DATA PROCESSING ADDENDUM – DPA MASTER DI GRUPPO ARTSER

(22.01.26 versione 1.0)

Il presente Data Processing Addendum ("DPA") disciplina i trattamenti di dati personali effettuati per conto del Cliente nell'esecuzione dei servizi oggetto del contratto principale (il "Contratto"), ai sensi dell'art. 28 del Regolamento (UE) 2016/679 ("GDPR").

Il DPA è parte integrante del Contratto; in caso di contrasto, per i profili privacy prevale il DPA.

L'"Allegato A – Catalogo dei servizi – trattamenti" costituisce parte integrante del DPA e riporta, per ciascun Servizio, gli elementi di specificità richiesti dall'art. 28(3) GDPR (natura e scopo, durata, categorie di interessati, tipologie di dati, categorie di operazioni, nonché sistemi/applicativi e istruzioni specifiche del Cliente).

Premesse

(a) L'esecuzione dei servizi di cui al Contratto (i "Servizi") comporta trattamenti di dati personali per conto del Cliente e su istruzione di quest'ultimo, ai sensi dell'art. 4(8) GDPR.

(b) Il presente DPA disciplina tali trattamenti ai sensi dell'art. 28 GDPR.

(c) Ai fini del DPA, per "Società del Gruppo Artser" si intendono Artser S.r.l. e le altre società elencate nell'Elenco Società di Gruppo (Allegato B), ciascuna limitatamente ai Servizi di propria competenza. Artser S.r.l. agisce in qualità di Lead Processor per il coordinamento privacy (notifiche, gestione sub-responsabili, gestione incidenti), su mandato espresso delle Società del Gruppo ferme restando le responsabilità delle singole società per i rispettivi trattamenti.

(d) Il Cliente nomina quale Responsabile del trattamento la specifica Società del Gruppo così indicata nell'Elenco Società di Gruppo con la quale ha sottoscritto il Contratto.

1. Oggetto, ruoli e perimetro

1.1 In esecuzione del Contratto, il Cliente nomina, ai sensi dell'art. 28 GDPR, quale Responsabile del trattamento la Società del Gruppo Artser con la quale ha sottoscritto il Contratto (di seguito, "Responsabile di Gruppo") per l'erogazione dei Servizi. Il presente DPA e i suoi allegati ne costituiscono parte integrante.

1.2 Le Società del Gruppo operano ciascuna per conto del Cliente nel rispetto delle istruzioni da questi ricevute e di quanto descritto nel Catalogo trattamenti/Servizi (Allegato A).

2. Istruzioni del Cliente

2.1 Il Responsabile di Gruppo tratta i dati personali esclusivamente su istruzioni documentate del Cliente, salvo che sia tenuto a farlo in forza del diritto dell'Unione o degli Stati membri.
2.2 È vietato ogni riutilizzo dei dati per finalità proprie o di terzi. Restano distinti e autonomi i trattamenti svolti dal Responsabile di Gruppo in qualità di titolare del trattamento per adempimenti propri (es. obblighi di legge quali contabilità, antiriciclaggio).
2.3 La Società del Gruppo nominata Responsabile informa immediatamente il Cliente qualora, a suo avviso, una sua istruzione infranga il GDPR o altre disposizioni italiane in materia di protezione dei dati. Artser S.r.l., in qualità di Lead Processor, coordina le comunicazioni, senza che ciò esoneri la Società nominata dagli obblighi di cui al presente articolo. In caso di istruzioni manifestamente non conformi alla normativa applicabile, il Responsabile potrà rifiutare la relativa esecuzione o recedere dal solo Servizio interessato, senza penali, fermo il diritto al corrispettivo secondo quanto previsto dal Contratto.

3. Specificità per Servizio (art. 28(3) GDPR)

3.1. Per ogni Servizio, l'Allegato A indica almeno: natura e scopo del trattamento, durata, tipologie di dati, categorie di interessati, categorie di operazioni, nonché le istruzioni tipiche di servizio, presenza di sub-responsabili.
3.2. L'Allegato A ha natura dinamica e può essere aggiornato in funzione delle esigenze dei Servizi. Il Cliente è tenuto a verificare periodicamente l'Allegato A in relazione ai Servizi attivi ai sensi del Contratto.

4. Personale autorizzato e riservatezza

4.1. Il Responsabile di Gruppo assicura che chiunque tratti dati personali sotto la propria autorità (dipendenti o collaboratori) sia espressamente designato come persona autorizzata al trattamento (incaricato) e operi esclusivamente su istruzioni documentate del Cliente e del Responsabile, ai sensi degli artt. 29 e 32(4) GDPR.
4.2. Le persone autorizzate sono vincolate da obblighi di riservatezza adeguati, che permangono anche dopo la cessazione dell'incarico. Il Responsabile di Gruppo conserva evidenze della sottoscrizione degli impegni di riservatezza.
4.3. Il Responsabile di Gruppo eroga formazione iniziale e periodica in materia di protezione dei dati personali, sicurezza delle informazioni e gestione degli incidenti, calibrata sui ruoli e sulla base di specifici KPI che l'azienda si prefigge di raggiungere.
4.4. L'accesso ai dati personali è limitato alle sole persone autorizzate per quanto strettamente necessario allo svolgimento delle attività assegnate (principio del "need-to-know"), con adeguata separazione dei compiti e profilazione coerente delle abilitazioni.
4.5. Le persone autorizzate utilizzano credenziali individuali; sono adottati meccanismi di autenticazione robusta (ove applicabile, MFA), politiche di password, revoca immediata

degli accessi in caso di cambio mansione o cessazione del rapporto e revisioni periodiche delle autorizzazioni. Gli accessi rilevanti sono loggati e monitorati nel rispetto della normativa applicabile in materia di riservatezza e controlli a distanza.

4.6. Le persone autorizzate sottoscrivono le policy aziendali interne del Responsabile di Gruppo. Le violazioni sono soggette a misure disciplinari proporzionate.

4.7. 4.7 Le persone autorizzate sono istruite e tenute a segnalare tempestivamente al Responsabile di Gruppo ogni evento di sicurezza o sospetta violazione dei dati personali, secondo la procedura di segnalazione dei data breach di Gruppo.

4.8. Ove le attività richiedano l'intervento o l'accesso di terzi, il Responsabile di Gruppo garantisce che tali soggetti operino come sub-responsabili ai sensi dell'art. 28(4) GDPR oppure, se meri manutentori senza accesso ai dati, sotto accordi di riservatezza e controlli tecnici che impediscano l'accesso ai dati personali.

4.9. Il Responsabile di Gruppo mantiene evidenze delle nomine a persone autorizzate, dei programmi formativi, delle policy accettate, delle revisioni degli accessi e mette a disposizione del Cliente estratti pertinenti su richiesta, anche ai fini di audit.

5. Sicurezza del trattamento

5.1. Il Responsabile di Gruppo adotta misure tecniche e organizzative adeguate ai rischi, ai sensi dell'art. 32 GDPR. Tali misure comprendono almeno:

- misure organizzative, quali policy interne in materia di protezione dei dati e sicurezza delle informazioni, nomine e istruzioni alle persone autorizzate, programmi di formazione, procedure per la gestione degli incidenti e dei data breach, gestione dei fornitori e dei sub-responsabili;
- misure fisiche, quali il controllo degli accessi ai locali, la protezione degli archivi cartacei, l'adozione di regole di "clean desk" e la protezione delle postazioni di lavoro da accessi non autorizzati;
- misure logiche/IT, quali la gestione delle identità e delle abilitazioni, l'uso di credenziali individuali e, ove applicabile, di meccanismi di autenticazione forte, politiche di password, logging e monitoraggio degli accessi rilevanti, soluzioni di protezione endpoint, procedure di backup e ripristino e gestione degli aggiornamenti di sicurezza;
- misure di continuità operativa e di disaster recovery, ove applicabili ai Servizi interessati, finalizzate ad assicurare la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.

5.2. Le misure di cui al presente articolo possono essere aggiornate e migliorate nel tempo, senza riduzione del livello di protezione dei dati personali. Il Responsabile di Gruppo mantiene documentazione interna di dettaglio delle misure adottate (policy, procedure, piani tecnici) e può metterne a disposizione del Cliente estratti pertinenti su richiesta, nei limiti strettamente necessari a dimostrare il rispetto del presente DPA e fermo restando il necessario bilanciamento con le esigenze di tutela della sicurezza e dei segreti aziendali.

6. Sub-responsabili (art. 28(2) e (4))

6.1. Il Cliente autorizza in via generale l'uso di sub-responsabili da parte del Responsabile di Gruppo ai sensi dell'art. 28(2) GDPR. L'elenco aggiornato dei sub-responsabili utilizzati per i Servizi è mantenuto dal Responsabile di Gruppo ed è messo a disposizione del Cliente su richiesta e/o secondo le modalità indicate nella documentazione di servizio o nel Contratto.

6.2. Il Lead Processor si obbliga a nominare e/o sostituire i Sub-Responsabili del trattamento esclusivamente con soggetti che garantiscano il pieno rispetto della normativa applicabile in materia di protezione dei dati personali (incluso il GDPR) e che adottino misure tecniche e organizzative, nonché un livello di protezione dei dati personali, almeno equivalenti a quelli previsti nel presente DPA.

6.3. Il Lead Processor informerà preventivamente per iscritto il Titolare del trattamento di qualsiasi prevista aggiunta o sostituzione di Sub-Responsabili, solo nelle ipotesi di modifiche rilevanti rispetto al precedente Sub-Responsabile da consentire al Titolare di effettuare le proprie valutazioni.

6.4. Il Responsabile di Gruppo, qualora si avvalga di sub-responsabili, si impegna a concludere con questi ultimi accordi di trattamento dei dati che garantiscano, anche mediante l'adesione a clausole o DPA standard predisposti dai relativi fornitori, un livello di protezione dei dati personali non inferiore, nel suo complesso, a quello previsto nel presente DPA. Resta ferma la responsabilità del Responsabile di Gruppo nei confronti del Cliente ai sensi dell'art. 28(4) GDPR.

7. Trasferimenti extra-SEE

7.1. Eventuali trasferimenti di dati personali verso Paesi terzi o organizzazioni internazionali, effettuati nell'ambito dei Servizi, sono effettuati nel rispetto del Capo V del GDPR e, in particolare, sulla base di decisioni di adeguatezza, clausole contrattuali tipo adottate dalla Commissione europea (SCC 2021/914), BCR o altri strumenti idonei, eventualmente integrati da misure supplementari.

Le informazioni sui Paesi di destinazione e sugli strumenti di trasferimento utilizzati sono mantenute dal Responsabile di Gruppo e messe a disposizione del Cliente su richiesta e/o secondo le modalità indicate nella documentazione di servizio o nel Contratto. In assenza di trasferimenti extra-SEE relativi ai Servizi, il Responsabile di Gruppo ne dà conferma al Cliente su richiesta.

8. Assistenza al Cliente

8.1. Tenendo conto della natura del trattamento e delle informazioni a disposizione, il Responsabile di Gruppo, con il supporto del Lead Processor, assiste il Cliente, nei limiti del perimetro affidato, per:
(a) la gestione delle richieste di esercizio dei diritti degli interessati (artt. 12–23 GDPR);
(b) gli adempimenti in materia di sicurezza del trattamento e gestione degli incidenti;

(c) le valutazioni relative ai trasferimenti extra-SEE e alle eventuali misure supplementari;
(d) ove pertinente, la predisposizione di DPIA e/o consultazioni preventive (art. 36 GDPR), limitatamente ai trattamenti oggetto del presente DPA.

Per rivolgersi al Lead Processor, il Cliente può scrivere all'indirizzo e-mail: data.protection@artser.it.

9. Violazioni dei dati personali

9.1. Il Lead Processor notifica al Cliente, per conto del Responsabile di Gruppo, senza ingiustificato ritardo e comunque entro 24 (ventiquattro) ore dalla scoperta, ogni violazione dei dati personali relativa ai Servizi, fornendo le informazioni di cui all'art. 33(3) GDPR, anche mediante aggiornamenti progressivi man mano che ulteriori dettagli divengano disponibili.

9.2. Resta inteso che la qualificazione finale della violazione ai sensi degli artt. 33 e 34 GDPR, così come la decisione in merito all'invio della notifica all'Autorità di controllo o della comunicazione agli interessati, compete esclusivamente al Titolare del trattamento. Il Lead Processor fornisce tutto il supporto necessario, ma non effettua alcuna comunicazione diretta.

10. Audit e verifiche

10.1. Il Responsabile di Gruppo mette a disposizione del Cliente, ove disponibili, attestazioni, certificazioni, report di audit di terze parti e altra documentazione idonea a dimostrare il rispetto degli obblighi derivanti dal presente DPA.

10.2. Il Responsabile di Gruppo consente altresì lo svolgimento di audit e ispezioni da parte del Cliente o di un terzo da questi incaricato, previo preavviso scritto di almeno 30 (trenta) giorni, durante il normale orario lavorativo e nel rispetto delle misure di sicurezza, nonché della tutela dei segreti industriali e commerciali, evitando per quanto possibile inutili duplicazioni di attività rispetto ad audit o verifiche già svolti.

10.3. 10.2 Salvo diversa previsione di legge o richiesta cogente di un'Autorità:
(a) tutti i costi diretti degli audit (ivi inclusi, a titolo esemplificativo, compensi e spese di consulenti esterni incaricati dal Cliente, costi di viaggio e soggiorno, ecc.) sono a carico esclusivo del Cliente;
(b) il costo delle risorse del Responsabile di Gruppo impiegate per supportare l'audit (tempo/uomo, attività di preparazione, assistenza durante le verifiche, ecc.) è a carico del Gruppo nei limiti della ordinaria tollerabilità, fermo restando che eventuali attività eccedenti tale limite potranno essere oggetto di specifica pattuizione tra le Parti.

11. Fine trattamento: restituzione e cancellazione

11.1. Salvo diverse istruzioni documentate del Cliente e fatti salvi eventuali obblighi di legge, alla cessazione del Servizio il Responsabile di Gruppo provvede, entro 90 (novanta)

giorni, alla restituzione e/o cancellazione di tutti i dati personali trattati per conto del Cliente. Su richiesta del Cliente, il Responsabile di Gruppo rilascia apposita attestazione dell'avvenuta cancellazione e/o restituzione. La restituzione dei dati personali avviene in un formato strutturato, di uso comune e leggibile da dispositivo automatico, salvo diverse istruzioni del Cliente.

11.2. Fermo restando quanto precede, qualora il Cliente richieda una conservazione ulteriore dei dati personali per adempiere a propri obblighi di legge (ad esempio, obblighi civilistici e fiscali di conservazione della documentazione contabile fino a 10 anni) o per esigenze di tutela o difesa dei propri diritti, il Responsabile di Gruppo potrà conservare tali dati per il periodo richiesto, e comunque non superiore ai termini di legge applicabili. I casi di conservazione ulteriore, i relativi termini (es. 10 anni) e le categorie di dati/Servizi interessati sono indicati nell'Allegato A.

12. Documentazione e registri

12.1. Il Lead Processor detiene il Registro dei trattamenti di Gruppo ai sensi dell'art. 30 GDPR e, su richiesta, mette a disposizione del Cliente gli estratti pertinenti relativi ai trattamenti oggetto del presente DPA.

12.2. Il Cliente mantiene e aggiorna il proprio registro dei trattamenti e le Istruzioni (Allegato A), assicurandone la coerenza con i trattamenti effettivamente affidati al Responsabile di Gruppo.

13. Aggiornamenti e prevalenza

13.1. Gli Allegati al presente DPA possono essere aggiornati con notifica al Cliente. Per le informazioni relative a sub-responsabili e trasferimenti extra-SEE si applicano le regole specifiche indicate agli artt. 6 e 7. Gli aggiornamenti producono effetto dalla data indicata nella comunicazione, salvo diverso termine ivi previsto.

13.2. In caso di conflitto tra le disposizioni del Contratto e il presente DPA, prevale il DPA per tutti gli aspetti inerenti alla protezione dei dati personali.

14.Legge applicabile e foro

14.1. Il presente DPA è regolato dalla legge italiana. Per ogni controversia tra le Parti relativa alla validità, interpretazione ed esecuzione del DPA è competente in via esclusiva il foro di Varese, fatti salvi i diritti degli interessati e le competenze dell'Autorità di controllo ai sensi del GDPR.