

**Oggetto: Atto di designazione a responsabile del trattamento di dati personali ai sensi dell'art. 28 del Regolamento (UE) n. 2016/679.**

In conformità a quanto stabilito dalla normativa nazionale ed europea applicabile in materia di protezione dei dati personali, con particolare riferimento al Regolamento (UE) n. 2016/679 (nel complesso, la "GDPR").

**PREMESSO CHE**

- a) AMIA VERONA S.p.A. ("Stazione Appaltante" - per brevità S.A.) e \_\_\_\_\_ ("Fornitore") hanno sottoscritto un contratto ("Contratto"), volto a disciplinare l'erogazione, da parte del Fornitore in favore di S.A., di servizi aventi ad oggetto quanto riportato nel frontespizio del CSA/Disciplinare di gara (nel complesso, i "Servizi");
- b) l'esecuzione dei Servizi comporta il trattamento, da parte del Fornitore, di dati personali di cui AMIA Verona S.p.A., ai sensi del GDPR, è Titolare;
- c) per mezzo del presente atto di designazione ("**Atto**"), S.A. ed il Fornitore intendono disciplinare i trattamenti di dati personali che quest'ultimo, in qualità di responsabile ai sensi del GDPR, svolgerà nell'interesse di S.A. nell'esecuzione dei Servizi.

Tutto ciò premesso e considerato, si conviene quanto segue:

- i) le parti concordano che, ai sensi della normativa applicabile, \_\_\_\_\_ è il titolare e/o responsabile dei dati che saranno messi a disposizione del Fornitore ai fini dell'esecuzione del Contratto ("**Dati condivisi**") e, di conseguenza, che quest'ultimo svolgerà i trattamenti connessi all'adempimento dei Servizi esclusivamente nella veste di responsabile come espressamente designato da Fornitore;
- ii) con la sottoscrizione del presente Atto, il Fornitore accetta la designazione quale responsabile del trattamento e conferma di possedere i requisiti di esperienza, capacità ed affidabilità richiesti dal GDPR, potendo dunque porre in essere, tra l'altro, misure tecniche e organizzative adeguate a garantire che i trattamenti dei Dati condivisi saranno eseguiti in conformità ai principi di legge, con particolare riferimento alla tutela dei diritti degli interessati;
- iii) il Fornitore si impegna ad osservare - e a fare in modo che tutti coloro che agiscono sotto la propria direzione a loro volta rispettino - gli obblighi stabiliti dalla normativa vigente in materia di protezione dei dati personali e, in particolare, a fare quanto segue:
  - a) svolgere esclusivamente le operazioni di trattamento delegate da parte di \_\_\_\_\_ e, per l'effetto, non utilizzare i Dati condivisi per finalità diverse da quelle collegate alla sola esecuzione del Contratto;

- b) trattare i Dati condivisi in piena conformità alle istruzioni qui fornite da parte di \_\_\_\_\_, o di quelle ulteriori che quest'ultima dovesse in un secondo momento ritenere opportuno fornire per la migliore e più efficiente esecuzione dei Servizi;
- c) individuare nominativamente, nell'ambito della propria struttura organizzativa, le persone autorizzate al trattamento dando loro le istruzioni necessarie all'esecuzione delle attività richieste;
- d) definire e mettere in atto misure tecniche e organizzative adeguate a garantire un idoneo livello di sicurezza dei Dati condivisi, tenendo conto delle *best practices* di settore, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità delle operazioni di trattamento connesse all'adempimento del Contratto, oltre che dei rischi che tali trattamenti possono determinare per i diritti e le libertà degli interessati;
- e) implementare misure e processi, nell'ottica di cui al punto che precede, che garantiscano l'attuazione dei principi di *privacy-by-design* e *privacy-by-default* e, più in generale, la minimizzazione e la sicurezza dei trattamenti, come ad esempio:
- l'adozione di sistemi di pseudonimizzazione<sup>1</sup> o cifratura dei Dati condivisi;
  - la capacità di assicurare con continuità la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi, oltre che quella di ripristinare tempestivamente la disponibilità e l'accesso ai Dati condivisi in caso di incidente fisico o tecnico;
  - l'attivazione di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative applicate al fine di garantire la sicurezza dei trattamenti;
- f) adottare le misure necessarie a 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 condivisi;
- g) fornire a \_\_\_\_\_ evidenza della procedura adottata per gestire eventuali violazioni della sicurezza da cui derivino, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati condivisi ("*Data breach<sup>2</sup> management policy*");
- h) conformarsi alla *Data breach management policy* adottata da parte di \_\_\_\_\_, laddove la propria sia ritenuta da \_\_\_\_\_, inadeguata a garantire i necessari livelli di sicurezza ai sensi della GDPR;
- i) notificare senza ingiustificato ritardo a \_\_\_\_\_ ogni possibile evento qualificabile come data breach ai sensi della normativa applicabile;
- j) informare prontamente \_\_\_\_\_ 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;

---

<sup>1</sup> il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

<sup>2</sup> la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

- k) non affidare alcun trattamento connesso all'esecuzione del Contratto ad eventuali sub-fornitori non espressamente autorizzati da \_\_\_\_\_. Resta inteso che il responsabile sarà obbligato a fare in modo che i sub-fornitori autorizzati ad operare siano vincolati al rispetto degli stessi obblighi applicabili al Fornitore in virtù del presente Atto e della normativa di volta in volta vigente. Il Fornitore sarà comunque responsabile di qualsiasi violazione o inadempimento commesso dai sub-fornitori, o dai loro dipendenti o collaboratori;
- l) adottare misure tecniche ed organizzative che consentano allo stesso di assistere \_\_\_\_\_ nell'adempimento del proprio obbligo di fornire riscontro alle richieste avanzate dagli interessati (ad esempio l'esercizio dei diritti di portabilità, di limitazione del trattamento e di cancellazione - "oblio" - dei dati);
- m) collaborare con \_\_\_\_\_, limitatamente ai trattamenti relativi ai Dati condivisi, nell'assolvimento degli obblighi di:
- notifica delle violazioni di dati all'Autorità Garante per la protezione dei dati personali (il "**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;
  - esecuzione, in tutti i casi in cui ciò sia necessario, di idonea valutazione di impatto sulla protezione dei dati (*data privacy impact assessment*), e di svolgimento delle procedure di consultazione preventiva con il Garante o con le altre autorità competenti.
- n) fermo l'obbligo di collaborazione di cui alla precedente lett. m), mettere \_\_\_\_\_ al corrente di qualsiasi richiesta di esercizio di diritti inviata da parte degli interessati che richieda un intervento di \_\_\_\_\_, entro un termine massimo di 24 ore dal ricevimento della stessa;
- o) non trasferire i Dati condivisi al di fuori dello Spazio Economico Europeo se non previa autorizzazione da parte di \_\_\_\_\_ ed in presenza di idonee garanzie ai sensi di legge (quali ad esempio decisioni di adeguatezza della Commissione UE, Clausole Contrattuali Standard o *Binding Corporate Rules*);
- p) non comunicare a terzi e, più in generale, non diffondere i Dati condivisi, se non in presenza di adeguati presupposti di liceità per tali ulteriori trattamenti;
- q) prestare nei confronti di \_\_\_\_\_ 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 di \_\_\_\_\_, dando altresì immediata esecuzione alle istruzioni ricevute e fornendo copia di ogni documento richiesto.
- r) predisporre e mantenere costantemente aggiornato, in formato elettronico o cartaceo, un registro di tutte le operazioni di trattamento svolte ai fini dell'esecuzione del Contratto, contenente in particolare:
- i propri dati di contatto, oltre a quelli del Titolare e, ove applicabile, del proprio responsabile della protezione dei dati (*data protection officer*);
  - le categorie dei trattamenti effettuati per conto di \_\_\_\_\_;
  - i dettagli relativi ad eventuali trasferimenti dei Dati condivisi al di fuori dello Spazio Economico Europeo (con indicazione del paese terzo o dell'organizzazione verso cui i

dati sono trasmessi) e le misure implementate a tutela dei dati, qualora il trasferimento non sia basato su una decisione di adeguatezza della Commissione UE o su altri meccanismi di garanzia (quali ad esempio Clausole Contrattuali Standard o *Binding Corporate Rules*) e non sia applicabile nessuna delle deroghe previste dalla normativa vigente;

- una descrizione generale delle misure di sicurezza tecniche e organizzative adottate in conformità al presente accordo e, più in generale, alla normativa applicabile.

Fermo tutto quanto sopra, il Fornitore dovrà mettere a disposizione di \_\_\_\_\_ tutte le informazioni necessarie a dimostrare il rispetto dei propri obblighi, cooperando altresì ad eventuali attività di *audit*, revisioni o controlli che \_\_\_\_\_ dovesse ritenere opportuno per monitorare il mantenimento dei dovuti livelli di sicurezza dei Dati condivisi per l'espletamento del Contratto.

Qualsiasi inadempimento o violazione degli obblighi sopra stabiliti e di ogni ulteriore norma di legge applicabile, con particolare riguardo ai necessari livelli di sicurezza, anche in tema di *data breach management*, ricadrà sotto l'esclusiva responsabilità del Fornitore. Ne consegue che quest'ultimo risponderà in via esclusiva (tranne casi di dolo o colpa grave da parte di \_\_\_\_\_) dell'inadempimento o della violazione rilevante, di ogni richiesta di risarcimento, danno o sanzione che dovesse derivare dal mancato puntuale assolvimento dei propri obblighi.

Il presente Atto avrà la medesima durata del Contratto. Pertanto, salvo il caso in cui lo stesso non venga prorogato su intesa delle parti, o che queste ultime non decidano di sciogliere il presente accordo prima della scadenza del Contratto, le disposizioni qui stabilite cesseranno di produrre ogni effetto nel momento stesso in cui il Fornitore avrà completato l'esecuzione dei Servizi.

Al termine – per qualsiasi causa – del Contratto, il Fornitore dovrà restituire a \_\_\_\_\_ tutti i Dati condivisi, provvedendo altresì alla definitiva cancellazione di ogni copia degli stessi, in qualsiasi formato essi siano (*back-up*, cartacea, su supporto mobile, in *cloud*, etc.), tranne quando diversamente richiesto da norme di legge o in ragione di prescrizioni dettate dal Garante o da altre autorità competenti.

\* \* \* \* \*

Si prega di restituire copia del presente Atto, sottoscritto per accettazione.

Luogo e data

\_\_\_\_\_

\_\_\_\_\_  
**Stazione Appaltante**

\_\_\_\_\_  
**Fornitore**