ALLEGATO A

MANDATO DI AFFIDAMENTO DELLE ATTIVITA' DEL PROCEDIMENTO DI CONSERVAZIONE E NOMINA RESPONSABILE DEL TRATTAMENTO DATI PERSONALI AI SENSI DELL'ART. 28 REG. UE 2016/679 DELLA DITTA MEDAS SRL DI MILANO

Il Dott. MARCO NERATTINI, in qualità di Responsabile della Conservazione (di seguito anche indicato brevemente con l'acronimo "RdC") della Società della Salute Di Firenze anche indicata con "SDS", giusto Decreto del Presidente n. 1 del 25/07/2018 avvalendosi della facoltà conferitagli ai sensi dell'art. 5 co. 2 lett. b) del DPCM del 3 dicembre 2013, di affidare in tutto o in parte lo svolgimento delle proprie attività a terzi certificati come Conservatori accreditati presso l'Agenzia per l'Italia digitale (AgID) che, per competenza ed esperienza, garantiscono la corretta esecuzione delle operazioni ad esse delegate,

PREMESSO CHE

- il servizio prevede la conservazione dei documenti provenienti dai sistemi informatici quali il Gestionale informatico della ditta Project srl che sottopone al sistema di conservazione Scryba i pacchetti di versamento contenenti DAE la cui tipologia è definita nel manuale della conservazione e il Sistema DocLoader della ditta Medas srl che sottopone al sistema di conservazione i pacchetti di versamento contenenti DAE la cui tipologia è definita nel manuale della conservazione.
- il servizio prevede di conservare un numero massimo di 100.000 DAE/anno complessivi.
- il servizio di cui al punto precedente è basato sul "Sistema di conservazione Scryba" della Società Medas srl di Milano.
- ll flusso di conservazione, oggetto del contratto, si riferisce ai documenti sottoposti a Scryba creati a partire dal 01 Ottobre 2018 e conseguentemente il contratto che ha durata triennale, scade il 30 Settembre 2021;
- il RdC della SdS Firenze ha appurato che la Ditta Medas srl (di seguito "MEDAS") dispone della qualità di conservatore accreditato dall'Agenzia per l'Italia Digitale (come risulta dall'elenco dei conservatori accreditati pubblicati sul sito AgID) e constatato dall'esperienza pluriennale presentata

dalla ditta che la stessa ha la struttura e le competenze idonee a gestire il procedimento di conservazione ed in particolare le attività a lei affidate con il presente mandato;

-la ditta Medas Srl, ha preventivamente valutato il ricevimento dell'incarico di affidamento dell'attività di conservazione, ai sensi e per gli effetti del DPCM del 3 dicembre 2013 art. 5 co.2 lett. b), e la possibilità di espletare tali compiti con propri collaboratori;

RICHIAMATO

il provvedimento del Direttore della SdS Firenze n. 34 del 5 settembre 2018, avente per oggetto "Affidamento diretto del servizio di conservazione digitale della documentazione amministrativa elettronica alla Ditta MEDAS s.r.l. dal 01/10/2018 al 30/09(2021 (CIG ZDE24766E9)

AFFIDA

alla ditta Medas srl, **per il periodo che decorre dalla data di sottoscrizione del presente mandato e termina il 30 Settembre 2021**, il servizio di Conservazione in outsourcing. In particolare nella tabella sottostante sono elencate con responsabilità "Medas" le attività a lei affidate. Per maggior chiarezza nella tabella sono state indicate anche le attività gestite direttamente dal RdC della SdS Firenze o delegati.

	ATTIVITA' DEL PROCEDIMENTO DI CONSERVAZIONE	RESPONSABILITA'
1.	Definizione delle caratteristiche dei requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente, al Manuale della Conservazione (MdC) e allegati tra cui in particolare il documento "Accordi di versamento" che specificale tipologie documentarie, i formati dei documenti inviati al sistema di conservazione e i relativi flussi di versamento. (DPCM 3-12-2013 art. 7 co.1 lett. a) e art. 6 co.5)	RdC o delegato
2.	Supporto al RdC per la definizione delle caratteristiche e dei requisiti del sistema di conservazione la cui evidenza è contenuta nel MdC ed allegati.	Medas
3.	Gestione del processo di conservazione con garanzia di mantenere nel tempo la conformità alla normativa vigente (DPCM 3-12-2013 art. 7 co.1 lett. b), nelle modalità indicate nel MdC e declinato nelle seguenti attività:	
	a) acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico (DPCM 3-12-2013 art. 9 co.1 lett. a);	Medas
	b) verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste dal manuale di conservazione e con quanto indicato all'art. 11 (DPCM 3-12-2013 art. 9 co.1 lett. b);	Medas
	c) rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla lettera b) o le regole di presa in carico definite negli Accordi di versamento abbiano evidenziato delle anomalie (DPCM 3-12-2013 art. 9 co.1 lett. c);	Medas

	d) generazione, anche in modo automatico, del rapporto di versamento relativo ad uno o più pacchetti di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo universale coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità descritte nel manuale di conservazione (DPCM 3-12-2013 art. 7 co.1 lett. c e art. 9 co.1 lett.e);	Medas
	e) preparazione, sottoscrizione con firma digitale o firma elettronica qualificata del responsabile della conservazione e gestione del pacchetto di archiviazione sulla base delle specifiche della struttura dati contenute nell'allegato 4 del D.P.C.M. 3 dicembre 2013 e secondo le modalità riportate nel Manuale della conservazione (DPCM 3-12-2013 art. 9 co.1 lett. f);	Medas
	f) scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dalla norma e concordati (DPCM 3-12-2013 art. 9 co.1 lett. k);	RdC
	g) supporto al RdC per l'espletamento della procedura di scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dalla norma e concordati (DPCM 3-12-2013 art. 9 co.1 lett. k);	Medas
4.	Generazione di pacchetti di distribuzione contenenti documenti informatici clinici (DPCM 3-12-2013 art. 7 co.1 lett. d e art. 9 co.1 lett. i). Tale attività viene svolta attraverso specifiche funzionalità dell'applicazione Scryba, accessibili ai soli delegati del RdC dotati di opportune credenziali di accesso.	RdC o delegato
5.	Sottoscrizione con firma digitale o firma elettronica qualificata, ove prevista nel MdC del pacchetto di distribuzione (DPCM 3-12-2013 art. 7 co.1 lett. d e art. 9 co.1 lett. g). Tale attività viene svolta attraverso specifiche funzionalità dell'applicazione Scryba, accessibili ai soli delegati del RdC dotati di opportune credenziali di accesso.	RdC o delegato
6.	Trasmissione dei pacchetti di distribuzione (DPCM 3-12-2013 art. 7 co.1 lett. d e art. 9 co.1 lett. g). Tale attività viene svolta attraverso specifiche funzionalità dell'applicazione Scryba, accessibili ai soli delegati del RdC dotati di opportune credenziali di accesso.	RdC o delegato
7.	Supporto alla generazione, firma e trasmissione dei Pacchetti di Distribuzione.	Medas
8.	Monitoraggio della corretta funzionalità del sistema di conservazione (DPCM 3-12-2013 art. 7 co.1 lett. e) secondo le seguenti attività:	
	a) monitoraggio dell'infrastruttura hardware del sistema di conservazione e reti trasmissione dati, lato server farm remota del conservatore;	Medas
	b) monitoraggio dell'infrastruttura di rete locale geografica e reti trasmissione dati che collegano i sistemi submitter al sistema di conservazione sito remotamente presso la server farm del conservatore, lato SDS;	RdC o delegato
	c) monitoraggio del corretto funzionamento di submission da parte dei sistemi informatici che sottopongono i pacchetti di versamento al sistema di conservazione Scryba, lato SDS e supervisione dell'attività del conservatore relativa alla ricezione dei pacchetti da parte di Scryba;	RdC o delegato
	d) manutenzione e aggiornamento del SW del sistema di conservazione Scryba;	Medas

	e) monitoraggio dei flussi documentali e rendicontazione periodica	Medas
9.	Verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi secondo quanto previsto dal MdC e allegati (DPCM 3-12-2013 art.7 co.1 lett. f).	RdC o delegato
10.	Supporto alla verifica periodica cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi	Medas
11.	Adozione di misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e ove necessario per ripristinare la corretta funzionalità (DPCM 3-12-2013 art.7 co.1 lett. g). Le evidenze sono date dalle notifiche di anomalia inviate al RdC a mezzo PEC.	Medas
12.	Attività di duplicazione o copia (riversamento) dei documenti informatici in relazione all'evolversi del contesto tecnologico secondo quanto previsto dal MdC e allegati (DPCM 3-12-2013 art. 7 co.1 lett. h).	RdC o delegato
13.	Supporto alla duplicazione o copia (riversamento) dei documenti informatici	Medas
14.	Adozione di misure necessarie per la sicurezza fisica e logica del sistema di conservazione (DPCM 3-12-2013 art. 7 co.1 lett. i e art.12 co.1), la cui evidenza è data dalla certificazione ISO 27001 e dal Piano di sicurezza del conservatore Medas.	Medas
15.	Assicurare la presenza di un pubblico ufficiale nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite (DPCM 3-12-2013 art. 7 co.1 lett. j).	RdC o delegato
16.	Assicurare agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza (DPCM 3-12-2013 art. 7 co.1 lett. k).	
	a) assicurare agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;	RdC o delegato
	b) supporto al RdC in caso di attività di verifica e vigilanza;	Medas
	c) assicurare agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza per quanto riguarda aspetti specifici delle attività affidate a Medas.	Medas
17.	Predisporre del Manuale di conservazione di cui all'art. 8 e aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti (DPCM 3-12-2013 art. 7 co.1 lett. m).	RdC o delegato
18.	Supporto alla predisposizione del Manuale di conservazione e aggiornamento periodico.	Medas

CONDIZIONI DELL'AFFIDAMENTO

1. MEDAS accettando l'incarico di affidamento assume, in ottemperanza all'art. 6 co. 8 del D.P.C.M. 3/12/2013, anche il ruolo di responsabile del trattamento dei dati come previsto dall'art. 28 del Regolamento UE 2016/679 sottoscrivendo, per l'effetto, il sotto esteso atto di nomina.
2. Nello svolgimento delle attività, MEDAS dovrà ottemperare a tutti i regolamenti e direttive dell'AZIENDA, oltre che a tutta la normativa vigente.

3. MEDAS é tenuta a segnalare tempestivamente tramite opportune relazioni, eventuali malfunzionamenti o anomalie del procedimento di conservazione rispetto a quanto definito nel Manuale di Conservazione e alle attività a lei affidate.
4. MEDAS dovrà periodicamente redigere e consegnare al RdC delle relazioni relative alle attività svolte per consentire al RdC di esercitare la funzione di controllo.
5. MEDAS sarà responsabile della corretta e tempestiva esecuzione delle attività a lei affidate e delle eventuali ulteriori istruzioni/direttive del RdC purché comunicate per iscritto e pertinenti all'oggetto contrattuale.
6. MEDAS sarà responsabile per qualsiasi atto che esorbiti dal presente incarico.
7. MEDAS rende disponibili al RdC, contestualmente alla sottoscrizione per accettazione del presente incarico, l'elenco dei suoi collaboratori, aggiornandolo quando necessario, che svolgeranno le attività affidate, individuati quali incaricati del trattamento ai sensi dell'art. 30 del Codice in materia di protezione dei dati personali.
8. La responsabilità generale inerente la conservazione dei documenti prodotti dalla AZIENDA e la responsabilità diretta e indiretta derivante da dovere di direzione e vigilanza sull'affidatario rimarranno in capo al RdC.

FIRENZE IL …… **Dott. Marco Nerattini**

Responsabile della Conservazione SdS Firenze

DICHIARAZIONE DI ACCETTAZIONE DEL MANDATO DI AFFIDAMENTO

Il dott. Umberto Ferri, in qualità di legale rappresentante della società Medas srl e responsabile del servizio di conservazione, dichiara di accettare il presente mandato e che le attività affidate verranno svolte dai seguenti collaboratori:

- FERRI Umberto Responsabile del servizio di conservazione
- SAVOLDI Matteo Responsabile della funzione archivistica di conservazione
- TOMBOLATO Paolo Responsabile del trattamento dei dati personali
- TOMBOLATO Paolo Responsabile della sicurezza dei sistemi per la conservazione
- BASSANINI Fabio Responsabile dei sistemi informativi per la conservazione

- TOMBOLATO Aldino Responsabile dello sviluppo e della manutenzione del sistema di conservazione

Medas è tenuta a comunicare ad AgID eventuali variazioni dei Responsabili del Sistema di Conservazione e ad aggiornare il relativo Manuale della conservazione del conservatore disponibile sul sito www.agid.gov.it nella sezione "Conservatori".

Amministratori di sistema e tecnici esperti

Ai sensi del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento (modificato con Provvedimento del 25 giugno 2009) gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite sono riportati in un documento interno a Medas, mantenuto aggiornato e disponibile in caso di accertamenti da parte del Garante.

Medas inoltre si avvale di tecnici esperti, formalmente designati, i quali possono intervenire sugli impianti in fase di installazione, configurazione, risoluzione di problemi, incidenti o in fase di exit (DS01 – Piano della Sicurezza – ISO 27001). L'elenco è un documento interno a Medas costantemente tenuto aggiornato e disponibile in caso di accertamenti da parte del Garante.

Milano, ….

Dott. Umberto Ferri

Presidente CDA Medas srl e

Responsabile del servizio di conservazione

ATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO DATI AI SENSI DELL'ART. 28 DEL REGOLAMENTO UE 2016/679

TRA

la Società della Salute di Firenze, in persona del Direttore dott. Marco Nerattini, codice fiscale NRTMRC63M05A558D domiciliato per la carica presso la sede della SDS sita in Viale Giovine Italia n. 1/1, Partita IVA/codice fiscale 94117300486, di seguito anche come "SDS",

E

La MEDAS S.R.L., partita IVA/codice fiscale 02398390217, con sede legale in Via Benadir, 14 nella persona di UMBERTO FERRI nato a BERGAMO il 19/06/1963, in qualità di Presidente del CDA e legale rappresentante, domiciliato per la carica presso la sede della società stessa, di seguito anche come "Responsabile" ,

congiuntamente anche come le "Parti"

Premesso che:

- l'art. 28, par. 3, del Regolamento UE n. 2016/679 (General Data Protection Regulation), di seguito anche GDPR, prevede che i trattamenti effettuati per conto del Titolare del trattamento (SDS) da parte di un Responsabile del trattamento siano regolati da un contratto o da altro atto giuridico che determini la materia del trattamento, la durata, la natura e la finalità, il tipo di dati personali trattati e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento;

• l'art. 28 del Regolamento (UE) n. 2016/679 riconosce, altresì, al Titolare del trattamento la facoltà di avvalersi di uno o più responsabili del trattamento dei dati, che abbiano esperienza, capacità, conoscenza per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del regolamento, anche relativamente al profilo della sicurezza;

- la SDS ha affidato alla ditta Medas mediante provvedimento del Direttore Generale n. 34/2018 avente ad oggetto "AFFIDAMENTO DEL SERVIZIO DI CONSERVAZIONE";

• ai fini del rispetto della normativa, ciascuna persona che tratta dati personali deve essere autorizzata e istruita in merito agli obblighi normativi per la gestione dei suddetti dati durante lo svolgimento delle proprie attività;

• il Titolare ha affidato alla società MEDAS s.r.l. (di seguito "Responsabile" o "Fornitore", e congiuntamente con il Titolare, "Parti") il SERVIZIO DI CONSERVAZIONE DI DOCUMENTI provenienti dai seguenti sistemi informatici:

- Gestionale informatico della ditta Project srl che sottopone al sistema di conservazione Scryba i pacchetti di versamento contenenti DAE la cui tipologia è definita nel manuale della conservazione;
- Sistema DocLoader della ditta Medas srl che sottopone al sistema di conservazione i pacchetti di versamento contenenti DAE la cui tipologia è definita nel manuale della conservazione;

• tenuto conto delle attività di trattamento necessarie e/o opportune per dare esecuzione agli obblighi concordati tra le Parti, previa valutazione di quanto imposto dal Regolamento (UE) n. 2016/679, il Titolare ha ritenuto che il Responsabile presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a soddisfare i requisiti del Regolamento (UE) n. 2016/679 ed a garantire la tutela dei diritti e le libertà degli interessati coinvolti nelle suddette attività di trattamento;

• tale nomina non comporta alcuna modifica della qualifica professionale del Responsabile e/o degli obblighi concordati tra le Parti.

Tutto quanto sopra premesso

la SDS, in qualità di Titolare del Trattamento, con la presente

NOMINA

in attuazione alle disposizioni del Regolamento del Parlamento Europeo n. 2016/679/UE (nel seguito "GDPR"),

la società MEDAS S.R.L. RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI ai sensi dell'art. 28 del GDPR per il trattamento dei dati personali di cui è Titolare l'Azienda e di cui il Responsabile può venire a conoscenza nell'esercizio delle attività espletate per conto del Titolare relativamente al servizio di conservazione citato in premessa affidato dal Titolare al Responsabile.

Articolo 1 - 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/convenzione.

Articolo 2 - 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 del GDPR;

• dati rientranti nelle categorie "particolari" di dati personali in particolare di carattere sanitario (p.e. 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 del GDPR;

• dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza di cui all'art. 10 GDPR.

Articolo 3 - Categorie di interessati cui si riferiscono i dati trattati

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

- pazienti/utenti;

- familiari dei pazienti/utenti;

- personale che opera a qualsiasi titolo e/o in forza di qualsivoglia atto all'interno della SDS (es. dipendenti, tirocinanti, interinale, ecc.);

Articolo 4 - Obbligo alla riservatezza

Trattandosi di dati personali e/o c.d. sensibili, il responsabile e i propri dipendenti e collaboratori sono tenuti alla assoluta riservatezza analogamente al segreto professionale e, così come previsto dal D.P.R. 62/2013 che il Responsabile si è impegnato a rispettare, al segreto d'ufficio, e comunque a trattare i dati in materia confidenziale e riservata, evitando l'eventuale comunicazione e/o conoscenza da parte di soggetti non autorizzati.

Articolo 5 – Disponibilità e uso dei dati

Qualunque sia la finalità e la durata del trattamento effettuato da parte del Responsabile:

- i dati non potranno essere venduti o ceduti, in tutto o in parte, ad altri soggetti e dovranno essere restituiti alla conclusione o revoca dell'incarico, o in qualsiasi momento il Titolare ne faccia richiesta;
- il Responsabile si impegna a non vantare alcun diritto sui dati e sui materiali presi in visione.

Coerentemente con quanto prescritto dal GDPR, è esplicitamente fatto divieto al Responsabile di inviare messaggio pubblicitari, commerciali e promozionali, e comunque di contattare gli "interessati" per finalità diverse da quelle nel presente atto.

Articolo 6 - Cessazione del trattamento

Una volta cessati i trattamenti oggetto del Contratto, salvo rinnovo, il Responsabile si impegna a restituire al Titolare i dati personali acquisiti, pervenuti a sua conoscenza o da questi elaborati in relazione all'esecuzione del servizio prestato e, solo successivamente, si impegna a cancellarli dai propri archivi oppure distruggerli, ad eccezione dei casi in cui i dati debbano essere conservati in virtù di obblighi di legge. Resta inteso che la dimostrazione delle ragioni che giustificano il protrarsi degli obblighi di conservazione è a carico del Titolare e che le uniche finalità perseguibili con tali dati sono esclusivamente circoscritte a rispondere a tali adempimenti normativi.

Articolo 7 - Validità e Revoca della nomina

La presente nomina avrà validità per tutta la durata del rapporto giuridico intercorrente tra le Parti e potrà essere revocata a discrezione del Titolare.

La presente nomina non costituisce aggravio in capo al Responsabile, rientrando la medesima negli obblighi normativi che regolano i rapporti con il Titolare sotto il profilo della protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Articolo 8 - Sub-responsabili

Il Responsabile del trattamento non potrà ricorrere ad altri Responsabili senza la preventiva autorizzazione specifica del Titolare del trattamento. In tale ipotesi il Responsabile dovrà inviare, a mezzo P.E.C., circostanziata e motivata richiesta al Titolare che avrà la facoltà di consentire o meno detta nomina.

Ai sensi dell'art. 28, par. 4 del GDPR, fermo restando quanto previsto al precedente paragrafo, quando un responsabile del trattamento ricorre a un altro responsabile del trattamento, per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR.

Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

Articolo 9 - Designazione e autorizzazione degli incaricati

Il Responsabile del trattamento garantisce la puntuale individuazione dei soggetti operanti a qualsiasi titolo nella propria organizzazione quali soggetti autorizzati al trattamento.

In particolare, il Responsabile del trattamento si impegna a consentire l'accesso e il trattamento dei dati personali solo a personale debitamente formato e specificamente designato anche ai sensi dell'art. 2-quaterdecies del D.Lgs 196/2003 e s.m.i.

Il Responsabile si impegna ad effettuare per iscritto le nomine e limitare l'accesso e il trattamento ai soli dati personali necessari per lo svolgimento delle attività oggetto della Convenzione/Contratto.

Il personale autorizzato dovrà ricevere idonea e specifica formazione in relazione al rispetto delle misure organizzative e tecniche, in particolare alle misure di sicurezza adottate, adeguate ad assicurare la tutela dei dati personali trattati nel rispetto delle previsioni normative e della prassi in materia.

Nello specifico il Responsabile:

• individua le persone autorizzate al trattamento dei dati impartendo loro, per iscritto, istruzioni dettagliate in merito alle operazioni consentite e alle misure di sicurezza da adottare in relazione alle criticità dei dati trattati;

• vigila regolarmente sulla puntuale applicazione da parte delle persone autorizzate di quanto prescritto, anche tramite verifiche periodiche;

• garantisce l'adozione dei diversi profili di autorizzazione delle persone autorizzate, in modo da limitare l'accesso ai soli dati necessari alle operazioni di trattamento consentite rispetto alle mansioni svolte;

• verifica periodicamente la sussistenza delle condizioni per la conservazione dei profili di autorizzazione di tutte le persone autorizzate, modificando tempestivamente detto profilo ove necessario (es. cambio di mansione);

• cura la formazione e l'aggiornamento professionale delle persone autorizzate che operano sotto la sua responsabilità circa le disposizioni di legge e regolamentari in materia di tutela dei dati personali.

Il Responsabile, su richiesta, invia al Titolare del trattamento a mezzo P.E.C. l'elenco nominativo con specifica evidenza delle relative mansioni dei soggetti autorizzati al trattamento dei dati personali svolti per suo conto e nell'ambito della Convenzione/Contratto.

Articolo 10 – Responsabile della protezione dei Dati

Il Responsabile – ove tale obbligo si applichi anche al Responsabile stesso in base alle disposizioni dell'art. 37 del GDPR – si impegna a nominare e comunicare al Titolare il nominativo e i dati di contatto del Responsabile della Protezione dei Dati.

Articolo 11 - Diritti degli interessati

Premesso che l'esercizio dei diritti riconosciuti all'interessato ai sensi degli artt. 15 e seguenti del GDPR sarà gestito direttamente dal Titolare, il Responsabile si rende disponibile a collaborare con il Titolare stesso fornendogli tutte le informazioni necessarie a soddisfare le eventuali richieste ricevute in tal senso.

Il Responsabile si impegna ad assistere il Titolare con misure tecniche e organizzative adeguate al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato.

In particolare, il Responsabile dovrà comunicare al Titolare, senza ritardo e comunque non oltre le 72 ore dalla ricezione, le istanze eventualmente ricevute e avanzate dagli interessati in virtù dei diritti previsti dalla vigente normativa (es. diritto di accesso, ecc.) e a fornire le informazioni necessarie al fine di consentire al Titolare di evadere le stesse entro i termini stabiliti dalla normativa.

Articolo 12 - Registro dei trattamenti

Il Responsabile – ove tale obbligo si applichi anche al Responsabile stesso in base alle disposizioni del comma 5 dell'art. 30 del GDPR - mantiene un registro (in forma scritta e/o anche in formato elettronico) di tutte le categorie di attività relative al trattamento svolte per conto del Titolare, contenente:

• il nome e i dati di contatto del Responsabile e/o dei suoi Sub – Responsabili;

• le categorie dei trattamenti effettuati per conto del Titolare;

• ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49 del GDPR, la documentazione delle garanzie adeguate adottate;

• ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art. 32, par. 1 del GDPR.

Il Responsabile garantisce, inoltre, di mettere a disposizione del Titolare e/o dell'Autorità di controllo che ne dovessero fare richiesta, il suddetto registro dei trattamenti.

Il Responsabile si impegna a coadiuvare il Titolare nella redazione del proprio Registro delle attività di trattamenti, segnalando anche, per quanto di propria competenza, eventuali modifiche da apportare al Registro.

Articolo 13 - Sicurezza dei dati personali

Il Responsabile è tenuto, ai sensi dell'art. 32 del GDPR, ad adottare le necessarie e adeguate misure di sicurezza (eventualmente anche ulteriori rispetto a quelle nel seguito indicate) in modo tale da ridurre al minimo i rischi di distruzione accidentale o illegale, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non consentito ai dati personali trasmessi, conservati o comunque trattati, o il trattamento non conforme alle finalità della raccolta.

Il Responsabile fornisce al titolare l'elenco delle adeguate misure di sicurezza adottate.

Articolo 14 - Sicurezza e Amministrazione del Sistema (ADS)

Il Responsabile fornirà al Titolare la lista nominativa degli ADS, con questi intendendo le persone fisiche che svolgono per conto del Responsabile ed in esecuzione dei compiti concordati ed affidati dal Titolare, attività di gestione e manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i software complessi che trattano dati del Titolare, le reti locali e gli apparati di sicurezza di quest'ultimo, o comunque che possano intervenire sulle misure di sicurezza a presidio dei medesimi dati. Con riferimento ai soggetti individuati, il Responsabile deve comunicare rispetto ad ognuno i compiti e le operazioni svolte.

Articolo 15 - Compiti e istruzioni per il Responsabile

Il Responsabile ha il potere ed il dovere di trattare i dati personali indicati nel rispetto della normativa vigente, attenendosi sia alle istruzioni di seguito fornite, sia a quelle che verranno rese note dal Titolare mediante procedure e/o comunicazioni specifiche.

Il Responsabile dichiara espressamente di comprendere ed accettare le istruzioni di seguito rappresentate e si obbliga a porre in essere, nell'ambito dei compiti contrattualmente affidati, tutti gli adempimenti prescritti dalla normativa di riferimento in materia di tutela dei dati personali al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato e di trattamento non consentito o non conforme alla raccolta.

Articolo 16 - Modalità di trattamento e requisiti dei dati personali

Il Responsabile si impegna:

• a trattare direttamente, o per il tramite dei propri dipendenti, collaboratori esterni, consulenti, etc. – specificamente designati incaricati del trattamento - i dati personali del Titolare, per le sole finalità connesse allo svolgimento delle attività previste dal Contratto/Convenzione, in modo lecito e secondo correttezza, nonchè nel pieno rispetto delle disposizioni previste dal GDPR, nonchè, infine, dalle presenti istruzioni;

• non divulgare o rendere noti a terzi - per alcuna ragione ed in alcun momento, presente o futuro ed anche una volta cessati i trattamenti oggetto del Contratto/Convenzione - i dati personali ricevuti dal Titolare o pervenuti a sua conoscenza in relazione all'esecuzione del servizio prestato, se non

previamente autorizzato per iscritto dal Titolare, fatti salvi eventuali obblighi di legge o ordini dell'Autorità Giudiziaria e/o di competenti Autorità amministrative;

• collaborare con il Titolare per garantire la puntuale osservanza e conformità alla normativa in materia di protezione dei dati personali;

• dare immediato avviso al Titolare in caso di cessazione dei trattamenti concordati;

• non creare banche dati nuove senza espressa autorizzazione del Titolare, fatto salvo quando ciò risulti strettamente indispensabile ai fini dell'esecuzione degli obblighi assunti;

• in caso di ricezione di richieste specifiche avanzate dall'Autorità Garante per la protezione dei dati personali o altre autorità, a coadiuvare il Titolare per quanto di sua competenza;

• segnalare eventuali criticità al Titolare che possono mettere a repentaglio la sicurezza dei dati, al fine di consentire idonei interventi da parte dello stesso;

• coadiuvare, su richiesta, il Titolare ed i soggetti da questo indicati nella redazione della documentazione necessaria per adempiere alla normativa di settore, con riferimento ai trattamenti di dati effettuati dal Responsabile in esecuzione delle attività assegnate.

Articolo 17 - Istruzioni specifiche per il trattamento dati particolari e/o relativi a condanne penali e reati

Il Responsabile deve:

• verificare la corretta osservanza delle misure previste dal Titolare in materia di archiviazione nel rispetto di quanto previsto dal precedente articolo 6, potendo derivare gravi conseguenze da accessi non autorizzati alle informazioni oggetto di trattamento;

• prestare particolare attenzione al trattamento dei dati personali rientranti nelle categorie particolari e/o relative a condanne penali o reati degli interessati conosciuti, anche incidentalmente, in esecuzione dell'incarico affidato, procedendo alla loro raccolta e archiviazione solo ove ciò si renda necessario per lo svolgimento delle attività di competenza e istruendo in tal senso le persone autorizzate che operano all'interno della propria struttura;

• conservare, nel rispetto di quanto previsto dal precedente articolo 6, la documentazione contenente dati particolari e/o relativi a condanne penali e reati adottando misure idonee al fine di evitare accessi non autorizzati ai dati, distruzione, perdita e/o qualunque violazione di dati personali;

• vigilare affinchè i dati personali degli interessati vengano comunicati solo a quei soggetti preventivamente autorizzati dal Titolare (ad esempio a propri fornitori e/o subfornitori) che presentino garanzie sufficienti secondo le procedure di autorizzazione disposte e comunicate dal Titolare. Sono altresì consentite le comunicazioni richieste per legge nei confronti di soggetti pubblici;

• sottoporre preventivamente al Titolare, per una sua formale approvazione, le richieste di dati da parte di soggetti esterni;

• non diffondere i dati personali, particolari e/o relativi a condanne penali e reati degli interessati;

• segnalare eventuali criticità nella gestione della documentazione contenente dati personali, particolari e/o relativi a condanne penali e reati al fine di consentire idonei interventi da parte del Titolare.

Articolo 18 – Violazione dei dati

Il Responsabile si impegna a notificare al Titolare, senza ingiustificato ritardo dall'avvenuta conoscenza, e comunque entro 36 ore, con comunicazione da inviarsi all'indirizzo PEC del titolare, ogni violazione dei dati personali (*data breach*) fornendo, altresì:

• la descrizione della natura della violazione e l'indicazione delle categorie dei dati personali e il numero approssimativo di interessati coinvolti;

• comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

• la descrizione delle probabili conseguenze;

• la descrizione delle misure adottate o di cui dispone per porre rimedio alla violazione o, quantomeno, per attenuarne i possibili effetti negativi.

Fermo quanto sopra previsto, il Responsabile si impegna a prestare ogni più ampia assistenza al Titolare al fine di consentirgli di assolvere agli obblighi di cui agli artt. 33 - 34 del GDPR.

Una volta definite le ragioni della violazione, il Responsabile di concerto con il Titolare e/o altro soggetto da quest'ultimo indicato, su richiesta, si attiverà per implementare nel minor tempo possibile

tutte le misure di sicurezza fisiche e/o logiche e/o organizzative atte ad arginare il verificarsi di una nuova violazione della stessa specie di quella verificatasi, al riguardo anche avvalendosi dell'operato di subfornitori.

Articolo 19 - Valutazione di impatto e consultazione preventiva

Con riferimento agli artt. 35 e 36 del GDPR, il Responsabile si impegna, su richiesta, ad assistere il Titolare nelle attività necessarie all'assolvimento degli obblighi previsti dai succitati articoli, sulle base delle informazioni in proprio possesso, in ragione dei trattamenti svolti in qualità di Responsabile del trattamento, ivi incluse le informazioni relative agli eventuali trattamenti effettuati dai Sub - Responsabili.

Articolo 20 - Trasferimento dei dati personali

Il Responsabile del trattamento si impegna a circoscrivere gli ambiti di circolazione e trattamento dei dati personali (es. memorizzazione, archiviazione, conservazione dei dati sui propri server) ai Paesi facenti parte dell'Unione Europea, con espresso divieto di trasferirli in Paesi extra UE che non garantiscano (o in assenza di) un livello adeguato di tutela, ovvero, in assenza di strumenti di tutela previsti dal Regolamento UE 2016/679 CAPO V.

Articolo 21 - Attività di audit

Il Responsabile si impegna a mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di sicurezza descritti nel presente documento e, in generale, il rispetto delle obbligazioni assunte in forza del presente atto e del GDPR, consentendo e, su richiesta, contribuendo alle attività di audit, comprese le ispezioni, realizzate dal Titolare o da altro soggetto da esso incaricato.

Qualora il Titolare rilevasse comportamenti difformi a quanto prescritto dalla normativa in materia nonchè dalle disposizioni contenute nei provvedimenti del Garante per la protezione dei dati personali, provvederà a darne comunicazione al Responsabile, senza che ciò possa far venire meno l'autonomia dell'attività di impresa del Responsabile ovvero possa essere qualificato come ingerenza nella sua attività.

Articolo 22 - Ulteriori istruzioni

Il Responsabile comunica tempestivamente al Titolare qualsiasi modificazione di assetto organizzativo o di struttura proprietaria che dovesse intervenire successivamente all'affidamento dell'incarico, affinchè il Titolare possa accertare l'eventuale sopravvenuta mancanza dei requisiti previsti dalla vigente normativa o il venir meno delle garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate per il corretto trattamento dei dati oggetto della presente nomina.

Il Responsabile informa prontamente il Titolare delle eventuali carenze, situazioni anomale o di emergenza rilevate nell'ambito del servizio erogato - in particolare ove ciò possa riguardare il trattamento dei dati personali e le misure di sicurezza adottate dal Responsabile - e di ogni altro episodio o fatto rilevante che intervenga e che riguardi comunque l'applicazione del GDPR (ad es. richieste del Garante, esito delle ispezioni svolte dalle Autorità, ecc.) o della normativa nazionale ancorchè applicabile.

Articolo 23 - Codici di Condotta e Certificazioni

Il Responsabile si impegna a comunicare al Titolare l'adesione a codici di condotta approvati ai sensi dell'art. 40 del GDPR e/o l'ottenimento di certificazioni che impattano sui servizi offerti al Titolare, intendendo anche quelle disciplinate dall'art. 42 del GDPR.

Articolo 24 – Norme finali e responsabilità

Il Titolare, poste le suddette istruzioni e fermi i compiti sopra individuati, si riserva, nell'ambito del proprio ruolo, di impartire per iscritto eventuali ulteriori istruzioni che dovessero risultare necessarie per il corretto e conforme svolgimento delle attività di trattamento dei dati collegate all'accordo vigente tra le Parti, anche a completamento ed integrazione di quanto sopra definito.

Il Responsabile dichiara sin d'ora di mantenere indenne e manlevato il Titolare da qualsiasi danno, onere, spesa e conseguenza che dovesse derivare al Titolare stesso a seguito della violazione, da parte del Responsabile o di suoi Sub – Responsabili, degli impegni relativi al rispetto della disciplina in materia di protezione dei dati personali o delle istruzioni contenute nei relativi atti di nomina anche in seguito a comportamenti addebitabili ai loro dipendenti, rappresentanti, collaboratori a qualsiasi titolo.

_____, lì _____

p. SDS Firenze _____

p. Medas r..l. Rappresentante legale_____