Accordo sul Trattamento dei Dati Personali

ai sensi dell'art. 28 del Regolamento (UE) 2016/679 (GDPR)

Allegato al Contratto di Fornitura 4cAi X

PARTE I – IDENTIFICAZIONE DELLE PARTI E PREMESSE

Articolo 1 – Identificazione delle Parti

Il presente Data Processing Agreement (di seguito "DPA" o "Accordo") è stipulato tra:

TITOLARE DEL TRATTAMENTO	Il Cliente, così come identificato nel Modulo d'Ordine allegato al Contratto principale (di seguito "Cliente" o "Titolare").
RESPONSABILE DEL TRATTAMENTO	**4cAi S.r.l.** Sede legale: Via Visconti di Modrone 2, 20122 Milano Sede operativa: Largo La Foppa 1, 20121 Milano P.IVA e C.F.: 11799250961 *Società soggetta a direzione e coordinamento di 4c S.r.l.* Di seguito: "4cAi" o "Responsabile".

Articolo 2 – Premesse e Natura del DPA

2.1. Il presente DPA costituisce parte integrante e sostanziale del Contratto di Fornitura dei Servizi 4cAi X (di seguito "Contratto") e disciplina il trattamento dei dati personali effettuato da 4cAi per conto del Cliente nell'ambito dell'erogazione dei Servizi tramite la Piattaforma 4cAi X.

2.2. In conformità all'art. 28(3) del Regolamento (UE) 2016/679 ("GDPR"), il presente Accordo definisce l'oggetto, la natura, le finalità e la durata del trattamento, il tipo di dati personali e le categorie di interessati, nonché gli obblighi e i diritti del Titolare.

2.3. Nell'ambito dell'esecuzione del Contratto, il Cliente agisce in qualità di Titolare del trattamento e 4cAi agisce in qualità di Responsabile del trattamento ai sensi dell'art. 28 GDPR.

PARTE II – OGGETTO DEL TRATTAMENTO E ISTRUZIONI DEL TITOLARE

Articolo 3 – Istruzioni del Titolare e Finalità del Trattamento

3.1. 4cAi tratta i dati personali esclusivamente per conto del Cliente e sulla base delle istruzioni documentate contenute nel presente DPA e nel Contratto.

3.2. Le finalità del trattamento effettuato da 4cAi per conto del Cliente sono le seguenti e unicamente le seguenti:

- consentire l'accesso e l'utilizzo della Piattaforma 4cAi X agli Utenti autorizzati dal Cliente;

- elaborare gli Input forniti dal Cliente e generare i relativi Output nell'ambito delle funzionalità AI della Piattaforma;
- garantire il funzionamento tecnico, la sicurezza, la continuità operativa e la manutenzione e il miglioramento della piattaforma SaaS 4cAi X e del servizio ad essa associato, nel rispetto dell'art. 3.4.

3.3. Qualora 4cAi ritenga che un'istruzione del Cliente violi il GDPR o altra normativa applicabile in materia di protezione dei dati, ne informa prontamente il Cliente ai sensi dell'art. 28(3)(h) GDPR, senza essere tuttavia obbligata a sospendere il trattamento in attesa di istruzioni aggiornate, salvo che ciò sia strettamente necessario per evitare una violazione grave.

3.4. 4cAi non utilizzerà i dati personali del Cliente per addestrare, fine-tuning o migliorare i propri modelli di intelligenza artificiale o quelli di terzi, senza esplicita istruzione scritta del Cliente.

Articolo 4 – Oggetto del Trattamento: Dati, Categorie di Interessati e Durata

4.1. I dati personali oggetto di trattamento ai sensi del presente DPA possono includere le seguenti categorie:

- Dati identificativi (es. nome, cognome, codice fiscale/partita IVA ove contenuti negli Input)
- Dati di contatto (es. indirizzo email professionale, numero di telefono)
- Dati professionali (es. qualifica, ruolo, studio di appartenenza, dossier e documenti giuridici caricati in Piattaforma)
- Log tecnici (IP, user-agent, eventi API)
- Contenuto immesso nei prompt e output forniti/ritornati dal servizio
- Eventuali categorie particolari di dati personali (art. 9 GDPR) e dati relativi a condanne penali e reati (art. 10 GDPR) contenuti negli Input caricati dal Cliente

4.2. Le categorie di interessati il cui trattamento può essere effettuato includono: dipendenti, collaboratori, consulenti, professionisti, assistiti, clienti e controparti del Cliente, nonché ogni altro soggetto i cui dati siano contenuti negli Input caricati sulla Piattaforma.

4.3. In considerazione della natura professionale dei Servizi, l'utilizzo della Piattaforma può comportare il trattamento di categorie particolari di dati personali (art. 9 GDPR) e di dati relativi a condanne penali e reati (art. 10 GDPR). In tal caso:

a. il Cliente, in qualità di Titolare, garantisce di disporre di idonea base giuridica e dei presupposti di liceità previsti dagli artt. 9 e 10 GDPR e dalla normativa nazionale applicabile, incluso l'art. 2-octies del D.Lgs. 196/2003, e resta responsabile della valutazione circa la necessità di una valutazione d'impatto ai sensi dell'art. 35 GDPR;
b. il caricamento di tali dati sulla Piattaforma costituisce istruzione documentata del Cliente a 4cAi a trattarli esclusivamente per le finalità di cui all'art. 3.2;
c. 4cAi applica a tali dati le misure tecniche e organizzative di cui all'art. 5, proporzionate al rischio connesso alla natura di tali categorie di dati, e fornisce al Cliente l'assistenza prevista dall'art. 9.1;
d. il Cliente non è tenuto ad anonimizzare o pseudonimizzare preventivamente i documenti caricati. Resta inteso che la Piattaforma non effettua in via automatica tali operazioni e che il Cliente, quale Titolare, valuta la pertinenza delle informazioni caricate nel rispetto dell'art. 5(1)(c) GDPR.

4.4. Il trattamento dei dati è effettuato per la durata del Contratto. Alla cessazione del rapporto contrattuale, i dati personali sono trattati ai sensi del successivo Articolo 11. I dati relativi al periodo di prova (Trial) sono conservati per un periodo massimo di 60 (sessanta) giorni in caso di mancata conversione a pagamento.

PARTE III – OBBLIGHI DI 4cAi IN QUALITÀ DI RESPONSABILE

Articolo 5 – Misure di Sicurezza Tecniche e Organizzative

5.1. 4cAi adotta misure tecniche e organizzative adeguate a garantire un livello di sicurezza proporzionato al rischio, tenendo conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, conformemente all'art. 32 GDPR.

5.2. Le misure di sicurezza implementate da 4cAi comprendono, a titolo non esaustivo:

Area	Misura	Riferimento
Riservatezza	Cifratura dei dati in transito (TLS 1.2+) e a riposo (AES-256)	Art. 32(1)(a) GDPR; ISO 27001 A.8.24
Integrità	Logging, audit trail, controlli di integrità	Art. 32(1)(b) GDPR; ISO 27001 A.8.15
Disponibilità	Architettura ridondante, backup regolari, piano BCP/DR	Art. 32(1)(b) GDPR; ISO 27001 A.8.14
Accesso	Autenticazione forte (MFA), RBAC, principio del least privilege	Art. 32(1)(b) GDPR; ISO 27001 A.5.15
Vulnerabilità	Patch management, vulnerability scanning	Art. 32(1)(d) GDPR; ISO 27001 A.8.8
Personale	Formazione privacy e sicurezza; accordi di riservatezza	Art. 32(4) GDPR; ISO 27001 A.6.3
Test e resilienza	Test periodici di ripristino, penetration test annuale	Art. 32(1)(d) GDPR; ISO 27001 A.8.29

5.3. Le misure descritte riflettono lo stato dell'arte alla data di sottoscrizione del presente DPA. 4cAi si impegna a riesaminare e aggiornare periodicamente tali misure, garantendo che il livello di protezione assicurato non sia mai inferiore a quello qui definito. Nella definizione e nel riesame delle misure di sicurezza, 4cAi tiene conto dello stato dell'arte, dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà delle persone fisiche, in conformità all'art. 32(1) GDPR.

5.4. In conformità all'art. 32(4) GDPR, 4cAi assicura che le persone fisiche autorizzate al trattamento dei dati personali abbiano assunto un impegno di riservatezza o siano soggette a un obbligo legale di riservatezza. Le persone autorizzate al trattamento ricevono adeguata formazione in materia di protezione dei dati personali.

5.5. Fatte salve le operazioni tecniche automatizzate strettamente necessarie all'erogazione del Servizio, né 4cAi né i suoi sub-responsabili accedono, consultano o utilizzano documenti, conversazioni (prompt e Output) o altri Contenuti del Cliente (come definiti nel Contratto), salvo: (i) richiesta o autorizzazione scritta del Cliente riferita a una specifica attività; (ii) invio volontario di un feedback da parte dell'Utente, nei limiti di cui all'art. 5.6; (iii) gestione di incidenti di sicurezza o adempimento di obblighi di legge o provvedimenti dell'Autorità, nei limiti strettamente necessari e con comunicazione al

Cliente ove consentito. L'accesso è riservato a personale autorizzato ai sensi dell'art. 29 GDPR e dell'art. 2-quaterdecies D.Lgs. 196/2003, vincolato alla riservatezza, ed è tracciato.

5.6. La Piattaforma consente all'Utente di inviare, su base volontaria, feedback qualitativi sugli Output generati. L'invio del feedback consente al personale autorizzato di 4cAi di consultare la sola conversazione cui il feedback si riferisce, comprensiva di prompt, Output ed eventuali canvas generati nella stessa, al solo fine di verificare e migliorare la qualità del Servizio e nel rispetto dell'art. 3.4. In nessun caso l'invio del feedback consente l'accesso ai documenti caricati dall'Utente. Il Cliente si impegna a informare gli Utenti autorizzati di tale funzionamento; resta in ogni caso nella facoltà dell'Utente non inviare feedback.

Articolo 6 – Sub-Responsabili del Trattamento

6.1. Autorizzazione generale. Il Cliente autorizza 4cAi a nominare sub-responsabili del trattamento per attività necessarie all'erogazione dei Servizi, in conformità all'art. 28(2) GDPR. 4cAi garantisce che i sub-responsabili siano vincolati da obblighi di protezione dei dati non inferiori a quelli previsti nel presente DPA, mediante la sottoscrizione di specifici accordi scritti. 4cAi informa il Cliente di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di sub-responsabili, anche mediante comunicazione e-mail o aggiornamento dell'elenco pubblicato, dando al Cliente l'opportunità di opporsi a tali modifiche ai sensi dell'art. 28(2) GDPR

6.2. 4cAi rimane pienamente responsabile nei confronti del Cliente per l'adempimento degli obblighi dei sub-responsabili qualora quest'ultimo non adempia ai propri obblighi in materia di protezione dei dati, ai sensi dell'art. 28(4) GDPR.

6.3. 4cAi mantiene un elenco aggiornato dei sub-responsabili attualmente nominati, disponibile su richiesta scritta del Cliente.

Articolo 7 – Trasferimenti di Dati verso Paesi Terzi

7.1. L'infrastruttura della Piattaforma 4cAi X è ospitata su data center di Amazon Web Services (AWS) localizzati nell'Unione Europea. Le funzionalità di intelligenza artificiale sono erogate tramite servizi di modelli linguistici resi disponibili da fornitori cloud con elaborazione all'interno dell'Unione Europea.

7.2. 4cAi non trasferisce i dati personali del Cliente verso Paesi terzi o organizzazioni internazionali al di fuori dello Spazio Economico Europeo (SEE) se non in presenza di almeno uno dei seguenti presupposti, conformemente al Capo V del GDPR:

- decisione di adeguatezza della Commissione Europea ex art. 45 GDPR;
- garanzie adeguate ai sensi dell'art. 46 GDPR (in particolare: Clausole Contrattuali Standard – SCC – adottate dalla Commissione Europea; Binding Corporate Rules);
- misure tecniche supplementari ove richiesto dalla valutazione d'impatto sul trasferimento (Transfer Impact Assessment – TIA).

Articolo 8 – Supporto al Titolare nell'Esercizio dei Diritti degli Interessati

8.1. 4cAi assiste il Cliente, nei limiti di quanto ragionevolmente possibile e tenuto conto della natura del trattamento, nell'adempimento degli obblighi derivanti dall'esercizio dei diritti degli interessati ai sensi degli artt. 15-22 GDPR (diritto di accesso, rettifica, cancellazione, limitazione, portabilità, opposizione; diritti relativi alle decisioni automatizzate).

8.2. Qualora 4cAi riceva una richiesta direttamente da un interessato, ne dà tempestiva comunicazione al Cliente senza ingiustificato ritardo, astendendosi dal rispondere alla richiesta salvo esplicita istruzione scritta del Cliente, nei limiti consentiti dalla legge.

8.3. Relativamente ai trattamenti effettuati mediante funzionalità di intelligenza artificiale agentica ai sensi del Regolamento (UE) 2024/1689 (AI Act) e dell'art. 22 GDPR, 4cAi fornirà al Cliente, su richiesta e nella misura in cui tale adempimento sia tecnicamente possibile, le informazioni necessarie a garantire trasparenza e a facilitare l'esercizio dei diritti degli interessati, incluse informazioni sulla logica sottostante i processi automatizzati che producono Output significativi, nei limiti di quanto consentito dalla tutela della proprietà intellettuale e del segreto industriale.

Articolo 9 – Supporto al Titolare nella Compliance GDPR (DPIA, Data Breach, Registri)

9.1. Supporto DPIA. 4cAi assiste il Cliente, tenuto conto della natura del trattamento e delle informazioni a propria disposizione, nell'adempimento degli obblighi derivanti dalla valutazione d'impatto sulla protezione dei dati (DPIA) prevista dall'art. 35 GDPR, ove applicabile.

9.2. Notifica violazioni dei dati personali (Data Breach). 4cAi si impegna a:

- notificare al Cliente senza ingiustificato ritardo qualsiasi violazione dei dati personali ai sensi dell'art. 4(12) GDPR;
- fornire al Cliente tutte le informazioni di cui all'art. 33(3) GDPR necessarie per l'eventuale notifica all'Autorità Garante competente, da effettuarsi entro 72 ore dalla scoperta;
- collaborare con il Cliente per contenere, analizzare e rimediare alla violazione;
- documentare le violazioni avvenute con tutte le informazioni pertinenti, in conformità all'art. 33(5) GDPR.

9.3. Registro delle attività di trattamento. 4cAi mantiene un registro delle categorie di attività di trattamento svolte per conto del Cliente ai sensi dell'art. 30(2) GDPR e ne fornisce copia al Cliente e/o all'Autorità di controllo su richiesta.

Articolo 10 – Audit e Verifica della Conformità

10.1. 4cAi mette a disposizione del Cliente tutte le informazioni necessarie a dimostrare il rispetto degli obblighi del presente DPA e contribuisce alle attività di revisione, comprese le ispezioni, effettuate dal Cliente o da un revisore da questo incaricato, ai sensi dell'art. 28(3)(h) GDPR.

10.2. Le richieste di audit devono essere effettuate con un preavviso scritto di almeno 30 (trenta) giorni, devono essere ragionevoli nella portata e nella frequenza (non più di una volta per anno solare, salvo legittimo motivo), e non devono compromettere la sicurezza dei sistemi o la riservatezza dei dati di altri clienti di 4cAi.

10.3. In alternativa o in aggiunta all'audit diretto, 4cAi potrà fornire al Cliente la documentazione pertinente attestante la conformità ai requisiti del presente DPA.

10.4. I costi dell'audit sono a carico del Cliente, salvo che l'audit rilevi un inadempimento materiale di 4cAi agli obblighi del presente DPA.

PARTE IV – CESSAZIONE DEL CONTRATTO E CANCELLAZIONE DEI DATI

Articolo 11 – Restituzione e Cancellazione dei Dati alla Cessazione

11.1. Alla cessazione del Contratto, per qualsiasi causa, 4cAi provvede, su richiesta scritta del Cliente da formularsi entro 30 (trenta) giorni dalla cessazione:

- alla restituzione al Cliente di tutti i dati personali trattati per suo conto, su supporto digitale in formato interoperabile, entro un termine ragionevole e comunque non superiore a 30 (trenta) giorni dalla richiesta; oppure
- alla cancellazione sicura e definitiva di tutti i dati personali dai sistemi di 4cAi, con distruzione delle copie esistenti incluse quelle di backup, previa attestazione scritta.

11.2. In assenza di istruzione scritta del Cliente entro il termine di cui al comma 11.1, 4cAi provvede alla cancellazione sicura dei dati entro 60 (sessanta) giorni dalla cessazione del rapporto contrattuale.

11.3. Resta salva la facoltà di 4cAi di conservare i dati per il periodo e nei limiti strettamente necessari al rispetto di obblighi di legge applicabili (es. obblighi fiscali, contabili, normativi), previa comunicazione scritta al Cliente.

11.4. I dati relativi al Trial sono conservati per un periodo massimo di 60 giorni in caso di mancata conversione a Piano di Abbonamento a pagamento, trascorsi i quali vengono cancellati in modo sicuro.

PARTE V – DISPOSIZIONI FINALI

Articolo 12 – Gerarchia Documentale e Prevalenza

12.1. In caso di conflitto tra le disposizioni del presente DPA e quelle del Contratto principale, prevalgono le disposizioni del presente DPA in materia di protezione dei dati personali. Qualora le Parti abbiano sottoscritto o sottoscrivano un Data Processing Agreement negoziato ad hoc in forma scritta, quest'ultimo prevarrà sul presente DPA limitatamente alle materie in esso disciplinate, fermo restando che le disposizioni del presente DPA continuano ad applicarsi per tutto quanto non espressamente derogato.

12.2. Il presente DPA è parte integrante del Contratto e non può essere interpretato separatamente dallo stesso.

Articolo 13 – Legge Applicabile e Foro Competente

13.1. Il presente DPA è regolato dal diritto italiano e dal diritto dell'Unione Europea in materia di protezione dei dati personali.

13.2. Per qualsiasi controversia relativa al presente DPA è competente in via esclusiva il Foro di Milano.

Articolo 14 – Accettazione del DPA

14.1. La registrazione al servizio 4cAi X costituisce firma elettronica ai sensi dell'art. 28 §3 GDPR.

14.2. Qualora il Cliente desideri sottoscrivere il presente DPA in forma scritta, potrà farne richiesta a 4cAi all'indirizzo privacy@4cportal.ai.