Designazione a Responsabile del trattamento dei dati personali
ai sensi dell'art. 28 del Regolamento Europeo n. 2016/679

TRA

Il Cliente, quale Titolare del trattamento dei dati personali relativi ai siti web di sua proprietà in forza del contratto in essere con Fortop S.r.l.,

(di seguito anche "**Titolare**")

E

Fortop S.r.l., avente sede legale in Corso Sempione, 10 - Milano, N. REA-MI 2010697, C. F. e P. IVA 02001910500, in persona del suo legale rappresentante dott.sa Claudia Guerri

(di seguito anche "**Responsabile**")
(di seguito congiuntamente anche "**Parti**")

PREMESSO CHE

- tra il Titolare e il Responsabile, unitamente ad altri soggetti, è in essere un rapporto giuridico per la gestione del progetto definito del contratto tra le parti;
- il Titolare ha affidato al Responsabile lo svolgimento del progetto digital oggetto del contratto, (di seguito anche "**Accordo**") e che, ai sensi del Regolamento Europeo n. 2016/679 (di seguito anche "**GDPR**"), lo svolgimento dell'Accordo prevede il trattamento di dati personali per conto del Titolare da parte del Responsabile che organizzerà, coordinerà ed effettuerà tali operazioni di trattamento;
- con il presente atto di incarico (di seguito anche "**Incarico**") il Titolare procede, ai sensi dell'art. 28 del GDPR, alla nomina del Responsabile, che accetta, quale responsabile del trattamento, e alla indicazione delle istruzioni relative al trattamento di dati personali da parte del Responsabile ai fini dell'espletamento delle Attività.

TUTTO CIÒ PREMESSO, TRA LE PARTI SI CONVIENE E SI STIPULA QUANTO SEGUE.

1. Premesse e allegati

1.1. Le premesse e gli allegati sono da considerarsi quali parti integranti e sostanziali dell'Incarico.

2. Definizioni

2.1. Fatti salvi i termini convenzionali di cui sopra, al fine di consentire la corretta applicazione della normativa in materia di tutela dei dati personali nello svolgimento dell'Incarico affidato al Responsabile, si specifica che si intendono qui integralmente richiamate le definizioni di cui all'art. 4 del GDPR.

2.2. Nell'ambito del presente Incarico, in aggiunta a quanto sopra, ai termini convenzionali di seguito riportati si intenderanno le definizioni rispettivamente indicate:

a) "**Normativa rilevante**": si intende il GDPR e qualsiasi provvedimento normativo o regolamentare adottato da autorità pubbliche nazionali in materia di trattamento di dati personali (ivi compresi i provvedimenti assunti dalle Autorità di controllo), applicabile durante il periodo di validità del presente Incarico.

b) "**Sub-responsabile/i**": si intende qualsiasi soggetto terzo incaricato dal Responsabile, in conformità alle procedure di cui al presente Incarico, che provvede – in tutto o in parte – alle operazioni di trattamento di dati personali di competenza del Responsabile;

c) "**Misure di sicurezza**": si intendono le misure tecniche e organizzative di sicurezza, adottate ai sensi dell'art. 32 del GDPR, cui si rinvia;

d) "**Richieste**": si intendono le richieste di informazioni (anche a titolo informale) / reclami / contestazioni da parte di terzi (a titolo esemplificativo e non esaustivo, interessati, Autorità di controllo o altre autorità giurisdizionali o amministrative) pervenute al Responsabile con riferimento alle operazioni di trattamento di cui al presente Incarico;

e) "**Spazio Economico Europeo**": gli Stati sovrani ricompresi nell'ambito di applicazione territoriale di cui all'art. 3 del GDPR.

3. Rapporti con l'Accordo

3.1. Il presente Incarico è espressamente collegato all'Accordo in essere tra le Parti; per ogni aspetto non espressamente disciplinato dal presente Incarico, si rinvia pertanto all'Accordo. In caso di contrasto tra le disposizioni dell'Accordo e quelle contenute nel presente Incarico, prevarranno queste ultime.

4. Dati personali trattati e finalità

4.1. Il Responsabile, per finalità di corretta esecuzione delle attività, come meglio specificate nel contratto in essere, potrà trattare i dati personali degli utenti.

4.2. Nello specifico, sulla base dei principali servizi erogati potranno essere trattati tipologie di dati diverse con modalità distinte, come di seguito indicato:

Nome servizio	Tipologia del dato	Finalità di gestione
Analisi di Mercato	Dati aggregati e/o pseudonimizzati, solo nel caso in cui per particolari ragioni gli intervistati siano identificabili.	Ulteriori operazioni di anonimizzazione a fini statistici
Visibilità Organica (accesso a Google Analytics o similari)	IP degli utenti del web, anche ove oggetto di pseudonimizzazione, qualora mediante altri elementi gli interessati siano comunque identificabili dalla piattaforma	elaborazione di informazioni statistiche aggregate, a fini commerciali e marketing
Visibilità Organica (accesso al CMS di gestione del sito)	Dati di accesso a sistemi applicazioni dei titolari del Trattamento quali: directory attive, indirizzo mail aziendale dipendente, dati personali comuni dell'utente web, identificativo della connessione degli utenti web, dati relativi agli ordini di acquisto, profilazione dell'utente.	gestione dei servizi richiesti a favore di clienti e utenti web al fine di migliorare le performance di marketing e vendita del sito web.
Piano di Tracciamento Analytics	Identificativo della connessione degli utenti web, qualora il servizio di Analytics impiegato ne conceda visibilità	gestione dei servizi richiesti a favore di clienti e utenti web
Data compliance GDPR	Identificativo dei Cookies e classificazione di scelta del profilo dei cookies (identificativi tecnici)	Indirizzare la corretta gestione dei cookies affinchè sia conforme alla normativa (GDPR e locale)
Gestione media ADV	Identificativo dei Cookies e classificazione di profilazione	Pubblicità on line sul sito rivolta agli utenti web interessati e che hanno prestato il relativo consenso

4.3. Tali dati potranno essere trattati esclusivamente per finalità di performance, profilazione e segmentazione dell'utenza nonché per l'arricchimento dei profili utenti creati e per gli adempimenti connessi a tali attività.

4.4. Nel caso in cui il Responsabile non disponga di informazioni sufficienti per procedere con i trattamenti dei dati personali del Titolare, informerà il Titolare. Il Titolare provvederà a fornire, per iscritto, le delucidazioni eventualmente richieste.

5. Istruzioni per il trattamento dei dati personali

5.1. Qualora il Responsabile ritenga che le istruzioni fornite vìolino o siano in contrasto con la Normativa Rilevante, procederà ad avvisare tempestivamente il Titolare per le valutazioni necessarie.

5.2. Il Responsabile dichiara e garantisce che:

a) tratterà i dati personali solo ed esclusivamente ai fini della prestazione delle attività descritte nel contratto con il cliente.

b) verificherà che ogni trattamento dei dati personali svolto, nell'interesse e per conto del Titolare, avvenga in modo lecito e secondo correttezza, nel rispetto dei principi di legittimità, esattezza, aggiornamento, pertinenza, completezza, adeguatezza, conservazione;

c) non porrà in essere operazioni di trattamento dei dati personali (o più, in generale, qualsiasi azione, omissione o condotta in relazione ai dati personali) per finalità proprie e autonome, e in generale per qualsivoglia finalità diversa dalla mera prestazione delle attività descritte nel contratto con il cliente.

d) adempirà ogni obbligazione prescritta dal presente Incarico, e più in generale porrà in essere ogni condotta richiesta per evitare che il Titolare incorra in violazioni della Normativa Rilevante, con riferimento ai dati personali trattati in esecuzione dell'Incarico;

e) nell'espletamento del presente Incarico, osserverà e si adeguerà prontamente ad ogni prescrizione prevista dalla Normativa Rilevante, provvedendo anche ad informare il Titolare di eventuali nuove disposizioni che possano comportare una variazione delle modalità e dei vincoli di trattamento dei dati personali. In particolare, il Responsabile procederà a:
    - tenere un idoneo registro ai sensi dell'art. 30 GDPR, ove richiesto;
    - nominare – ove opportuno o necessario – un Responsabile della Protezione dei Dati ai sensi degli artt. 37, 38 e 39 GDPR;
    - identificare e nominare gli Amministratori di Sistema, come da Provvedimento dell'Aurorità Garante del 27 novembre 2008 e ss.mm.ii., in quanto applicabile al tempo;
    - adottare ogni procedura interna e misura di sicurezza idonea alla protezione dei trattamenti e dei relativi dati personali trattati;
    - designare per iscritto le persone autorizzate al trattamento;
    - fornire al Titolare l'assistenza ed il supporto in ragione di quanto richiesto dagli artt. 35 e 36 GDPR, con riferimento alla redazione di una valutazione d'impatto sulla protezione dei dati;
    - presterà ogni supporto in relazione agli impegni posti a carico del Titolare dagli artt. 32-36 GDPR.

5.3. Il Responsabile, dietro espresse richieste del Titolare, si impegna ad adeguare i propri sistemi informativi, compatibilmente con la tipologia di dati trattati e le finalità perseguite dal Titolare, aggiornando le misure di sicurezza, gli strumenti e le procedure interne in materia di trattamento di dati personali, in modo da conformarsi all'art. 25 del GDPR e consentire una protezione dei dati personali trattati sin dalla progettazione (con implementazione di procedure, strumenti e Misure di sicurezza che consentano, sia al momento di determinare i mezzi del trattamento sia al momento del trattamento stesso, una maggiore tutela dei diritti degli interessati) e per impostazione predefinita (con implementazione di procedure tali da trattare solo i dati personali strettamente necessari per ogni finalità di trattamento).

6. Misure di sicurezza

6.1. Il Responsabile è obbligato ad adottare misure di sicurezza idonee a proteggere i dati personali trattati per conto del Titolare. Alle misure di sicurezza adottate dovrà conseguire un livello di sicurezza per i dati personali trattati, che sia idoneo e proporzionato in considerazione (i) della natura, dell'oggetto, del contesto e delle finalità del trattamento, (ii) dei rischi per i diritti e le libertà degli interessati, (iii) dello stato dell'arte della tecnica e della tecnologia e infine (iv) dei costi per l'implementazione ed eventuale aggiornamento di tali Misure di sicurezza.

6.2. Nello specifico, il Responsabile adotterà misure di sicurezza finalizzate a proteggere i dati personali trattati in generale da qualsiasi forma di trattamento illecito, e in particolare dalla distruzione, dalla modifica, dalla divulgazione o dall'accesso illeciti o non autorizzati. Le misure di sicurezza adottate dal Responsabile comprenderanno, se del caso:

a) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
b) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; e
c) una procedura per testare, verificare e valutare regolarmente l'efficacia delle Misure di sicurezza al fine di garantire la sicurezza del trattamento.

6.3. All'interno dell'Allegato A sono indicati i requisiti di base richiesti ai fini dell'implementazione delle Misure di sicurezza che il Responsabile dovrà adottare. Ulteriori Misure di sicurezza specifiche concretamente adottate dal Responsabile con riferimento a tutti o alcuni dei trattamenti di dati personali svolti per conto del Titolare saranno comunicate al Titolare nel corso dell'Incarico.

7. Violazioni di dati personali ai sensi degli artt. 33 – 34 del GDPR (c.d. data breach)

7.1. Il Responsabile si impegna a comunicare al Titolare tempestivamente, senza ingiustificato ritardo dalla scoperta dell'evento e comunque entro 72 ore dalla scoperta stessa, qualsivoglia incidente di sicurezza ovvero qualsiasi evento che comporti una violazione o l'imminente minaccia di violazione dei dati personali trattati (quali, a titolo meramente esemplificativo, compromissioni al funzionamento del sistema informatico, accessi non autorizzati, azione di malware, divulgazione non autorizzata, furto o perdita di documentazione), fornendo la necessaria collaborazione per la risoluzione dell'incidente.

7.2. La comunicazione di cui all'art. 7.1 dovrà contenere almeno le informazioni richieste dall'art. 33 del GDPR.

7.3. Il Responsabile presterà tutta l'assistenza e la collaborazione eventualmente richiesta dal Titolare al fine di porre rimedio alla violazione di dati personali, o di fornire all'Autorità di controllo ogni informazione o chiarimento richiesto.

8. Rapporti con terzi

8.1. Qualora gli interessati, le Autorità di controllo o qualsiasi altro terzo (ivi compresi, a titolo esemplificativo e non esaustivo, Autorità giurisdizionali e amministrative diverse dalle Autorità di controllo) avanzassero Richieste nei confronti del Responsabile (ivi comprese anche richieste per l'esercizio dei diritti riconosciuti agli interessati, quali il diritto di accesso, di rettifica, di opposizione, il diritto alla cancellazione, il diritto di limitazione di trattamento, il diritto di portabilità, il diritto di non essere sottoposto a una decisione basata sul trattamento automatizzato, compresa la profilazione), questo informerà immediatamente (e comunque non più tardi di 72 ore dalla ricezione della richiesta di informazioni / reclamo / contestazione) per iscritto il Titolare.

8.2. Il Responsabile avrà cura, in particolare, di trasmettere al Titolare copia delle Richieste pervenute, allegando altresì ogni ulteriore eventuale informazione o circostanza ritenuta utile.

8.3. Resta inteso che il Responsabile potrà fornire riscontro alle Richieste solo dietro espressa autorizzazione scritta del Titolare (che si riserva pertanto la facoltà di agire autonomamente), e comunque secondo le direttive, istruzioni e indicazioni fornite per iscritto da quest'ultimo. Il Responsabile, pertanto, non potrà in alcun modo agire in via autonoma, o in qualità di rappresentante / mandatario del Titolare (salvo espressa indicazione di questo a tal riguardo).

8.4. E' fatto espresso divieto al Responsabile di comunicare o divulgare a terzi, anche in riscontro alle Richieste, i dati personali trattati per conto del Titolare o qualsiasi eventuale ulteriore informazione relativa al trattamento dei dati personali senza aver ottenuto previe autorizzazioni e istruzioni per iscritto dal Titolare.

8.5. Qualora fosse obbligato – in esecuzione di obblighi normativi, o dietro richieste di autorità giurisdizionali, amministrative o di pubblica sicurezza – a divulgare o comunicare a terzi i dati trattati per conto del Titolare o le informazioni relative al trattamento. Il Responsabile:

a) notificherà immediatamente per iscritto al Titolare tale circostanza;
b) adotterà ogni accorgimento volto a limitare o restringere l'ambito della divulgazione / comunicazione (ad esempio, omettendo informazioni non espressamente richieste);
c) porrà in essere ogni ragionevole sforzo volto a ottenere dai destinatari delle comunicazioni impegni di riservatezza.

9. Sub-responsabili

9.1. Qualora, nel corso dell'esecuzione dell'Incarico, il Responsabile manifestasse la necessità di coinvolgere Sub-responsabili, questi potranno svolgere operazioni di trattamento di dati personali previa comunicazione scritta inviata dal Responsabile al Titolare, contenente i nominativi e/o elementi identificativi dei Sub-responsabili. L'incarico dei Sub-responsabili avverrà a condizione che gli eventuali Sub-responsabili sottoscrivano un accordo di incarico nel quale siano obbligati a prestare garanzie equivalenti a quelle poste a carico del Responsabile.

9.2. In caso di eventuale opposizione alla nomina di uno o più Sub-responsabili, il Responsabile si impegna a sottoporre al Titolare un ulteriore fornitore di propria fiducia per lo svolgimento dei trattamenti individuati.

9.3. Si ritengono in ogni caso autorizzati sin d'ora i Sub-responsabili indicati di volta in volta all'interno dell'incarico di consulenza formalizzato tra le parti, nonché i fornitori di servizi tecnologici sottesi alle attività previste.

9.4. Resta in ogni caso inteso che il Responsabile sarà responsabile nei confronti del Titolare per il corretto, puntuale e regolare adempimento delle obbligazioni assunte dai Sub-responsabili.

10. Trasferimento di dati personali

10.1. Il Responsabile vigilerà affinché i dati personali trattati per conto del Titolare non siano oggetto di trasferimento, anche a soggetti terzi, verso Paesi extra UE, senza la preventiva autorizzazione del Titolare.

10.2. Il Titolare dà atto di consentire in ogni caso al trasferimento di dati personali verso Paesi extra UE per ragioni tecnologiche o comunque necessarie in ragione dei fornitori o dei mezzi impiegati per lo svolgimento delle attività, in ogni caso nel rispetto dei requisiti di legge e in particolare mediante stipula delle Condizioni Contrattuali Tipo nella versione vigente, come approvata dalla Commissione Europea.

10.3. Nel caso in cui il trasferimento dei dati personali verso paesi terzi o organizzazioni internazionali sia richiesto dalla normativa vigente, il Responsabile informerà il Titolare circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.

11. Audit, ispezioni, verifiche

11.1. Il Responsabile si impegna a consentire la verifica e il controllo, da parte della Titolare della puntuale osservanza delle disposizioni impartite, anche in materia di sicurezza e di protezione dei dati, mettendo a disposizione tutte le informazioni necessarie per dimostrare il rispetto degli obblighi derivanti dalla normativa vigente.

12. Durata e destinazione dei dati personali

12.1. La presente nomina sarà efficace per tutta la durata dell'Accordo e dovrà intendersi revocata in caso di cessazione, per qualunque causa, dello stesso.

12.2. In caso di cessazione della presente nomina, sarà cura del Titolare richiedere al Responsabile di riconsegnare gli eventuali dati personali trattati per suo conto, ovvero distruggerli definitivamente, senza conservarne copia alcuna, salvo espresso diverso accordo o previsione di legge.

12.3. Qualora il Titolare ometta, decorsi trenta giorni dalla cessazione della nomina, di comunicare al Responsabile come intenda procedere, quest'ultimo avrà la facoltà di procedere con la cancellazione e distruzione definitiva di ogni dato personale.

13. Responsabilità e manleve

13.1. Il Responsabile terrà indenne il Titolare da ogni responsabilità direttamente derivante dalla esecuzione da parte del Responsabile (e/o dei Sub-responsabili da questo incaricati) delle disposizioni del presente Incarico, secondo le prescrizioni della Normativa Rilevante.

13.2. Il Responsabile non sarà in ogni caso tenuto a manlevare e tenere indenne il Titolare, qualora le responsabilità derivino dall'esecuzione delle istruzioni impartite dal Titolare e il Responsabile abbia informato il Titolare ai sensi del precedente art. 5.1.

14. Comunicazioni

14.1. Ai fini dell'Incarico e delle comunicazioni tra le Parti, le stesse dichiarano di eleggere domicilio presso la sede legale indicata in epigrafe.

14.2. Tutte le comunicazioni tra le Parti saranno validamente effettuate per iscritto a mezzo di lettera raccomandata con ricevuta di ritorno, ovvero a mezzo PEC all'indirizzo riportato nella visura camerale di ciascuna Parte.

14.3. Qualsivoglia modifica degli indirizzi sopra riportati avrà efficacia nei confronti delle Parti solo se sia stata portata a conoscenza dell'altra Parte con le modalità sopra specificate.

15. Varie

15.1. Qualsiasi modifica del presente Incarico dovrà, a pena di nullità, essere prevista in forma scritta.

15.2. L'Incarico annulla e sostituisce ogni precedente accordo o intesa tra le Parti in relazione al trattamento di dati personali svolti dal Responsabile per conto del Titolare.

15.3. Le Parti dichiarano che tutte le clausole contenute nel presente Incarico sono state oggetto di attenta e singola valutazione e riflettono la comune volontà.

15.4. Qualora una qualsiasi clausola del presente Incarico venisse dichiarata invalida, tale dichiarazione non inficerà la validità di tutte le altre clausole ivi contenute. In tale eventualità e per quanto possibile, tale clausola invalida dovrà venire sostituita da altra il cui effetto sia il più possibile equivalente a ciò che le Parti intendevano al momento della stipula dell'Incarico.

15.5. Il mancato esercizio da parte del Titolare di uno o più dei diritti che gli derivano dal presente Incarico, non costituirà né potrà essere inteso in alcun modo come rinuncia agli stessi.

15.6. I titoli degli articoli costituenti il presente Incarico hanno l'esclusivo fine di facilitare i riferimenti e non possono essere usati al fine di interpretare il contenuto dell'Incarico medesimo.

15.7. Resta inteso che la nomina a Responsabile del trattamento non attribuisce diritto ad alcun corrispettivo ulteriore rispetto a quanto previsto dall'Accordo, ed è finalizzata a garantire il corretto trattamento dei dati effettuato dal nominato Responsabile.

Allegato A

Misure di sicurezza

A - Prescrizioni in materia di misure di sicurezza logica e informatica

Il Responsabile garantisce che:
- all'interno della propria organizzazione aziendale è presente una struttura preposta al controllo e alla implementazione della sicurezza delle informazioni e dei dati personali trattati;
- sono eseguite, da detta struttura, le opportune periodiche verifiche e controlli di sicurezza;
- collabora con soggetti terzi alla propria struttura aziendale, a condizione che questi rispettino caratteristiche di affidabilità e attendibilità con riferimento alle misure di sicurezza adottate o da adottare.

Il Responsabile dovrà:
a) adottare elevati standard di sicurezza (e mantenerli aggiornati in considerazione dello stato dell'arte della tecnologia);
b) adottare una procedura in materia di sicurezza delle informazioni e dei dati personali processati, che sia conforme alle *best practices* di settore e che venga periodicamente aggiornata. Detta procedura sarà resa a disposizione del Titolare, dietro semplice richiesta;
c) implementare una procedura di segmentazione degli accessi alle informazioni e ai dati personali (a livello sia informatico, sia logico / fisico), su base *need-to-know* (potranno cioè accedere solo i soggetti che necessitino di conoscere date informazioni per l'esecuzione delle Attività), e una procedura di aggiunta / integrazione / dismissione di detti accessi;
d) utilizzare password complesse (minimo 8 caratteri di tipologia differente, reimpostazione password obbligatoria al primo accesso, scadenza password) per l'accesso ai sistemi informativi;
e) assegnare ad ogni utente credenziali (user e password) personali, uniche e non assegnabili ad altri utenti;
f) rimuovere gli account inattivi per più di 60 giorni o non più necessari per il trattamento di dati personali per conto del Titolare;
g) aggiornarsi costantemente e in modo continuativo su disposizioni normative, novità tecnologiche ed eventuali vulnerabilità in materia di sicurezza;
h) garantire che tutti gli apparati preposti all'archiviazione di dati e informazioni provenienti dal Titolare (ivi compresi gli apparati preposti al backup periodico) siano conservati in aree sicure e controllate a livello ambientale, detenute, gestite o contrattate dal Responsabile. Le aree di archiviazione utilizzate per memorizzare tali supporti dovranno essere programmate per ridurre ragionevolmente impatti derivanti da minacce ambientali;
i) assicurare che tutte le connessioni esterne ai propri sistemi (inclusi, senza limitazione, reti o accesso remoto) siano individuate, verificate, registrate e approvate individualmente;
j) assicurare che l'accesso wireless ai propri sistemi sia soggetto all'autorizzazione di autenticazione e ai protocolli di crittografia in linea con le *best practice* e siano consentiti solo dalle posizioni approvate dal Responsabile stesso.

B - Prescrizioni in materia di sicurezza fisica

Il Responsabile dovrà:
a) definire e mantenere aggiornate le procedure per garantire la sicurezza fisica nei locali sotto il proprio controllo;
b) proteggere da rischi ambientali e avarie infrastrutturali le apparecchiature del data center e i sistemi di sicurezza utilizzati;
c) proteggere fisicamente e conservare i supporti portatili che contengono dati personali trattati per conto del Titolare, assicurandosi che l'accesso agli stessi sia permesso solo al personale autorizzato;
d) adottare procedure e accorgimenti tali da consentire che i sistemi informatici consentano la possibilità di revocare immediatamente l'accesso alle apparecchiature di elaborazione dati, ai servizi e ai supporti di memorizzazione.