggettati a un'apposita clausola statutaria di riservatezza.

10. Responsabilità e manleve

- 10.1. Il Responsabile tiene indenne e manlevato il Titolare da ogni perdita, costo, spesa, multa e/o sanzione, danno e da ogni responsabilità di qualsiasi natura derivante o in connessione con una qualsiasi violazione da parte del Responsabile stesso delle disposizioni in materia di protezione dei dati personali contenute nel presente Accordo.

11. Durata

- 11.1. L'Accordo produrrà i suoi effetti a partire dalla data della sua sottoscrizione (la "Data") e rimarrà in vigore sino alla data di cessazione del rapporto con il Titolare.

12. Legge applicabile e Foro competente

- 12.1. Il presente Accordo è regolato dalla legge italiana.
- 12.2. Tutte le controversie derivanti dal presente Accordo, comprese quelle relative alla sua validità, interpretazione, esecuzione e risoluzione, che dovessero insorgere tra le Parti saranno deferite in via esclusiva alla competenza del Foro di Roma.

Per la CAMERA DI COMMERCIO, INDUSTRIA,
ARTIGIANATO E AGRICOLTURA DI FOGGIA
il Segretario Generale
dott.ssa Lorella Palladino

Per UNIONCAMERE
il Segretario Generale
dott. Giuseppe Tripoli

ANNEX A – Descrizione Operazioni di trattamento – CRM di sistema

<p>Categorie di Soggetti Interessati</p> <p>Specificare le categorie di Soggetti Interessati i cui Dati Personali verranno trattati dal Fornitore</p>	<ul style="list-style-type: none"> ● Dati relativi alle imprese e ai rappresentanti legali ● Dati relativi a professionisti/imprenditori o aspiranti imprenditori ● Dati relativi agli studenti ● Dati relativi a persone che cercano impiego ● Dati dipendenti di PA
<p>Categorie di Dati</p> <p>Specificare i Dati Personali che verranno trattati dal Fornitore</p>	<ul style="list-style-type: none"> ● Dati identificativi ● Dati di contatto ● Dati di autenticazione
<p>Operazioni di trattamento</p> <p>Specificare tutte le attività di trattamento che verranno condotte dal Fornitore</p>	<ul style="list-style-type: none"> ● Raccolta; ● Elaborazione; ● Registrazione; ● Uso; ● Consultazione; ● Estrazione.
<p>Luogo delle Operazioni di trattamento</p> <p>Specificare tutti i luoghi dove i Dati Personali verranno trattati dal Fornitore</p>	<p>Italia</p>
<p>Finalità</p> <p>Specificare tutti gli scopi per i quali i Dati Personali verranno trattati dal Fornitore per conto del Titolare</p>	<ul style="list-style-type: none"> ● Erogazione del CRM evoluto e dei relativi servizi integrato con il sito della CCIAA a favore delle categorie degli interessati coinvolti, tra cui, in particolare, la promozione degli eventi e/o di altri incontri; ● Promozione degli eventi organizzati dalla CCIAA, anche nei confronti delle altre Camere di Commercio, svolgendo il ruolo di filtro; ● Gestione iniziative ed erogazione di servizi a supporto della competitività delle imprese (tra cui, organizzazione di seminari, convegni, iniziative di

	<p>informazione e formazione, assistenza tecnica collettiva ed individuale, servizi di orientamento, servizi di <i>auto-assessment</i> etc);</p> <ul style="list-style-type: none"> ● Monitoraggio e filtro di campagne di comunicazione organizzate da Enti del Sistema Camerale di interesse territoriale allargato, per conto e nell'interesse della Camera; ● Analisi dei dati relativi alle categorie degli interessati, con l'utilizzo, anche, di sistemi di Intelligenza Artificiale anche predittivi; ● Monitoraggio e produzione di Reportistica aggregata relativa al monitoraggio su tutto il territorio degli eventi e delle attività svolte da parte di tutte le CCIAA.
<p>Durata Specificare il periodo di tempo nel quale le attività di trattamento verranno eseguite</p>	<p>Per tutto il tempo dello svolgimento delle attività, fino alla cessazione del conferimento delle Attività nei confronti del Fornitore.</p>
<p>Periodo di Conservazione Specificare il periodo di conservazione per ogni categoria di dati e la ragione della loro conservazione</p>	<p>In seguito alla cessazione del rapporto con il Fornitore, quest'ultimo dovrà restituire i dati personali trattati per conto del Titolare del trattamento.</p>
<p>Trasferimento al di fuori dell'EEA Se il Fornitore è al di fuori dell'EEA, specificare il meccanismo di adeguatezza utilizzato per garantire che il trasferimento dei Dati sia lecito</p>	<p>N/A</p>

ANNEX B - Sub-appaltatori autorizzati

Identificazione dei sub-appaltatori Inserire i dettagli dei Sub-appaltatori autorizzati e dei loro sub-incaricati: <i>Nome completo, Codice Fiscale e p.IVA, indirizzo dell'Ufficio, nome del loro Data Protection Officer, dettagli del loro Rappresentante (se presente)</i>	Scopi Specificare gli scopi per i quali i Dati Personali verranno trattati dal Sub-appaltatore e autorizzato	Operazioni di trattamento Specificare tutte le operazioni di trattamento che il Sub-appaltatore autorizzato effettuerà (inclusi i Soggetti interessati e le categorie di Dati Personali, se differenti rispetto al Fornitore)	Luoghi delle Operazioni di trattamento Specificare i luoghi presso i quali le attività di trattamento verranno effettuate dal Sub-appaltatore autorizzato	Trasferimento al di fuori dell'EEA Se il Sub-appaltatore autorizzato risiede al di fuori dell'EEA, specificare il meccanismo di adeguatezza utilizzato per garantire che il trasferimento dei Dati sia lecito
Business Integration Partners S.p.A. (BIP)	Configurazione e gestione della piattaforma di CRM di Sistema Sviluppo tecnico delle funzionalità tecniche e operative del CRM di sistema e relativa erogazione dei servizi afferenti il CRM di sistema; Servizi di assistenza e manutenzione)	Raccolta, gestione e conservazione dei dati personali delle imprese, imprenditori, studenti, aspiranti imprenditori, tra cui i dati identificativi e di contatto, di titolarità delle Camere di Commercio	Italia	N/A
Euroforce	Coordinamento con per comprendere esigenze e	Raccolta, gestione e conservazione dei dati personali	Italia	N/A

	<p>definire requisiti evolutivi del CRM, assicurando che sussista l'adeguato supporto per l'adempimento degli obiettivi dello stesso.</p> <p>Gestione campagne centralizzate e formazione agli utenti che utilizzano il CRM, nonché coordinamento con eventuali ulteriori fornitori per personalizzazione delle campagne (ove applicabile).</p> <p>Ottimizzazione dei processi con analisi dati e proposizione di innovazioni strategiche per migliorare l'efficienza anche organizzativa dei sistemi.</p>	<p>delle imprese, imprenditori, studenti, aspiranti imprenditori, tra cui i dati identificativi e di contatto, di titolarità delle Camere di Commercio</p>		
--	--	--	--	--

ANNEX C MISURE DI SICUREZZA

Il presente Annex C riporta le misure di sicurezza implementate dal Fornitore, a seguito del rispetto del Regolamento generale sulla protezione dei dati (UE) 2016/679, su tutti gli ambiti fisici, organizzativi, infrastrutturali e applicativi che sottendono ai trattamenti dei dati personali.

Tali misure sono implementate attraverso policy, procedure, formazione al personale, tool di gestione e monitoraggio.

Di seguito l'elenco di misure di sicurezza applicate ai trattamenti:

1. Salesforce CRM Core:

- Autenticazione a più fattori;
- Password Policy;
- Device activation;
- Protezione della sessione (es.: time-out predefiniti);
- Gestione dei permessi degli utenti;
- Controllo degli accessi agli oggetti;
- Impostazione dei profili;
- Set di privilegi;
- Ruoli;
- Regole di condivisione;
- Monitoraggio dello storico dei log;
- Monitoraggio dello storico dei campi;
- Abilitazione dell'Audit Trail
- Monitoraggio degli eventi in tempo reale.

2. Marketing Cloud Engagement:

- Impostazioni di sessione;
- Credenziali di accesso;

- Autenticazione a più fattori;
- Password Policy;
- Impostazioni per l'esportazione dei dati;
- Sicurezza della connessione;
- Eredità delle impostazioni di sicurezza di Enterprise e Agency
- Audit Trial