ATTO DI NOMINA A RESPONSABILE ESTERNO DEL TRATTAMENTO DATI PERSONALI TENUTO CONTO DELLA NORMATIVA PRIVACY VIGENTE

Premesso che

- a decorrere dal 14 aprile 2016 è in vigore il Regolamento (UE) n. 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (d'ora innanzi anche "GDPR" o "Regolamento);
- la normativa privacy riconosce 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;
- per "trattamento", ai sensi dell'art. 4 punto 2 del Regolamento, si intende "*qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati*";
- per "dati personali", ai sensi dell'art. 4 punto 1 del Regolamento, si intende "*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)*"; *altresì si considera identificabile "la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*";
- 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 mansioni;
- l'Istituto QUADRIFOR, con sede legale in Roma, via Cristoforo Colombo n. 137 (di seguito "Titolare") con contratto vigente ha affidato e/o affiderà, attraverso accordi contrattuali, a _____. P.Iva _____ - C.F. _____, sede legale e Amministrativa: _____, (di seguito "Responsabile", e congiuntamente con il Titolare, "Parti"), i servizi di assistenza, gestione e manutenzione del Sistema Informativo di Quadrifor e della relativa infrastruttura tecnica, attività che comportano inevitabilmente il trattamento di dati personali di titolarità dell'Istituto medesimo e dei soggetti interessati che con esso entrano in contatto, trattando all'uopo i dati personali dei partecipanti forniti dal Titolare;
- 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 stesso ed a garantire la tutela dei diritti e le libertà degli interessati coinvolti nelle attività di trattamento inerenti all'espletamento dei suddetti servizi;

- tale nomina non comporta alcuna modifica della qualifica e/o delle prestazioni professionali contrattualmente stabilite.

Tutto quanto sopra premesso

L'Istituto Quadrifor, in persona del Presidente e Legale Rappresentante Francesca Mandato, con sede in Roma, Via Marco e Marcelliano, 45, Cod. Fisc. 97115220580, in qualità di Titolare del Trattamento, con la presente nomina _____, in persona del legale rappresentante, con sede legale in _____, P.Iva _____ - C.F. _____.

RESPONSABILE ESTERNO

per il trattamento dei dati personali di cui è Titolare l'Istituto Quadrifor e di cui può venire a conoscenza nell'esercizio delle attività espletate in esecuzione del vigente contratto di servizi (o dei futuri eventuali accordi contrattuali).
Il Responsabile ha il potere e dovere di trattare i dati personali indicati nella tabella sottostante nel rispetto della normativa vigente, attenendosi sia alle istruzioni di seguito fornite, sia a quelle che verranno rese note mediante procedure e/o comunicazioni specifiche.

Autorizzazione al trattamento: categorie di interessati e finalità di trattamento	• Dati personali dei dipendenti di Quadrifor per la gestione dell'office automation e della posta elettronica • Dati personali dei Quadri iscritti per la gestione dei sistemi a supporto del rapporto amministrativo, della formazione e delle ricerche statistiche • Dati personali dei referenti e dei legali rappresentanti delle aziende iscritte per la gestione dei sistemi a supporto del rapporto amministrativo, della formazione e delle ricerche statistiche • Dati personali dei docenti, dei referenti e dei legali rappresentanti delle scuole e società di formazione per la gestione dei sistemi a supporto della formazione • Dati personali di collaboratori amministrativi Quadrifor, per dare esecuzione alle fasi commerciali ed amministrative relative al contratto • Ogni altro dato personale derivante dalla gestione del sistema informativo di Quadrifor
Validità e Revoca della nomina	La presente nomina inizierà a decorrere dalla data di vigenza degli accordi contrattuali sottoscritti, ha validità per tutta la durata del rapporto giuridico intercorrente tra le parti, potrà essere revocata a discrezione del Titolare e

	non costituisce ulteriore incarico, rientrando negli obblighi normativi imposti dalla vigente disciplina in materia di Privacy. La perdita da parte del Responsabile dei requisiti di cui all'art. 28 e al considerando 81 del Regolamento(UE) n. 2016/679 e s.m.i. consentirà al Titolare di esercitare il diritto di revoca. L'esercizio del diritto o della facoltà di revoca, da parte del Titolare – senza obbligo di corresponsione di alcun risarcimento e/o indennità al Responsabile e fatto salvo quanto meglio specificato nel rapporto presupposto – avverrà mediante invio di una semplice comunicazione contenente la manifestazione di volontà di revoca.
Istruzioni generali per il trattamento dati; il Responsabile deve:	**1.** collaborare con il Titolare per garantire la puntuale osservanza e conformità alla normativa in materia di protezione dei dati personali; **2.** individuare e autorizzare le persone al trattamento che operino sotto la propria direzione e/o autorità; dare loro le istruzioni idonee per il trattamento dei dati personali ad essi affidato, nel rispetto e nell'osservanza dei limiti e delle indicazioni fornite dal Titolare, e procedere alla loro eventuale revoca; **3.** vigilare affinché le persone autorizzate rispettino le istruzioni impartite e le misure tecniche e organizzative predisposte dal Titolare; si precisa che l'obbligo di vigilanza in capo al Responsabile è da intendersi funzionale allo svolgimento delle ordinarie attività lavorative, e pertanto non si risolve in un aggravio ulteriore a carico di questi; **4.** provvedere a rilasciare le informative ex art. 13 del Regolamento (UE) n. 2016/679 e s.m.i. secondo le specifiche istruzioni date dal Titolare, istruendo a tal fine anche le persone autorizzate, qualora coinvolte direttamente; **5.** richiamare le persone autorizzate al rispetto delle istruzioni impartite, nei casi più gravi, segnalando al Titolare l'eventuale mancato rispetto; **6.** porre in essere per tutta la durata del Contratto, adeguate misure tecniche e organizzative, incluse quelle riportate nella sezione "Misure di sicurezza" di questo documento, ai sensi dell'articolo 32 del GDPR, per proteggere la riservatezza dei Dati Personali e per proteggere i Dati Personali contro la distruzione accidentale o illecita, la perdita accidentale, l'alterazione, la divulgazione o l'accesso non autorizzati; **7.** verificare che le misure di sicurezza, tecniche e organizzative, predisposte dal Titolare siano rispettate dalle persone autorizzate che operano sotto la sua autorità; **8.** in caso di richieste di esercizio da parte dell'interessato dei diritti di cui agli artt. 15, 16, 17, 18, 20 e 21 Regolamento (UE) n. 2016/679 e s.m.i., ricevute direttamente o indirettamente da soggetti interessati, provvedere

	all'immediato invio al Titolare al fine di consentire al medesimo un riscontro nei termini di legge; resta inteso che il Responsabile dovrà inviare detta comunicazione provvedendo ad allegare tutte le informazioni richieste, al fine di consentire una risposta esaustiva; **9.** dare immediato avviso al Titolare nel caso di nuovi trattamenti e/o della cessazione di quelli già esistenti; **10.** conservare i dati oggetto di trattamento secondo le *policy* di *data retention* definite dal Titolare; **11.** in caso di ricezione di richieste specifiche avanzate dall'Autorità Nazionale per la protezione dei dati personali o altre autorità, il Responsabile dovrà seguire le istruzioni contenute nella procedura specifica e comunque coadiuvare il Titolare, per quanto di sua competenza; **12.** verificare periodicamente la corretta storicizzazione dei consensi prestati dagli interessati per il trattamento dati e per i trattamenti ricadenti nell'ambito della funzione svolta; **13.** segnalare eventuali criticità al Titolare che possono mettere a repentaglio la sicurezza dei dati, al fine di consentire idonei interventi da parte dello stesso; **14.** coadiuvare il Titolare ed il DPO, segnalando per quanto di propria competenza rispetto all'incarico svolto, la necessità svolgere una DPIA; **15.** coadiuvare il Titolare ed il DPO nella redazione del Registro delle categorie dei trattamenti, segnalando anche, per quanto di propria competenza, eventuali modifiche da apportare al Registro; **16.** verificare periodicamente o su indicazione del Titolare e/o del DPO che i trattamenti posti in essere rispettino le condizioni di liceità previste dall'art. 6 Regolamento (UE) n. 2016/679; **17.** prestare particolare attenzione al trattamento dei dati personali rientranti nelle categorie particolari conosciuti, anche incidentalmente, nell'esercizio delle proprie mansioni, 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 dell'area; **18.** valutare l'eventuale legittimità delle richieste di dati da parte di soggetti esterni, sottoponendo eventuali dubbi direttamente al Titolare/DPO. Al Responsabile è richiesta, in ogni caso, una condotta propositiva in tema di *data protection*, esplicantesi in suggerimenti o/o proposte di modifica sulle misure adottate dal Titolare in adempimento al Regolamento (UE) n. 2016/679 e s.m.i..

Istruzioni specifiche per il trattamento dei dati nella funzione di riferimento; il Responsabile deve:	**19.** segnalare eventuali criticità nella gestione della documentazione contenente dati personali all'interno dell'area di riferimento al fine di consentire idonei interventi da parte del Titolare; **20.** limitare il trattamento dei dati di interesse alle finalità strettamente legate all'ambito di propria competenza, evitando trattamenti eccedenti; **21.** fornire le istruzioni specifiche a coloro che operano a contatto diretto con gli interessati nello svolgimento del trattamento affinché usino ogni più utile cautela nella gestione dei dati ricevuti e della loro raccolta, nonché della volontà degli interlocutori; **22.** prestare particolare attenzione affinché i dati personali siano trattati all'interno dell'area di riferimento per dar corso al rapporto instaurato ed evitare che soggetti non autorizzati possano accedervi, segnalando eventuali criticità legate all'archiviazione e conservazione della documentazione che dovesse nel caso riscontrare, anche su segnalazione degli altri responsabili dell'area; **23.** verificare che i consensi eventualmente raccolti per il trattamento dati siano stati registrati correttamente; **24.** curare la riservatezza delle informazioni ricevute e veicolate attraverso gli strumenti messi a disposizione del Titolare anche nel caso in cui siano scambiate tra le diverse aree e/o i diversi uffici aziendali; **25.** non ricorrere a sub-responsabili del trattamento se non autorizzati da Quadrifor; **26.** garantire che la propria società e i propri eventuali Sub-responsabili hanno adottato misure tecniche e organizzative in grado di identificare prontamente eventuali violazioni di dati personali e fornire le informazioni e compiere le attività di cui la presente clausola, secondo le modalità e la tempistica ivi indicata.
Processi e procedure	Il responsabile deve rispettare i processi e le procedure, predisposte dal Titolare, per la protezione dei dati personali che abbiano uno specifico impatto sulla funzione ricoperta dal Responsabile. Compito del responsabile è garantire che gli incaricati sotto la sua autorità rispettino le procedure predisposte dal Titolare. I processi e le procedure predisposte a fini della protezione dei dati personali sono reperibili presso la Direzione o il DPO
Diritto di audit	Il Titolare avrà il diritto di esercitare il proprio potere di controllo e ispezione per verificare il rispetto degli obblighi di cui alla suddetta normativa e/o delle istruzioni del Titolare di cui al presente Atto di nomina nonché delle misure di sicurezza tecniche e organizzative adottate dal Responsabile. A tal fine il Responsabile presterà ogni necessaria collaborazione e fornirà tutte le informazioni richieste per il proficuo svolgimento delle attività di audit effettuate dal Titolare stesso direttamente o tramite propri incaricati. Per

	l'avvio delle predette attività Quadrifor fornirà un preavviso di 20 giorni lavorativi.
Durata del trattamento	La durata del trattamento è stabilita dalle *policy* di *data retention* predisposte dal Titolare. In particolare, salvo gli obblighi di legge relativi alla conservazione, in particolare quelli di natura fiscale, si richiede la cancellazione dei dati personali entro 30 giorni dalla conclusione del contratto, previa restituzione a Quadrifor delle informazioni ivi presenti in un formato standard e trasportabile.
DPO	Il Responsabile è tenuto a collaborare e a coadiuvare il DPO nello svolgimento delle attività da questo effettuate. Il DPO è contattabile al seguente indirizzo email: l.viscione_rpd@quadrifor.it
Misure di sicurezza	La presente sezione fornisce i requisiti minimi per il rispetto dei livelli di sicurezza ritenuti necessari dal Titolare. L'implementazione delle Misure di sicurezza ivi descritte rientrano integralmente tra le obbligazioni del presente Contratto. 1. Esistenza di procedure/istruzioni operative in materia di Information Security e Data Protection. 2. Formazione continua e sensibilizzazione dei dipendenti sulla security e sulla data protection. 3. Esecuzione della profilazione degli accessi relativi alle utenze. 4. Conservazione di tutti i supporti di backup e di archiviazione che contengono informazioni riservate del Titolare in aree di memorizzazione sicure e controllate a livello ambientale. 5. Ove necessario, esistenza di tecniche di cifratura e/o pseudonimizzazione. 6. Esistenza di procedure di disaster recovery e di business continuity. 7. Esecuzione periodica di test di sicurezza sui sistemi (vulnerability assessment, penetration test, security assessment, ecc.). 8. Segmentazione e compartimentazione della rete dati. 9. Verifiche periodiche sui fornitori (ad es. tramite verifica documentale, certificazioni del fornitore o audit presso il fornitore). 10. Monitoraggio degli ingressi/uscite alle sedi aziendali e dove sono collocati i data center, tramite controllo degli ingressi fisici per il personale autorizzato (con tessera magnetica e tracciata sul sistema di controllo). 11. Protezione dei locali dell'azienda, ivi compresi quelli ospitanti i data center, attraverso adeguati sistemi di difesa passiva (es. allarmi antintrusione, inferriate o blindatura alle finestre, porte antisfondamento, servizi di guardiania). 12. Protezione delle apparecchiature informatiche centralizzate (server, storage) con mezzi specifici (sistema antincendio dedicato, elevazione contro eventuali allagamenti, alimentazione ridondante e/o aria condizionata, ecc.) e accesso limitato ai soli addetti. 13. Impiego di password complesse (minimo 12 caratteri di tipologia differente, reimpostazione password obbligatoria al primo accesso, scadenza password). 14. Adozione in tutti i casi possibili dell'autenticazione con due fattori;

	15. Assegnazione ad ogni utente di credenziali (user e password) personali, uniche e non assegnabili ad altri utenti. 16. Esistenza di una procedura interna che gestisca i cambi di ruolo e la cessazione del rapporto con l'azienda aggiornando o rimuovendo gli account e i relativi diritti di acceso. 17. Limitazione degli accessi agli archivi cartacei (es. mediante chiusura a chiave degli armadi etc…) 18. Gestione della dismissione di hardware o della sua riassegnazione ad altri utenti aziendali mediante cancellazione sicura (irreversibile) dei dati ivi contenuti. 19. Blocco automatico della sessione quando la postazione di lavoro non viene utilizzata per un determinato periodo di tempo. 20. Adozione di software firewall con limitazione dell'apertura delle porte di comunicazione a quelle strettamente necessarie al corretto funzionamento delle applicazioni. 21. Adozione di software antivirus automaticamente aggiornati. 22. Conservazione dei dati degli utenti su uno spazio di archiviazione centralizzato, regolarmente supportato e accessibile tramite la rete dell'organizzazione evitando la conservazione sulle postazioni di lavoro. 23. Esistenza di una politica di aggiornamento periodico del software, che eviti l'impiego di sistemi operativi e software obsoleti e non più aggiornabili con adeguate patch di sicurezza; 24. Assegnazione dei diritti di amministratore di sistema soltanto a personale debitamente incaricato e formato. 25. Divieto dell'uso di applicazioni scaricate da fonti non autorizzate dall'azienda. 26. Adozione, in caso di telelavoro, di una VPN per il collegamento sicuro ai sistemi aziendali.

Roma, lì _____

(Per Accettazione)

Il Titolare del trattamento
Francesca Mandato

Il Responsabile Esterno
(nome, timbro e firma del legale rappresentante)

_____ _____