

**ACCORDO DI NOMINA A RESPONSABILE ESTERNO TRATTAMENTO DATI ai sensi
dell'art. 28 del Reg. UE 2016/679**

Il presente Accordo di nomina a responsabile esterno del trattamento dati (di seguito denominato "Accordo") è concluso tra:

Denominazione / ragione sociale	
Con sede legale in (indirizzo)	
Codice Fiscale n.	
Partita Iva n.	
Legale rappresentante p.t.	
Di seguito denominata	
	o "Titolare del trattamento"

e

Myfoglio Italia S.r.l con sede legale in Via Bocconi 9 , 20136 Milano, P.IVA/C.F. 08997140960 in persona del legale rappresentante p.t. Roberto Stefanini, di seguito **"Myfoglio"** o **"Responsabile del trattamento"**.

PREMESSE

Premesso che:

- Il **Responsabile del trattamento**, al fine dell'esecuzione del rapporto contrattuale in essere tra le Parti, tratterà dati personali (d'ora in avanti "Dati Personali") di cui _____ è Titolare del trattamento;
- Le Parti intendono disciplinare il loro rapporto ai sensi dell'art. 28 del Reg. UE 2016/679.

Tutto ciò premesso, che costituisce parte integrante e sostanziale del presente Accordo, si conviene e si stipula quanto segue:

Art. 1 – Oggetto

Con il presente Accordo, il Titolare del trattamento nomina Myfoglio quale Responsabile esterno del trattamento dei dati personali di cui _____ è Titolare del trattamento, in accordo al disposto dell'art. 28 del Reg. UE 2016/679.

Il Responsabile del trattamento dovrà, in particolare:

- provvedere all'aggiornamento, modifica, rettifica e cancellazione dei Dati Personali qualora ciò sia necessario in relazione alle finalità del trattamento e se richiesto dal Titolare del trattamento;
- curare la conservazione dei Dati Personali in conformità a quanto previsto dall' art. 5 del Reg. UE 2016/679 (d'ora in avanti "GDPR") e, in generale, nel rispetto dei tempi e delle modalità imposte dalla normativa vigente;
- individuare e adottare le misure di sicurezza e organizzative adeguate previste dalla normativa Privacy applicabile, e in particolare:

a. ridurre al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità del trattamento stesso dei Dati Personali, adottando le misure di sicurezza così come individuate ed implementate dal Titolare del trattamento e in particolare: (i) adottare un sistema di autenticazione informatica con credenziali di almeno 8 caratteri, permettendo l'accesso solo agli incaricati e/o agli amministratori di sistema e/o ai responsabili interni del trattamento all'uopo muniti di credenziali di autenticazione; (ii) adottare procedure di gestione delle credenziali di autenticazione, nonché di disattivazione delle stesse se non utilizzate da almeno 6 (sei)

mesi o in caso di perdita della qualità che consente l'accesso ai Dati Personali; (iii) impartire istruzioni per regolare le modalità per assicurare la disponibilità dei Dati Personali in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per necessità di operatività e sicurezza; (iv) utilizzare un sistema di autorizzazione per gli incaricati, i responsabili interni e gli amministratori di sistema e aggiornare periodicamente l'ambito del trattamento consentito a detti soggetti; (v) redigere e aggiornare la lista degli incaricati; (vi) proteggere gli strumenti elettronici e i Dati Personali rispetto a trattamenti illeciti e ad accessi non consentiti, adottando antivirus e software volti a prevenire la vulnerabilità di strumenti elettronici, da aggiornare con cadenza almeno semestrale; (vii) adottare procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei Dati Personali e dei sistemi, che prevedano il salvataggio dei Dati Personali con frequenza almeno settimanale;

b. dare istruzione ai propri incaricati, responsabili interni e amministratori di sistema di mantenere come confidenziale ogni dato personale di terzi portato a loro conoscenza nel corso dell'esecuzione dei servizi oggetto del rapporto contrattuale tra le Parti, allo stesso modo dei relativi trattamenti, evitando che le credenziali restino incustodite o il terminale accessibile durante una sessione di trattamenti;

c. adottare, rispettare e far rispettare ai propri incaricati, responsabili interni e amministratori di sistema misure di sicurezza tecniche e organizzative adeguate ai sensi dell'art. 32 del GDPR, tra cui: (i) misure e procedure volte ad assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi, nonché la disponibilità e l'accesso dei Dati Personali in caso di incidente fisico o tecnico; (ii) procedure per la notifica di eventuali data breach all'autorità competente; (iii) formazione del personale; (iv) policy, processi e strumenti adottati dal Titolare del trattamento per assicurare e incrementare la conformità con il GDPR; (v) misure di cifratura e pseudoanonimizzazione; (vi) procedure per testare, verificare e valutare l'efficacia delle misure adottate; (vii) impostazione dei propri sistemi secondo i principi di privacy by design e by default e includere l'Analisi sull'Impatto della Protezione dei dati e il risk assessment nelle proprie procedure privacy; (viii) conservazione dei registri delle attività di trattamento svolte e loro messa a disposizione del Titolare del trattamento su richiesta; (ix) nomina di un Data Protection Officer ove necessario; (x) revisione della propria strategia di trasferimento di dati transfrontaliero in linea con il GDPR;

- vigilare che gli incaricati, i responsabili interni, i responsabili e sub-responsabili esterni e gli amministratori di sistema trattino i Dati Personali nel rispetto del GDPR in particolare: (i) che effettuino il trattamento in modo lecito e corretto, esclusivamente ai fini della prestazione dei servizi oggetto del rapporto contrattuale tra le Parti; (ii) che trattino i Dati Personali unicamente per finalità inerenti i compiti loro assegnati; (iii) che non comunichino o diffondano i Dati Personali senza la preventiva autorizzazione del Titolare del trattamento; (iv) che verifichino, in caso di interruzione anche temporanea del lavoro, che i Dati Personali trattati non siano accessibili a terzi non autorizzati; (v) che custodiscano e mantengano strettamente riservate le credenziali di autenticazione; (vi) che rispettino le misure di sicurezza adottate dal Titolare del trattamento;

- individuare gli amministratori di sistema, ove necessario, e nominarli per iscritto adempiendo a tutti i requisiti previsti dal Provvedimento del Garante Privacy del 27 novembre 2008;

- periodicamente e, comunque, almeno annualmente verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli incaricati, responsabili e amministratori di sistema;

- collaborare con il Titolare del trattamento nel rispondere alle richieste del Garante per la Protezione dei Dati Personali in caso di effettuazione di controlli ed accertamenti da parte dell'Autorità;

- assicurare il rispetto delle prescrizioni del Garante Privacy competente, informando il Titolare del trattamento circa eventuali richieste formulate dal Garante Privacy o da qualsiasi altra Autorità Giudiziaria e/o pubblica, nonché di ogni questione rilevante in materia di trattamento dei Dati Personali che dovesse sorgere durante l'espletamento dei servizi oggetto del rapporto contrattuale;

- avvisare tempestivamente il Titolare del trattamento di ogni eventuale richiesta ricevuta dagli interessati inerente l'esercizio dei diritti previsti dagli artt. 15-21 GDPR;

- ove richiesto dal Titolare del trattamento, rendere l'informativa di cui all'art. 13 GDPR e/o richiedere il consenso secondo quanto disposto dall'art. 6 GDPR e/o predisporre la richiesta di autorizzazione per il trattamento dei dati sensibili e per il trasferimento di dati personali all'estero, nei casi non previsti dalle autorizzazioni generali rilasciate dal Garante per la Protezione dei Dati Personali;

- consentire al Titolare del trattamento l'esercizio del potere di controllo ai sensi dell'art. 28 GDPR: in tal contesto, mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi del presente Accordo;

- interrompere, in caso di revoca o cessazione per qualsiasi ragione del presente Accordo, ogni operazione di trattamento dei Dati Personali e, su istruzione del Titolare del trattamento, provvedere alla restituzione dei Dati Personali

al Titolare del trattamento e, quindi, alla cancellazione degli stessi in tempi adeguati e comunque non oltre i 60 (sessanta) giorni dalla richiesta;

- notificare il Titolare del trattamento delle violazioni di Dati Personali (“data breach” o “data loss”) di cui il Responsabile del trattamento viene a conoscenza, senza ingiustificato ritardo. Nel caso in cui il “data loss” richieda un’operazione di ripristino dei dati, il Responsabile del trattamento indicherà al Titolare del trattamento la data del backup da cui vengono ripristinati i dati in modo da permettere al Titolare del trattamento di conoscere l’esatto intervallo temporale dei dati persi.

Il Titolare del trattamento vigilerà periodicamente sulla puntuale osservanza delle istruzioni qui impartite al Responsabile del trattamento e verificherà il perdurare dei requisiti di esperienza, capacità ed affidabilità che hanno influito sulla designazione del Responsabile del trattamento.

Il presente incarico non prevede alcun compenso aggiuntivo a favore del Responsabile del trattamento rispetto a quello già pattuito nel rapporto contrattuale tra le Parti.

Il Titolare del trattamento si riserva, ove ne ravvisasse la necessità, la facoltà di integrare ed adeguare, tempo per tempo, le istruzioni qui contenute anche in ottemperanza alle evoluzioni normative in materia di trattamento di Dati Personali: a tal fine, modificherà l’Elenco dei dati trattati e l’Elenco delle operazioni di trattamento, integrandoli con gli eventuali Dati Personali e le operazioni di trattamento ulteriori affidate al Responsabile del trattamento.

La nomina a Responsabile del trattamento esterno del trattamento dei Dati Personali decorre dalla sottoscrizione del presente Accordo e resterà valida sino a revoca o comunque fino al venir meno per qualsiasi ragione del rapporto contrattuale tra le Parti o sino alla cessazione dei servizi oggetto dello stesso e/o di ogni attività di trattamento dei Dati Personali di cui sopra.

Per quanto non espressamente previsto nel presente Accordo, si rinvia alle disposizioni generali vigenti in materia di protezione di dati personali.

Elenco dei Dati Personali trattati dal Responsabile del trattamento:

- (dati identificativi)
 - nome cognome
 - email
 - indirizzo
 - numero telefono fisso
 - numero telefono mobile
 - dati bancari
 - dati di solvibilità economica
 - indirizzo IP
 - immagine
- (dati sensibili)
 - dati che rivelano l'origine razziale o etnica
 - dati che rivelano le opinioni politiche
 - dati che rivelano le convinzioni religiose o filosofiche
 - dati che rivelano l'appartenenza sindacale
 - dati biometrici
 - dati relativi alla salute
 - dati relativi alla vita/orientamento sessuale
- (dati giudiziari)
 - dati relativi a indagini penali in corso
 - dati relativi a condanne penali
 - dati relativi a carichi pendenti
 - dati relativi a casellario giudiziale

I Dati Personali trattati si riferiscono ai seguenti soggetti interessati:

- Candidati
- Dipendenti
- Collaboratori (stagisti, interinali, progetto, co.co.co/pro, apprendisti)

- Utenti web
- Clienti
- Potenziali Clienti
- Fornitori
- Potenziali Fornitori

Elenco delle operazioni di trattamento:

- Raccolta
- Registrazione
- Organizzazione
- Strutturazione
- Conservazione
- Modifica
- Estrazione
- Consultazione
- Uso
- Elaborazione
- Comunicazione
- Limitazione
- Cancellazione
- Distruzione
- Raffronto fra dati

Art. 2 – Modalità di esecuzione dell’incarico

Il Responsabile del trattamento, al fine di controllare i rischi di accesso non autorizzato, divulgazione, mancanza di integrità ed indisponibilità dei Dati Personali, sia accidentali sia illegali, si impegna ad adottare le misure idonee a garantire la sicurezza dei Dati Personali così come indicato nel presente Accordo o richiesto dalla normativa.

Le suddette misure tecniche ed organizzative dovranno essere costantemente monitorate dal Responsabile del trattamento al fine di verificarne l’efficienza e garantire la sicurezza del trattamento dei Dati Personali.

Salvo previo consenso scritto del Titolare del trattamento, il Responsabile del trattamento si impegna a non trasmettere o conservare i Dati Personali in paesi esterni al territorio dell’Unione Europea eccetto che la Svizzera ed a non consentire l’accesso ai Dati Personali al proprio personale dipendente e/o a soggetti terzi siti fuori dal territorio dell’Unione Europea eccetto che la Svizzera.

Il Responsabile del trattamento garantisce la gestione delle richieste avanzate dal Titolare del trattamento o dagli interessati al trattamento entro il termine massimo di 30 (trenta) giorni dal ricevimento delle stesse al fine di permettere l’esercizio dei diritti degli interessati al trattamento dei Dati Personali.

Il Responsabile del trattamento, inoltre, avrà l’obbligo di comunicare al Titolare del trattamento nel minor tempo possibile, e comunque non oltre 48 (quarantotto) ore da quando ne abbia avuto conoscenza, qualsiasi distruzione, perdita, alterazione, divulgazione o accesso non autorizzato ai Dati Personali, ivi incluse quelle che abbiano riguardato i propri subfornitori. In tale ipotesi, sarà compito del Responsabile del trattamento fornire adeguata assistenza al Titolare del trattamento.

Art. 3 – Diritto di audit e di verifica periodica

Il Titolare del trattamento si riserva il diritto di compiere attività di audit e, in particolare, avrà facoltà di verificare, con un preavviso di almeno 7 (sette) giorni lavorativi, anche presso la sede del Responsabile del trattamento, la conformità delle procedure adottate da quest’ultima rispetto a quanto indicato nel presente Accordo ovvero richiesto dalla normativa.

A tal fine, lo stesso si impegna a concordare con il Responsabile del trattamento il programma di audit.

Il Titolare del trattamento procederà secondo quanto stabilito di volta in volta nel programma di audit, attraverso interviste, esame di documentazione ed osservazioni sull’utilità e sulle condizioni operative al fine di raccogliere un numero di evidenze oggettive sufficiente alla determinazione della conformità ai requisiti prefissati.

Il diritto rappresentato nel presente articolo si estende anche a eventuali subfornitori del Responsabile del trattamento.

In accordo all’art. 28, co. 3, del Reg. UE 2016/679, il Responsabile del trattamento si riserva la facoltà di rilevare e segnalare al Titolare del trattamento qualunque istruzione o procedura ritenga violare il Reg. UE 2016/679.

Art. 4 – Personale del Responsabile del trattamento

Il Responsabile del trattamento si impegna a stipulare con il proprio personale dipendente un obbligo di riservatezza pari a quello contenuto nel presente Accordo. Si impegna inoltre ad adoperare, per il trattamento dei Dati Personali, solo ed esclusivamente personale debitamente formato in materia di trattamento dei dati personali.

Art. 5 – Sub responsabili

Il Responsabile del trattamento avrà la facoltà di subappaltare il trattamento dei Dati Personali esclusivamente previo consenso scritto del Titolare del trattamento stesso. Inoltre, lo stesso Responsabile del trattamento si impegna a stipulare con eventuali sub responsabili un accordo scritto contenente le medesime condizioni contrattuali previste dal presente Accordo.

Art. 6 – Condizioni per le eventuali modifiche dell'Accordo

Il Titolare del trattamento ha la facoltà di apportare al presente Accordo, in qualsiasi momento, le modifiche e gli adeguamenti che dovessero rendersi necessari, anche per conformarsi ad eventuali aggiornamenti normativi.

Di ogni modifica verrà data comunicazione all'altra Parte a mezzo posta elettronica certificata.

A seguito della suddetta modifica, la Parte ricevente avrà 60 giorni per recedere dall'Accordo. Trascorso tale termine, le variazioni si riterranno accettate dalla Parte ricevente.

Art. 7 – Responsabilità del Responsabile del trattamento

Il **Responsabile del trattamento** tiene indenne e manlevato il Titolare del trattamento da ogni perdita, costo, spesa, multa e/o sanzione, danno e da ogni responsabilità di qualsiasi natura (sia essa prevedibile, contingente o meno) derivante da o in connessione con una qualsiasi violazione da parte dello stesso delle disposizioni contenute nel presente Accordo. In particolare, il Responsabile del trattamento tiene indenne il Titolare del trattamento da qualsiasi perdita derivante da qualsiasi violazione delle disposizioni contenute nel presente Accordo o previste della normativa applicabile, anche da parte di ogni subfornitore di cui si avvale; o dalla subfornitura o all'esternalizzazione di qualsiasi trattamento affidato a terzi soggetti.

Art. 8 - Durata

Il presente Accordo decorre dalla data della sua sottoscrizione e rimarrà in vigore fin tanto che il **Responsabile del trattamento** effettuerà il trattamento dei Dati Personali di cui _____ è Titolare del trattamento.

Art. 9 – Cancellazione o restituzione dei Dati Personali

Il Responsabile del trattamento si impegna a cancellare o restituire i Dati Personali al Titolare del trattamento al termine del presente Accordo ovvero in qualsiasi altro momento in cui tale richiesta venga avanzata dal Titolare del trattamento stesso, salvo che non sia previsto diversamente dalla normativa specifica applicabile ai servizi oggetto del rapporto contrattuale tra le Parti.

Art. 10 – Titolarità e riservatezza dei Dati Personali

Il Responsabile del trattamento si impegna a mantenere strettamente riservate e confidenziali e ad usare solo per l'esecuzione delle obbligazioni previste dall'Accordo ogni informazione relativa all'altra Parte e/o agli interessati al trattamento dei Dati Personali e/o ai prodotti, servizi, organizzazione, strategia commerciale o tecnica ricevute dall'altra Parte o di cui vengano a conoscenza in occasione dell'esecuzione dell'Accordo (nel seguito denominate "Informazioni Riservate").

Il Responsabile del trattamento si impegna a non utilizzare le Informazioni Riservate al di fuori degli scopi previsti dal presente Accordo, né a rivelarle a soggetti non previsti dallo stesso, senza l'approvazione scritta del Titolare del trattamento.

Il Responsabile del trattamento adotterà ogni misura necessaria a non divulgare o rendere in alcun modo disponibili le Informazioni Riservate del Titolare del trattamento e/o degli interessati a terzi e sarà comunque ritenuta direttamente responsabile nei confronti del Titolare del trattamento di ogni violazione da parte dei propri dipendenti e/o subfornitori degli obblighi di riservatezza di cui al presente articolo.

Le disposizioni del presente articolo non si applicano o cesseranno di applicarsi a quelle singole informazioni che il Responsabile del trattamento possa dimostrare:

- a) essere già divenute di pubblico dominio per ragioni diverse dall'inadempimento del Responsabile del trattamento stesso;
- b) essere già note prima di averle ricevute dal Titolare del trattamento;
- c) essere comunicate o divulgate in ottemperanza ad un ordine legittimo di qualsiasi autorità o in forza di un obbligo di legge.

Le Informazioni Riservate rivelate rimangono di proprietà del Titolare del trattamento. A seguito di richiesta scritta dello stesso Titolare del trattamento tali informazioni devono essere restituite o distrutte dal Responsabile del trattamento.

Art. 11 – Legge applicabile, Foro competente e Risoluzione stragiudiziale delle controversie

In caso di controversie concernenti la validità, l'interpretazione, l'esecuzione e la risoluzione del presente Accordo o allegati a esso collegati, le Parti si impegnano a cercare tra loro un equo e bonario componimento.

Qualora la controversia non sia risolta bonariamente, la stessa deve ritenersi di competenza esclusiva dell'Autorità Giudiziaria di Milano.

Per la risoluzione di ogni controversia concernente la validità, l'interpretazione, l'esecuzione e la risoluzione del presente Accordo sarà applicata la Legge Italiana.

Art. 12 – Data breach

Il Responsabile del trattamento si obbliga a informare, senza giustificato ritardo e comunque entro 48 (quarantotto) ore dal momento in cui ne è venuto a conoscenza, di ogni violazione della sicurezza che comporti anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque trattati ed a prestare ogni necessaria collaborazione al Titolare del trattamento in relazione all'adempimento degli obblighi sullo stesso gravanti di notifica delle suddette violazioni all'Autorità ai sensi dell'art. 34 del GDPR o di comunicazione della stessa agli interessati ai sensi dell'art. 34 del GDPR.

La comunicazione al Titolare del trattamento, ai sensi del paragrafo che precede, deve contenere almeno una descrizione della natura della violazione di Dati Personali e/o informazioni ed elencare le misure raccomandate per attenuare i possibili effetti pregiudizievoli della violazione di Dati Personali e/o informazioni. La comunicazione descrive, inoltre, le conseguenze della violazione di Dati Personali e/o informazioni e le misure proposte o adottate dal Responsabile del trattamento per porvi rimedio. Quanto previsto al periodo che precede deve essere applicato anche qualora la violazione sia solo presunta o esista un sospetto pur in assenza di certezze.

Il Responsabile del trattamento dovrà tenere un aggiornato inventario delle violazioni dei Dati Personali, ivi incluse le circostanze in cui si sono verificate, le loro conseguenze e i provvedimenti adottati per porvi rimedio, in modo da consentire al Titolare del trattamento di verificare il rispetto delle disposizioni del presente articolo. Nell'inventario devono figurare unicamente le informazioni necessarie a tal fine.

Il Titolare del trattamento avrà diritto, direttamente e/o indirettamente tramite terzi di propria fiducia, di effettuare ogni verifica, anche presso le sedi del Responsabile del trattamento, utile al fine di verificare il rispetto da parte del Responsabile del trattamento delle prescrizioni del presente articolo. Il Titolare del trattamento avrà altresì il diritto di richiedere la compilazione da parte del Responsabile del trattamento di questionari di self assessment.

Resta ferma l'applicabilità di ogni eventuale disposizione di legge di ogni genere e natura in materia di segnalazione delle violazioni dei dati.

Art. 13 – Amministratori di Sistema

Il Responsabile si impegna a conformarsi al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 *“Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”*, così come modificato dal Provvedimento del Garante del 25 giugno 2009 *“Modifiche del provvedimento 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”*, così come eventualmente modificato o sostituito dallo stesso Garante, e ad ogni altro pertinente provvedimento dell'Autorità.

Il Responsabile si impegna, in particolare, a:

- a. designare quali amministratori di sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di Dati Personali;
- b. predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali amministratori di sistema e le funzioni ad essi attribuite;
- c. comunicare periodicamente al Titolare del trattamento l'elenco aggiornato degli amministratori dei sistemi;
- d. verificare annualmente l'operato degli amministratori di sistema, informando il Titolare del trattamento circa le risultanze di tale verifica;
- e. mantenere i file di log previsti in conformità a quanto previsto nel suddetto provvedimento.

Art. 14 – Clausole finali

Il presente Accordo sostituisce ogni precedente intesa, anche verbale, fra le parti e costituisce l'unico esistente in relazione alle materie in esso trattate.

L'eventuale tolleranza di una parte all'inadempimento dell'altra non potrà in alcun modo essere considerata come rinuncia ai diritti derivanti dal presente Accordo.

Le parti dichiarano di aver negoziato in modo specifico tutte le clausole del presente Accordo.

Qualsiasi notifica, lettera o altra comunicazione prevista dal presente Accordo è comunicata per iscritto tramite lettera agli indirizzi di seguito indicati:

Per il Titolare del trattamento:

Nome e Cognome	
Denominazione / ragione sociale	
Persona di riferimento	
Email (PEC)	
Telefono	

Per il Responsabile del trattamento: **myfoglio italia srl, Via Bocconi 9 – 2016 Milano, privacy@myfoglio.com, telefono +39 02 30 46 86 44.**

Luogo e data

Il responsabile del trattamento

Il titolare del trattamento
