Atto di nomina del Responsabile del Trattamento dei Dati Personali

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

TRA
AST FERMO
con Sede: Via Zeppilli, 18 – 63900 (FM)
PEC: ast.fermo@emarche.it

- TITOLARE DEL TRATTAMENTO -

E

LA SOCIETA':
con sede:
Tel.:
e-mail / PEC:

- RESPONSABILE DEL TRATTAMENTO -

L' **AST FERMO** (di seguito anche Azienda) in qualità di Titolare del Trattamento dei dati personali relativi alle attività istituzionali di competenza, considerato che:

- L'Azienda e la SOCIETÀ hanno stipulato un contratto di _____, affidato con determina n. …. del ….;

- in virtù di tale rapporto contrattuale, è di seguito riportata l'attività di trattamento conferita alla SOCIETÀ:
  - _____

ai sensi e agli effetti dell'art. 28 del Regolamento UE 2016/679 - GDPR con il presente atto, formalmente

NOMINA:

la SOCIETÀ nella veste di Responsabile del trattamento dei dati personali (di seguito: Responsabile), nell'ambito e nei limiti dell'oggetto del contratto vigente tra le parti di cui il presente atto di nomina è l'allegato e parte integrante.

Con l'adesione al presente atto, inoltre, il Responsabile dichiara e garantisce di svolgere la propria attività di trattamento di dati personali con le capacità, l'esperienza e l'affidabilità tali da poter garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento di dati personali, ivi compreso il profilo relativo alla sicurezza.

La natura e le finalità del trattamento di dati personali affidati al Responsabile sono descritte nel contratto di cui il presente atto è l'Allegato. Resta fermo il divieto, per il Responsabile, di utilizzare i dati personali trattati per conto del Titolare per perseguire finalità differenti rispetto a quelle delineate da quest'ultimo, salvo comunicazione scritta al Titolare, che ne autorizzi il diverso fine. Rimane inteso che, qualora il Responsabile determini finalità e mezzi di trattamento differenti e ulteriori rispetto a quelli individuati dal contratto, questi agirà in veste di Titolare del trattamento di tali dati, con le conseguenze di natura amministrativa e civilistica previste dalla normativa vigente in materia di protezione dei dati personali.

Il Responsabile dovrà attenersi alle istruzioni del Titolare e alle relative integrazioni che potranno intervenire nel corso del rapporto contrattuale.

ISTRUZIONI PER IL RESPONSABILE

Nell'ambito delle attività di trattamento affidate con la Nomina a Responsabile sono riportate le istruzioni a cui deve attenersi il Responsabile nel corso del trattamento dei dati personali per conto del Titolare, in conformità alle normative vigenti sulla protezione dei dati personali.

1. REQUISITI E AFFIDABILITÀ DEL RESPONSABILE

Il Responsabile deve:

i. garantire la riservatezza delle informazioni, dei documenti e degli atti amministrativi di cui abbia conoscenza durante l'esecuzione del servizio;
ii. trattare e/o utilizzare i dati esclusivamente per le finalità connesse allo svolgimento del servizio oggetto del contratto, con divieto di qualsiasi altra diversa utilizzazione/trattamento non attinente allo scopo dei servizi offerti;
iii. svolgere un'analisi dei rischi in conformità a quanto previsto dalla vigente normativa;
iv. vigilare sulla corretta osservanza delle istruzioni impartite ai suoi autorizzati;
v. astenersi dal modificare, correggere, trasferire, diffondere e/o comunicare i dati al di fuori dei casi previsti per legge o per contratto.

Il Responsabile deve garantire, inoltre, che tutte le persone autorizzate al trattamento dei dati personali del Titolare:

vi. siano informate della natura confidenziale dei dati personali del Titolare e degli obblighi del Responsabile del trattamento, secondo quanto disposto dal presente Atto e dal Contratto/Accordo/Incarico intercorrente tra il Responsabile e il Titolare, in relazione ai dati personali di quest'ultimo;
vii. siano state debitamente formate in merito alla corretta applicazione della normativa in materia di protezione di dati personali, per ciò che attiene i compiti loro affidati;
viii. siano soggetti ad impegno di riservatezza in relazione ai dati trattati per conto del Titolare;
ix. siano soggetti all'autenticazione dell'Utente in caso di accesso ai dati personali del Titolare, conformemente al presente Atto, al contratto vigente tra le parti nonché alle norme di legge in materia di protezione dei dati personali.

2. RICORSO AD ALTRO RESPONSABILE DEL TRATTAMENTO

Il Titolare fornisce autorizzazione generale al Responsabile ad avvalersi di altri Responsabili del trattamento (di seguito: Sub-responsabili) nel rispetto di quanto segue.

Il Responsabile:

i. garantisce al Titolare del trattamento che il Sub-responsabile è in grado di assicurare il livello di protezione dei dati personali del Titolare, ponendo in atto le misure tecniche e organizzative idonee a soddisfare i requisiti del GDPR in materia di protezione dei dati personali, nonché quanto previsto dall'art. 28 GDPR e dal presente Atto nei confronti del Responsabile principale del trattamento;
ii. dà atto che, qualora un Sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati personali, il Responsabile conserva nei confronti del Titolare la piena responsabilità in relazione agli obblighi imposti dal presente atto;
iii. comunica, su richiesta del Titolare, l'elenco dei soggetti individuati, di cui si avvale per prestare quanto oggetto del contratto e che assumeranno, rispetto allo stesso, il ruolo di sub-responsabili, in modo da essere preventivamente condiviso con il Titolare stesso (v. Allegato 2);
iv. si impegna, altresì, ad informare il Titolare di eventuali modifiche riguardanti la sostituzione di altri sub-responsabili dando così al Titolare la possibilità di opporsi a tali modifiche.

3. DURATA DEL TRATTAMENTO E OBBLIGHI DI CANCELLAZIONE DEI DATI PERSONALI DEL TITOLARE

Il Responsabile dovrà, alla cessazione del rapporto derivante dal contratto per qualsiasi causa e, comunque, non oltre 30 giorni, cessare il trattamento dei dati personali del Titolare e provvedere alla cancellazione sicura (*file o disk wipe*) di tutti di dati personali (e delle eventuali copie) trattati per conto del Titolare.

Dell'avvenuta cancellazione, il Titolare può richiedere al Responsabile conferma scritta.

Su richiesta del Titolare, il Responsabile restituisce copia completa di tutti i dati personali trattati per suo conto in virtù dell'incarico oggetto del contratto, mediante trasferimento sicuro di file nel formato indicato dal Titolare.

4. OBBLIGHI DEL TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento si impegna, in virtù di quanto previsto dal presente Atto a:

i. fornire agli Interessati destinatari del servizio oggetto della presente contratto, reso dal Responsabile, l'informativa di cui agli Artt. 13-14 GDPR per le operazioni del trattamento al momento della raccolta dei dati;
ii. trasmettere al Responsabile i dati personali da trattare per suo conto, in virtù di quanto necessario per l'adempimento, da parte del Responsabile, del contratto sottoscritto tra le parti;
iii. documentare per iscritto tutte le istruzioni riguardanti il trattamento dei dati da parte del Responsabile del trattamento;
iv. vigilare, prima e durante il trattamento da parte del Responsabile, sul rispetto degli obblighi previsti dal GDPR sulla protezione dei dati e dalla disciplina nazionale;
v. supervisionare il trattamento svolto dal Responsabile per suo conto, sulla base di quanto previsto dal presente Atto e dalla normativa sulla protezione dei dati personali.

5. OBBLIGHI DEL RESPONSABILE

Il Fornitore, nel corso dell'attività di trattamento dei dati personali per conto del Titolare, garantisce:

a) L'adozione del Registro dei trattamenti del Responsabile del Trattamento

Il fornitore (responsabile), con la sottoscrizione del presente Atto, assicura al Titolare di aver adottato un registro contenente i suoi dati di contatto, i dati di contatto del Titolare per conto del quale svolge i trattamenti, le categorie di trattamenti effettuati sotto la sua responsabilità per conto del Titolare, gli eventuali trasferimenti di dati verso paesi terzi od organizzazioni internazionali nonché una descrizione generale delle misure di sicurezza tecniche e organizzative attuate, secondo quanto previsto dall'art. 30 GDPR.

b) Misure tecniche e organizzative per la sicurezza dei dati personali

Il Fornitore, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché delle categorie dei trattamenti effettuati per conto del Titolare, come anche del rischio di varia probabilità e gravità per i diritti e le libertà degli Interessati, mette in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, come, ad esempio:

i. la pseudonimizzazione e la cifratura dei dati personali;
ii. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
iii. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

iv. una Procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
v. la nomina, se necessario, del personale impiegato nell'ambito dell'oggetto del contratto per le attività configurabili come Amministratore di Sistema, in particolare per la gestione del network, dei sistemi, del middleware e dei database, e infine del livello applicativo conformemente a quanto previsto dal Provvedimento del Garante della Protezione dei dati Personali "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008*", come successivamente modificato dal provvedimento del 25 giugno 2009;
vi. la comunicazione, a richiesta, della lista degli Amministratori di Sistema nominati e della relativa funzione, che saranno impegnati nelle attività di supporto, manutenzione o aggiornamento;
vii. la conformità alle procedure tecniche e operative previste dal Titolare come la procedura di gestione di eventuali data breach.

Il Fornitore dichiara e garantisce che le Misure di sicurezza adottate sono idonee a ridurre al minimo i rischi di distruzione perdita, modifica, divulgazione e accesso non autorizzato nonché di trattamenti non conformi alle finalità stabilite dal Contratto/Accordo/Incarico e dal presente Atto.

c) Garanzia per l'esercizio dei Diritti dell'Interessato

Il Fornitore, prima di iniziare il trattamento dei dati personali per conto del Titolare, deve fornire alle persone Interessate dalle operazioni di trattamento dei loro dati personali le informazioni relative ai trattamenti che esso realizza. La formulazione e il formato dell'informazione deve essere convenuta con il Titolare del trattamento prima della raccolta dei dati.
Il Fornitore si impegna ad assistere il Titolare, anche implementando misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti che la normativa riconosce agli Interessati, ovvero l'accesso, la cancellazione dei dati personali, l'opposizione e la limitazione dei trattamenti, la portabilità dei dati e il diritto di non essere oggetto di una decisione individuale automatizzata (compresa la profilazione).

Nel caso in cui il Fornitore riceva richieste concernenti il trattamento dei dati personali dagli Interessati, da Autorità amministrative o giudiziarie, egli ha l'obbligo di darne comunicazione scritta al Titolare, entro e non oltre il terzo giorno dal ricevimento delle richieste stesse, allegandone copia.

d) Adempimenti in caso di Violazione di dati personali

Il Fornitore ha l'obbligo di comunicare al Titolare ogni violazione della sicurezza dei dati personali trattati per conto dello stesso, entro e non oltre 24 ore dal momento in cui ne sia venuto a conoscenza. Tale comunicazione deve contenere, almeno, le seguenti informazioni:

(i) la descrizione della natura della violazione, le categorie di dati personali violati, il numero degli Interessati coinvolti e le registrazioni di trattamento corrispondenti;
(ii) la comunicazione dei dati di contatto dell'eventuale Responsabile per la protezione dei dati personali da cui ottenere eventuali ulteriori informazioni;
(iii) la descrizione delle probabili conseguenze della violazione per gli Interessati;
(iv) la descrizione delle misure adottate e/o proposte per porre rimedio alla violazione dei dati personali.

e) Collaborazione del Fornitore per la Valutazione d'impatto sulla protezione dei dati personali

Il Fornitore si impegna, su richiesta del Titolare, a collaborare con quest'ultimo per consentire il corretto svolgimento di una Valutazione d'impatto di cui all'art. 35 GDPR, contribuendo a individuare e implementare le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per

garantire la protezione dei dati personali e dimostrare la conformità alla normativa in materia, tenuto conto dei diritti degli Interessati e degli altri soggetti coinvolti.

f) Istruzioni del Titolare e garanzia di conformità alla normativa in materia di protezione dei dati personali (diritto di Audit)

Il Fornitore si impegna a trattare i dati personali del Titolare conformemente alle istruzioni documentate del Titolare del trattamento. Ove il Fornitore ritenga che una o più Istruzioni costituiscano violazione del GDPR o di altre disposizioni delle leggi dell'Unione o delle leggi degli stati membri relative alla protezione dei dati, deve informarne immediatamente il Titolare.
Il Fornitore si impegna, altresì, ad informare il Titolare, prima dell'inizio del trattamento, dell'esistenza di un obbligo giuridico, dettato da leggi dell'Unione o da leggi dello Stato membro al quale è sottoposto, di procedere al trasferimento dei dati verso un paese terzo o un'organizzazione internazionale, salvo che la normativa applicabile vieti una tale informazione, per ragioni di interesse pubblico.

Il Fornitore si impegna a consentire, su richiesta motivata del Titolare, l'effettuazione di verifiche periodiche volte a verificare la corretta esecuzione dei trattamenti, il rispetto del Contratto/Accordo/Incarico e di quanto previsto dal presente Atto, previo accordo tra le parti sui tempi e le modalità della verifica. Su richiesta del Titolare, il Fornitore fornisce al Titolare del trattamento tutte le informazioni e i report utili ad attestare l'adempimento degli obblighi quivi previsti, con particolare riguardo alle misure di sicurezza adottate.

6. VIGENZA E VINCOLATIVITÀ DELLE DISPOSIZIONI

Le parti danno atto e accettano la vigenza e vincolatività delle disposizioni del presente Atto fino alla scadenza, risoluzione ed esistenza del contratto esistente tra il Titolare del trattamento e il Responsabile del servizio oggetto del contratto. La violazione di qualsiasi disposizione del presente Atto, da parte di entrambi i firmatari, costituisce violazione sostanziale del contratto sottoscritta tra le parti, e può essere causa di risoluzione della stessa, ove ne sussistano i requisiti di legge.

Qualora sussistano incongruenze sostanziali tra le disposizioni contenute nel presente Atto e quelle risultanti dal contratto vigente tra le parti, devono considerarsi prevalenti le disposizioni contenute nel presente Atto, per quanto riguarda gli obblighi imposti alle parti in materia di protezione dei dati personali e di tutela degli Interessati coinvolti nei trattamenti svolti per conto del Titolare.

_____, ../../….

Il Titolare

Il Responsabile

Allegato 1

DESCRIZIONE DEL TRATTAMENTO

1. OPERATIVITÀ DEL TRATTAMENTO

Le attività di trattamento di dati personali devono essere relazionate in via univoca alle operatività sopradescritte, nello specifico:

- ☐ conservazione di dati;
- ☐ operatività di Amministratore di sistema.

2. NATURA E FINALITÀ DEL TRATTAMENTO

Il trattamento dei dati personali è effettuato esclusivamente per la corretta esecuzione delle attività concordate tra le Parti e di cui al citato contratto.

3. CATEGORIE DI DATI PERSONALI TRATTATI

Il Responsabile del trattamento per espletare le attività pattuite tra le Parti per conto del Titolare tratta direttamente o anche solo indirettamente le seguenti categorie di dati:

- ☐ dati personali, di cui all'art. 4 n. 1 GDPR;
- ☐ dati rientranti nelle categorie "particolari" di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute, alla vita sessuale, all'orientamento sessuale della persona) di cui all'art. 9 GDPR;
- ☐ dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza di cui all'art. 10 GDPR.

4. CATEGORIE DI INTERESSATI I CUI DATI PERSONALI SONO TRATTATI

Per effetto della presente nomina, le categorie di interessati i cui dati personali possono essere trattati, sono:

- ☐ Cittadini di Paesi non appartenenti all'U.E.;
- ☐ Persone vulnerabili (minori di età, persone disabili ecc.);
- ☐ Persone giuridiche costituite in forma di società di persone;
- ☐ Personale dipendente;
- ☐ Pazienti;
- ☐ Utenti (anche potenziali);
- ☐ altro _____

5. DURATA DEL TRATTAMENTO

Per tutta la durata del rapporto contrattuale in essere sino a sua scadenza o risoluzione.

Allegato 2

Elenco dei sub-responsabili del trattamento

Il Titolare del trattamento ha autorizzato il ricorso ai seguenti sub-responsabili del trattamento:

	Denominazione Sociale – Indirizzo – P.IVA	Ambito Del Trattamento (*se Extra UE indicare le garanzie ex. 44 ss. GDPR*)	Incarico Assegnato
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			