

ACCORDO PRINCIPALE PER IL TRATTAMENTO DEI DATI PERSONALI – MASTER DATA PROCESSING AGREEMENT (ex art. 28 del Regolamento EU 2016/679)

Il presente accordo per la protezione dei dati personali è concluso tra il Fornitore, come di seguito definito, e il Cliente che accetta il presente accordo.

Per "**Fornitore**" si intende **Maggioli S.p.A.**, con sede in Santarcangelo di Romagna (RN) Via del Carpino n. 8 – iscritta al Registro delle CCIAA della Romagna Forlì-Cesena e Rimini al n. 06188330150, al R.E.A. di Rimini al n. 219107, C.F. 06188330150 e Partita IVA 02066400405 in persona del proprio Procuratore Speciale;

E

il soggetto indicato nel Contratto quale cliente (di seguito il "**Cliente**").

Nel seguito il Cliente ed il Fornitore saranno individualmente denominati la "**Parte**" e congiuntamente come le "**Parti**".

PREMESSO CHE

- a)** il Cliente ha sottoscritto uno o più contratti con il Fornitore (di seguito il "**Contratto**");
- b)** La sottoscrizione del Contratto prevede, in capo al Fornitore, il porre in essere alcune operazioni di trattamento aventi ad oggetto i dati del Cliente e pertanto soggette all'applicazione delle regole e dei principi di cui al Regolamento (EU) n. 2016/679 (nel seguito anche "**GDPR**");
- c)** Alla luce di quanto rappresentato al precedente punto (b) le Parti intendono disciplinare con il presente accordo il trattamento dei dati personali – Data Processing Agreement (nel seguito "**DPA**" o "**Accordo sul trattamento dati**") in relazione alle condizioni ed alle modalità di trattamento dei dati personali eseguite dal Fornitore nell'ambito del Contratto e dell'erogazione dei Servizi;
- d)** Essendo state verificate dal Cliente le competenze tecniche ed organizzative del Fornitore ed in conformità rispetto a quanto stabilito dall'art. 28 del GDPR, il Cliente intende, in ragione di quanto suesposto, conferire al Fornitore, senza alcun onere aggiuntivo rispetto al Contratto, l'incarico di Responsabile del Trattamento (nel seguito anche "**Responsabile**").

Tutto quanto sopra premesso le Parti convengono quanto segue:

DEFINIZIONI E INTERPRETAZIONE

Le premesse costituiscono parte integrante del presente Accordo.

Nel DPA i termini utilizzati avranno il medesimo significato loro attribuito nel Contratto e con le seguenti definizioni; ogni ulteriore termine non contemplato nel Contratto assumerà il significato rappresentato con la lettera iniziale maiuscola e connotato da uno specifico significato, in particolare con:

"**Data di Decorrenza dell'Accordo sul Trattamento Dati**" si intende la data in cui il Cliente ha sottoscritto il Contratto a cui il presente Accordo è legato;

"**Dati Personali**" si intende il significato di cui alla Legislazione in materia di Protezione dei Dati Personali e includerà, a titolo puramente esemplificativo ma non esaustivo, tutti i dati forniti, archiviati, inviati, ricevuti o altrimenti elaborati, o creati dal Cliente, o Terzo Titolare in relazione alla fruizione dei Servizi, nella misura in cui siano oggetto di trattamento da parte del Fornitore, sulla base del Contratto;

“Decisione di Adeguatezza” si intende una decisione della Commissione Europea sulla base della quale sono previsti strumenti vincolanti per i Paesi dell’Unione ed in base ad esse è ammesso il trasferimento di dati verso il Paese indicato nella Decisione di Adeguatezza emanata;

“Istruzioni” si intendono le istruzioni scritte e impartite dal Cliente al Fornitore all’interno del presente Accordo con lo scopo di delimitare i poteri decisorii del Fornitore Responsabile nella scelta dei mezzi e delle finalità di trattamento;

“Legislazione in materia di Protezione dei Dati Personali” si intende il Regolamento EU n. 2016/679 ovvero GDPR, nonché ogni eventuale ulteriore norma e/o regolamento sul trattamento dei dati personali vigenti in Italia, ivi incluso il Decreto Legislativo n. 196/2003, come modificato e integrato dal D. Lgs. n. 101/2018, nonché ogni provvedimento vincolante che risulti emanato dalle Autorità di controllo competenti in materia;

“Personale del Fornitore” si intende ogni persona fisica con la qualifica, a titolo esemplificativo ma non esaustivo, di dirigente, dipendente, consulente e/o collaboratore, nonché ogni altra figura a ciò incaricata dal Fornitore facente parte dell’organizzazione del Fornitore stesso;

“Interessato/i”: si intende il/i soggetto/i persona fisica, determinata o determinabile, cui i dati personali si riferiscono. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come: il nome e cognome, un numero di identificazione, dati relativi all’ubicazione, un identificativo on line, oppure a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

“Richiesta” si intende una richiesta di esercizio di taluno dei diritti spettanti all’Interessato/i e previsti dal GDPR (artt. 15 - 22); Il Fornitore non ha diretto rapporto con gli Interessati, verso i quali ha contatti unicamente il Cliente. Alla luce di ciò il Fornitore si impegna ad informare il Cliente delle Richieste pervenute ma si asterrà dal riscontrarle autonomamente in quanto la gestione di tali Richieste è di precipua spettanza del Cliente Titolare;

“Sub-Responsabile” si intende qualunque ulteriore fornitore, che abbia un assetto societario autonomo rispetto al Fornitore, cui Maggioli abbia affidato un servizio collegato agli obblighi assunti contrattualmente nel Contratto e che Maggioli ha vincolato mediante DPA al rispetto dei medesimi obblighi dalla stessa assunti con il presente Accordo sul trattamento dati;

“Ordine” si intende qualsiasi OdA/RdA effettuato dal Cliente in relazione al Servizio/i;

“Servizio/i” si intende quanto concordato tra le Parti nell’Ordine o nel Contratto;

“Terzo Titolare”: si intende il Titolare del trattamento allorché il Cliente di Maggioli sia qualificato come Responsabile;

“Evento di Sicurezza Informatica” o data breach si intende la violazione di sicurezza che può comportare accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai Dati Personali occorsa sui sistemi IT gestiti dal Fornitore o comunque sui quali il Fornitore abbia o debba avere un controllo.

RUOLO DELLE PARTI

Le Parti riconoscono e convengono che il Fornitore agisce “di regola” quale Responsabile in relazione ai Dati Personali oggetto di trattamento in relazione all’espletamento del Servizio, mentre il Cliente agisce “di regola” quale Titolare dei Dati Personali.

Qualora il Cliente svolga operazioni di trattamento per conto di altro titolare ovvero del Terzo Titolare, il Cliente assumerà la qualifica di Responsabile. In tal caso, il Cliente garantisce che le Istruzioni impartite e le attività intraprese in relazione al trattamento dei Dati Personali, inclusa la nomina, da parte del Cliente verso il Fornitore quale Sub-Responsabile derivante dalla stipulazione del presente Accordo, è stata autorizzata in via generale o specifica dal Terzo Titolare. Il Cliente si impegna pertanto ad esibire al Fornitore, dietro sua semplice richiesta scritta, la documentazione comprovante quanto sopra.

Ciascuna delle Parti si impegna a conformarsi, nel trattamento dei Dati Personali, ai rispettivi obblighi derivanti dalla Legislazione in materia di Protezione dei Dati Personali applicabile.

Il Fornitore ha nominato un Responsabile della protezione dei dati (DPO), domiciliato presso la sede di Maggioli S.p.A. che può essere contattato al seguente indirizzo e-mail: dpo.privacy@maggioli.it o PEC: dpo.privacy@maggioli.legalmail.it.

Il Titolare ha valutato che Maggioli S.p.A. sotto il profilo della strutturazione, dell'organizzazione di mezzi e uomini, delle conoscenze, competenze e Know how disponibili possiede i requisiti di affidabilità, capacità ed esperienza tali da fornire l'idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza. Il Cliente può richiedere documentazione di compliance a supporto di quanto suesposto contattando l'Ufficio Privacy scrivendo al seguente indirizzo di posta privacy@maggioli.it.

Tutto ciò premesso,

DESIGNA

Maggioli S.p.A. in virtù dell'art. 28 del Reg. UE 2016/679 quale *Responsabile del trattamento dei dati personali* (di seguito "*Maggioli S.p.A.*" o "*Responsabile*").

Il Trattamento è affidato esclusivamente con le finalità proprie del *Cliente*, al fine di consentire l'esecuzione delle attività affidate a Maggioli S.p.A.

Si rileva che il *Fornitore* esegue il trattamento dei Dati Personali di titolarità del *Cliente* esclusivamente come conseguenza delle attività e finalità strettamente inerenti allo svolgimento del Servizio di cui in premessa ed oggetto del Contratto.

Nell'espletamento dell'incarico, il *Responsabile* dovrà attenersi alle disposizioni vigenti disposte dalla legislazione in materia e specificatamente il trattamento dovrà essere realizzato in osservanza delle norme Regolamento Europeo Privacy (GDPR) 2016/679 e delle apposite prescrizioni che verranno impartite dal *Titolare*.

Il trattamento è affidato esclusivamente con le finalità proprie del *Titolare* e cioè di consentire l'esecuzione delle attività del fornitore dei servizi sopra elencati.

Sia il *Titolare* che il *Responsabile*, sono tenuti ad attuare le misure tecniche ed organizzative tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, 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 per quanto previsto agli articoli 32-33 e 35-36 del GDPR. Inoltre devono ottemperare a specifici requisiti previsti dal GDPR per ridurre i rischi del trattamento e assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

OBBLIGHI DEL RESPONSABILE

Il *Responsabile* ha anche altri obblighi specifici:

- I dati personali dei quali il *Responsabile* verrà a conoscenza sono di proprietà del *Titolare*; il *Responsabile*, pertanto, potrà tenerne copia solo per l'espletamento dei compiti affidati e limitatamente al tempo strettamente necessario a svolgere le operazioni consentite.
- Il *Responsabile* ha l'obbligo specifico di attenersi al divieto di comunicazione non espressamente autorizzata e di diffusione a qualsiasi titolo dei dati personali, nonché al divieto di utilizzo autonomo per finalità diverse rispetto a quanto qui specificato. Inoltre i dati personali saranno trattati dal Personale del Fornitore opportunamente informato e/o incaricato dal *Responsabile*.
- (Qualora la natura dell'incarico prevedesse l'intervento di Amministratori di sistema) Il *Responsabile* provvede all'osservanza di quanto stabilito dal provvedimento a carattere generale - 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" (G.U. n. 300 del 24/12/2008) e successive modifiche, emesso dall'autorità Garante per la protezione dei dati personali.
- (Qualora la natura dell'incarico prevedesse l'intervento di Amministratori di sistema) Il *Responsabile* adotta le misure tecniche ed organizzative del menzionato provvedimento, con riferimento: alla conservazione presso la propria organizzazione degli estremi identificativi delle persone preposte quali amministratori di sistema ed autorizzate quali incaricati al trattamento designati, le nomine degli stessi come amministratori di sistema secondo quanto previsto dal suddetto provvedimento e l'applicazione diligente dello stesso;
- (Qualora la natura dell'incarico prevedesse l'intervento di Amministratori di sistema) Il *Responsabile* secondo quanto stabilito dal provvedimento in materia di Amministratori di Sistema, comunicherà al *Titolare* i nominativi dei soggetti designati quali amministratori di sistema, che opereranno con tale qualifica presso la struttura del *Titolare* per le attività limitate all'affidamento. L'archiviazione dei log secondo quanto previsto dal provvedimento 27 novembre 2008 in termini di amministratori di sistema è a carico del *Titolare*.
- Il *Responsabile* fornisce se richiesto le Linee Guida per il Trattamento dei Dati Personali ai sensi del GDPR 2016/679.
- All'interno dell'organizzazione del *Responsabile* i dati potranno essere trattati soltanto da soggetti che dovranno utilizzarli per l'esecuzione delle prestazioni oggetto dei servizi affidati dal *Titolare*. Il *Responsabile* dovrà impartire ai suddetti soggetti autorizzati al trattamento, ogni necessaria istruzione (anche per iscritto) in merito al corretto utilizzo di tutti gli apparati di sistema ed informatici coinvolti in operazioni di trattamento di dati personali e mantenere la lista degli autorizzati al trattamento aggiornata. Il *Responsabile* dovrà inoltre vigilare sul rispetto delle Istruzioni impartite ai propri autorizzati al trattamento.
- Il Personale del Fornitore che sarà incaricato dal *Responsabile* di svolgere le prestazioni assicurerà serietà ed affidabilità e sarà debitamente formato ed informato sulle modalità del trattamento, sui rischi che incombono sui dati e sui profili della vigente normativa.
- Il *Responsabile* deve rispettare, salvo diversa prescrizione scritta del *Titolare*, quanto previsto all'articolo 28 paragrafi 2,3,4. In particolare in riferimento a quanto previsto dal paragrafo 3 alle lettere a, b, c, d, e, f, g, h.
- Il *Titolare* autorizza sin d'ora il *Responsabile* a trasferire, qualora necessario, i dati personali trattati per suo conto al di fuori dello Spazio Economico Europeo. In tale ipotesi, il *Responsabile* dovrà assicurare e garantire che il trattamento avvenga verso Paesi terzi e Organizzazioni internazionali che garantiscano un livello di sicurezza e protezione adeguato, basando il trasferimento stesso su una Decisione di Adeguatezza della Commissione UE o su altri meccanismi di garanzia (quali ad esempio Clausole Contrattuali Standard o Binding Corporate Rules) oppure su una delle deroghe previste dalla normativa vigente.
- Il *Responsabile* si impegna a garantire i diritti spettanti agli Interessati per come stabiliti dal GDPR 679/2016, il *Responsabile* non potendo gestire e/o riscontrare direttamente le richieste degli Interessati si

impegna a comunicare immediatamente al *Titolare* qualsiasi richiesta di esercizio diritti pervenuta da un Interessato, al fine di consentire al *Cliente* la possibilità di fornire riscontro all'Interessato.

GESTIONE DELLE TERZE PARTI

In coerenza con quanto predisposto all'interno del Contratto:

- Nel caso in cui sia prevista *autorizzazione generale*, il Responsabile ove, per l'esecuzione dell'attività, ritenga opportuno o necessario nominare altri Responsabili (c.d. *Sub-Responsabili*) è autorizzato sin d'ora a nominarli, con l'obbligo di darne notizia al Titolare.

A tale fine il *Responsabile* mette a disposizione del *Titolare* la lista dei *Sub-Responsabili* al seguente link <https://assistenza.maggioli.it/privacy/>. La lista è tenuta costantemente aggiornata dal responsabile e può essere consultata in ogni momento dal *Titolare* che potrà prendere visione di modifiche e sostituzioni. Il *Titolare* autorizza sin d'ora i responsabili elencati potendo richiedere informazioni di dettaglio all'indirizzo privacy@maggioli.it.

- In caso contrario, nell'eventualità in cui il *Titolare* debba concedere *autorizzazione specifica*, il *Responsabile* entro i venti (20) giorni successivi alla stipula del Contratto, si impegna a fornire l'elenco delle terze parti qualificate quali *Sub-Responsabili* utilizzati per l'esecuzione dell'attività di cui al Servizio. L'elenco delle terze parti sarà trasmesso al *Titolare* via PEC.

- In mancanza di un'espressa indicazione/istruzione da parte del *Titolare*, il *Fornitore* rispetto alla gestione delle terze parti si conformerà a quanto stabilito dalla Legislazione in materia di Protezione dei Dati Personali, nonché ogni ulteriore normativa a ciò applicabile.

- Nel caso in cui il *Responsabile* ricorra a un altro soggetto per l'esecuzione di specifiche attività di trattamento per conto del Titolare, sarà tenuto a imporre su tale *Sub-Responsabile* gli stessi obblighi in materia di protezione dei dati contenuti nella presente nomina, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento.

- Qualora il *Sub-Responsabile* ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi dell'altro Responsabile.

ADEMPIMENTI DEL RESPONSABILE IN CASO DI DATA BREACH

Il *Responsabile* si è dotato di un proprio modello di incident response volto alla gestione degli Eventi di Sicurezza Informatica; alla luce di ciò provvederà ad informare come per legge, entro 24 massimo 48 ore dalla qualificazione dell'evento, in forma scritta il *Cliente* circa l'Evento di Sicurezza Informatica occorso. Tale comunicazione sarà in linea con quanto previsto dagli articoli 33, 34 del GDPR.

Il *Responsabile* del trattamento procederà con le operazioni di trattamento dei dati personali in presenza delle misure di sicurezza richieste ai sensi e per gli effetti dell'art. 32 del GDPR e valutate dal *Responsabile* in base al contesto del trattamento. Le misure di sicurezza adottate sono quelle dichiarate in appositi documenti (tra cui il questionario di qualifica del fornitore allegato) messi a disposizione del *Titolare*.

DURATA E CESSAZIONE DEL TRATTAMENTO

Il presente Accordo avrà la durata indicata nel Contratto al quale si riferisce ed assumerà efficacia dalla Data di Decorrenza dell'Accordo.

Nel caso in cui la cessazione delle Operazioni di Trattamento da parte del *Responsabile* configuri una cessazione del trattamento, questi provvede a notificarlo per iscritto con congruo anticipo al *Titolare* per l'adozione degli opportuni provvedimenti di Legge.

In fine, all'atto della cessazione, per qualsiasi causa, delle operazioni di trattamento da parte di Maggioli S.p.A., quest'ultima, trascorsi dodici (12) mesi, provvederà alla integrale distruzione dei dati, salvo diverso accordo tra le parti, fatta eccezione per la documentazione amministrativa la cui tenuta è gestita in ottemperanza agli obblighi di conservazione stabiliti per legge.

Inoltre il *Responsabile* sarà autorizzato a trattare i dati per conto del *Titolare* - anche ai fini dell'erogazione del servizio - nel periodo intercorrente tra la cessazione di un contratto e le conseguenti attività di migrazione, per un periodo non superiore a dodici mesi dalla cessazione degli effetti del contratto.

VERIFICHE DEL TITOLARE DEL TRATTAMENTO

Il *Titolare* del trattamento, come previsto dalla vigente normativa, sarà chiamato ad esercitare vigilanza e controllo sull'osservanza delle Istruzioni impartite al *Responsabile* e delle vigenti disposizioni in materia di trattamento dei dati personali. L'attività di verifica potrà concretizzarsi attraverso la richiesta al *Responsabile* di compiere attività di autovalutazione rispetto alle misure di sicurezza adottate, sull'osservanza delle misure impartite, fornendone, a richiesta, documentazione scritta. Il *Titolare* ha il diritto di esercitare controlli o attività di audit relative all'oggetto del contratto stipulato tra le parti, presso le sedi del *Responsabile* o da remoto, finalizzati ad una verifica della puntuale applicazione delle Istruzioni impartite, nonché della conformità alla legge delle operazioni di trattamento. Tali controlli dovranno essere effettuati mediante comunicazione preventiva a Maggioli S.p.A., da comunicarsi con congruo anticipo (almeno con quattordici (14) giorni di anticipo), di convocazione di un meeting pre-audit tra le parti volto a concertare gli step da seguire.

ULTERIORI DISPOSIZIONI

Il *Responsabile*, con l'accettazione della presente nomina, si impegna a tenere indenne il *Titolare* da ogni responsabilità, costo, spesa o altro onere, discendenti da pretese, azioni o procedimenti di terzi a causa della violazione da sua parte o di suoi dipendenti e/o collaboratori o Sub-Responsabili degli obblighi a proprio carico in base alla presente nomina e/o della violazione delle prescrizioni contenute nel Regolamento Europeo 2016/679.

Il *Titolare* tiene indenne e manlevato il *Responsabile* da ogni perdita, costo, spesa, multa e/o sanzione, danno e da ogni responsabilità di qualsiasi natura connessa al trattamento dei dati personali effettuato dal *Responsabile* nel rispetto e nella piena osservanza di tutte le Istruzioni e prescrizioni impartite dal *Titolare* con la presente nomina e per qualsiasi responsabilità connessa al trattamento dei dati personali e per operazioni al trattamento per cui lo stesso non è espressamente nominato *Responsabile*. Il *Titolare* tiene altresì indenne e manlevato il *Responsabile* da eventuali pretese di terzi che dovessero lamentare l'illegittimo trattamento dei loro dati personali effettuato dal *Responsabile* su richiesta del *Titolare*.

Per tutto quanto non espressamente specificato in questa scrittura, il *Titolare* ed il *Responsabile* si atterrano in generale a quanto previsto dalla vigente disciplina in materia di dati personali, Reg. UE 2016/679.