CONTRATTO TRA TITOLARE DEL TRATTAMENTO E RESPONSABILE DEL TRATTAMENTO

(Regolamento europeo sulla protezione dei dati personali - GDPR)

Cernitalia s.r.l. con sede legale in **Via Asiago 20128 Milano** e rappresentato da **Isa Maria Di Biagio** con P.iva/cod. fisc. **07739820152**
(qui di seguito, “il Titolare del trattamento”) da una parte,

e

Nereal srl con sede legale in viale Beatrice d'Este 1 e rappresentato da Claudio Frizziero
(qui di seguito, “il Responsabile del trattamento”)

Si conviene e stipula quanto di seguito riportato,

I. Oggetto

Oggetto delle presenti condizioni è definire le modalità nelle quali il Responsabile del trattamento si impegna ad effettuare per conto del Titolare le operazioni di trattamento dei dati personali definite di seguito.
Nel quadro delle loro relazioni contrattuali, le parti si impegnano a rispettare la regolamentazione in vigore applicabile al trattamento dei dati a carattere personale (personali) e, in particolare, il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 applicabile a partire dal 25 maggio 2018 (di seguito, “il regolamento europeo sulla protezione dei dati”).

II. Descrizione delle prestazioni del Responsabile del trattamento

Il Responsabile del trattamento è autorizzato a trattare per conto del Titolare del trattamento dei dati a carattere personale necessari per fornire il servizio di hosting e/o altri i servizi definiti all'interno del Contratto di Servizio Hosting

La finalità o le finalità del trattamento sono l'erogazione dei servizi, registrazione domini, fatturazione, archiviazione e backup, con modalità appropriate per garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrita` e riservatezza»);
I dati a carattere personale (personali) trattati sono: **Comunicazioni (es: telefono, email), Dati contrattuali, Dati personali, Log**
Le categorie di persone interessate sono: **Miei Clienti e dipendenti, Miei Clienti e parti interessate**
Qualora i dati trattati dal Titolare del Trattamento (Cliente) siano o rientrino in categorie particolari, il Titolare del Trattamento (Cliente) deve notificare per iscritto al Responsabile del Trattamento (Fornitore), nell'immediato o in tempi ragionevoli entro 72 ore, la categoria particolare in cui i dati appartengono, e coordinarsi con il Responsabile del Trattamento (Fornitore) per concordare nuove modalità di gestione e quindi essere conforme al GDPR secondo tale specifica situazione
Per l'esecuzione del servizio oggetto del presente contratto, il Titolare del trattamento mette a disposizione del Responsabile del trattamento le seguenti informazioni necessarie: dati di fatturazione, indirizzo email, indirizzo PEC, dati per registrazione domini in base ai requisiti dei singoli Registrar.

III. Durata del contratto

Il presente contratto entra in vigore a far data dal 25 maggio 2018 fino alla decorrenza del/i servizio/i contrattualizzato/i.

IV.Obblighi del Responsabile del trattamento di fronte al Titolare del trattamento

Il Responsabile del trattamento si impegna a:

1. Trattare i dati solo per la finalità o le finalità sopra specificate e per l'esecuzione delle prestazioni contrattuali.

2. Trattare i dati conformemente alle misure tecniche di Trattamento del Dato di seguito indicate:

I. Confidenzialità

- Controllo degli accessi fisici
  - Data center Milano (KPN), Siziano (Supernap), Nürnberg (Hetzner), Falkenstein (Hetzner)
    - Controllo elettronico con log
    - Protezioni perimetrali di alta sicurezza
    - Accesso solo ai rack di pertinenza
    - Personale data center presente 24x7
    - Video monitoraggio
    - Visitatori solo accompagati
  - Monitoring
    - Controllo degli accessi con log
    - Video sorveglianza degli accessi e uscite
- Controllo Elettronico degli accessi
  - Server dedicati, colocation, VPS: password gestibili e modificabili dai Titolari (Clienti)
  - Managed server, web hosting, storage: gestione con password

- Trasferimento controllato dischi
- Isolamento dei dati
  - Per amministrazione interna dati e backup sono fisicamente e logicamente separati
  - Per server dedicati, colocation, VPS:
    - Il Titolare del Trattamento (Cliente) è responsabile dell'isolamento dei dati
  - Managed server, web hosting, storage:
    - I dati e i backup saranno logicamente e/o fisicamente separati
- Pseudoanonimizzazione
  - Il Titolare del Trattamento (Cliente) è responsabile della pseudoanonimizzazione dei dati ove necessario

II. Integrità (Art. 32 Parag.1 Clausola b GDPR)

- Trasferimento dei dati
  - Tutti i collaboratore sono istruiti per trattare i dati in accordo con Art. 32 Parag. 4 GDPR
  - Cancellazione dei dati dopo il termine del contratto
- Data entry
  - Per i sistemi interni e amministrativi
    - Dati inseriti o raccolti dal Titolare del Trattamento (Cliente)

        - Cambiamenti dei dati sono loggati
    - Server dedicati, colocation, VPS
        - La responsabilità dei dati inseriti è a carico del Titolare del Trattamento (Cliente)
    - Managed server, web hosting, storage:
        - Dati inseriti o raccolti dal Titolare del Trattamento (Cliente)
        - Cambiamenti dei dati sono loggati

III. Disponibilità e capacità di recupero (Art. 32 Parag. 1 Clausola b GDPR)

- Availability control
    - Per sistemi interni e amministrativi
        - backup e recovery giornalieri dei dati rilevanti
        - Utilizzo di software di protezione (virus scanners, firewalls, encryption programs, spam filters)
        - Disk mirroring su tutti i server importanti
        - Monitoraggio di tutti i server e servizi importanti
        - UPS per corrente elettrica
        - Doppi circuiti elettrici in webfarm Supernap, KPN
        - Protezione anti-DDoS per webfarm Supernap, Hetzner

        - Server dedicati, colocation, VPS
            - Backup a carico del Titolare del Trattamento (Cliente) ove non espresso altrimenti
            - UPS per corrente elettrica
            - Doppi circuiti elettrici in webfarm Supernap, KPN
            - Protezione anti-DDoS per webfarm Supernap, Hetzner
        - Managed server, web hosting, storage
            - Backup e ripristino dei dati in funzione del Servizio scelto
            - Disk mirroring (RAID)
            - UPS per corrente elettrica
            - Software firewalls
            - Protezione anti-DDoS per webfarm Supernap, Hetzner
    - Misure di ripristino rapido (Art. 32 Parag. 1 Clausola c GDPR)
        - Sistemi interni con escalation per ripristino il più veloce possibile

IV. Procedure per controlli, validazione e verifiche regolari (Art. 32 Parag. 1 Clausola d GDPR; Art. 25 Parag. 1 GDPR)

- Policies
    - Gestione incidenti interno

- Utilizzo di Data-protection-friendly default settings nello sviluppo dei sistemi interni (Art. 25 Parag. 2 GDPR).

- Accordi e collaborazioni

  - I Collaboratori di Nereal srl sono istruiti per rispettare le leggi sulla protezione dei dati, le procedure e le linee guida per il trattamento dei dati dei Titolari (Clienti)

se il Responsabile del trattamento considera che un'istruzione costituisca una violazione del regolamento europeo sulla protezione dei dati o di tutte le altre disposizioni delle leggi dell'Unione o delle leggi degli stati membri relative alla protezione dei dati, deve informare immediatamente il Titolare del trattamento. Inoltre, se il Responsabile del trattamento è tenuto a procedere ad un trasferimento dei dati verso un paese terzo o un'organizzazione internazionale, in virtù delle leggi dell'Unione o delle leggi dello stato membro al quale è sottoposto, deve informare il Titolare del trattamento di quest'obbligo giuridico prima del trattamento, a meno che le leggi interessate proibiscano una tale informazione per motivi importanti di interesse pubblico.

3. Garantire la riservatezza dei dati a carattere personale (personali) trattati nell'ambito del presente contratto

4. Controllare che le persone autorizzate a trattare i dati a carattere personale in virtù del presente contratto:

   - Si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza

   - Ricevano la formazione necessaria in materia di protezione dei dati a carattere personale.

5. Tenere conto, utilizzando i materiali, i prodotti, le applicazioni od i servizi, dei principi di protezione dei dati a partire da quando questi vengono progettati e della protezione dei dati di default.

6. Ulteriore Responsabile del trattamento

   Il Responsabile del trattamento può ricorrere ad un altro Responsabile del trattamento (di seguito, “l’ulteriore Responsabile del trattamento”) per gestire attività di trattamento definite come quei servizi direttamente connessi alla fornitura della commessa principale. Questo non include servizi accessori che il Fornitore usi, es. servizi di telecomunicazione; servizi postali/di trasporto; servizi di manutenzione e di assistenza agli utenti; così come altre misure per assicurare la confidenzialità, disponibilità, integrità e resilienza dell’hardware e software dei sistemi del trattamento dei dati. Comunque, il Fornitore è obbligato ad adottare appropriate e giuridicamente vincolanti disposizioni ed implementare appropriate misure di controllo per garantire la protezione dei dati e la sicurezza dei dati dei dati dei Clienti, anche nel caso di servizi accessori esternalizzati.

   Per gli scopi di questo Accordo, i rapporti di subappalto sono definite come quei servizi direttamente connessi alla fornitura della commessa principale. Questo non include servizi accessori che il Fornitore usi, es. servizi di telecomunicazione; servizi postali/di trasporto; servizi di manutenzione e di assistenza agli utenti; così come altre misure per assicurare la confidenzialità, disponibilità, integrità e resilienza dell’hardware e software dei sistemi del trattamento dei dati. Comunque, il Fornitore è obbligato ad adottare appropriate e giuridicamente vincolanti disposizioni ed implementare appropriate misure di controllo per garantire la protezione dei dati e la sicurezza dei dati dei dati dei Clienti, anche nel caso di servizi accessori esternalizzati.

   Se il Cliente seleziona una località fuori dalla UE per i suoi server dedicati, server condivisi, e server Cloud WebMe, hosting Condivisi, etc. egli accetta quindi il subappaltatore del Fornitore come operatore e subappaltatore di data center in questa ubicazione. Una lista specifica per prodotto dei subappaltatori che operano ad ogni ubicazione può essere reperita a: https://webme.it/it/webfarm

7. Diritto di informazione delle persone interessate

   Spetta al Titolare del trattamento fornire l’informativa di cui agli art. 13-14 alle persone interessate per le operazioni del trattamento al momento della raccolta dei dati.

8. Esercizio dei diritti delle persone

   Per quanto possibile, il Responsabile del trattamento deve assistere il Titolare del trattamento nell'espletamento dei propri obblighi di far seguito alle domande di esercizio dei diritti delle persone interessate: diritto di accesso, di rettifica, di cancellazione e di opposizione, diritto alla limitazione del trattamento, diritto a trasportare i dati, diritto di non essere oggetto di una decisione individuale automatizzata (compreso il profilo).

   Qualora le persone interessate esercitino tale diritto presso il Responsabile del trattamento presentandogli la relativa richiesta, il Responsabile del trattamento deve inoltrare queste domande di ricevimento per posta elettronica a help@webme.it

9. Notifica della violazione di dati a carattere personale

   Il Responsabile del trattamento notifica al Titolare del trattamento ogni violazione di dati a carattere personale nel tempo massimo di 72 ore dopo esserne venuto a conoscenza e tramite email all'indirizzo indicato dal Titolare in fase di sottoscrizione del Contratto. Tale notifica è accompagnata da ogni documentazione utile per permettere al Titolare del trattamento, se necessario, di notificare questa violazione all'autorità di controllo competente.

   La notifica deve almeno:

   a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

   b) 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;

   c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

10. Assistenza del Responsabile del trattamento nell'attuazione degli obblighi del Titolare del trattamento
    Il Responsabile del trattamento assiste il Titolare del trattamento nella realizzazione di analisi d'impatto relative alla protezione dei dati, conformemente all'articolo 35
    Il Responsabile del trattamento assiste il Titolare del trattamento nella consultazione preventiva dell'autorità di controllo, prevista dall'articolo 36

11. Misure di sicurezza
    Il Responsabile del trattamento s'impegna a mettere in opera misure di sicurezza ed organizzative che garantiscono un livello di sicurezza adattato al rischio, ivi compresi,

    Il Responsabile stabilirà la sicurezza delle informazioni in conformità all'Art. 28 Par. 3 Prop. 2 Clausola c, e l'Art. 32 del GDPR nonché in particolare all'Art. 5 Par. 1 e Par. 2 del GDPR. Le misure da prendere sono misure di sicurezza dei dati e misure che garantiscano un livello di protezione appropriato al rischio relativo alla confidenzialità, integrità, disponibilità e resilienza dei Sistemi. Lo stato della tecnologia; i costi di implementazione; la natura, ambito, e scopo del trattamento; così come la probabilità dell'accadimento e della severità del rischio ai diritti e alle libertà delle persone fisiche all'interno dell'ambito dell'Art. 32 Par. 1 del GDPR devono essere tenuti in conto.

    Le misure tecniche e organizzative dovranno essere soggette al progresso tecnologico e successivo sviluppo. A questo proposito, al Responsabile è permesso implementare adeguate misure alternative. Il livello di sicurezza delle specifiche misure non deve essere compromesso.

Le principali misure di sicurezza comprendono:

a) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento tramite sistemi Raid

b) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico tramite backup frequenti ed eventuali location fisiche distinte

c) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Il Responsabile del trattamento s'impegna a mettere in opera le misure di sicurezza previste dal codice di comportamento interno.

12. Disposizione dei dati al termini delle prestazioni contrattuali

    Al termine della prestazione dei servizi relativi al trattamento di questi dati, il Responsabile del trattamento s'impegna a:

    - Distruggere tutti i dati a carattere personale

13. Responsabile della protezione dei dati
    Il Responsabile del trattamento comunica al Titolare del trattamento il nome ed i dati del proprio Responsabile della protezione dei dati, qualora ne abbia designato uno conformemente all'articolo 37 del regolamento europeo sulla protezione dei dati.

V. Obblighi del Titolare del trattamento di fronte al Responsabile del trattamento

Il Titolare del trattamento s'impegna a:

1. Fornire al Responsabile del trattamento i dati previsti al punto II delle presenti clausole
2. Documentare per iscritto tutte le istruzioni riguardanti il trattamento dei dati da parte del Responsabile del Trattamento
3. Vigilare, in anticipo e durante la durata di tutto il trattamento, sul rispetto degli obblighi previsti dal regolamento europeo sulla protezione dei dati da parte del Responsabile del trattamento
4. Supervisionare il trattamento, comprese le revisioni e le ispezioni da parte del Responsabile del trattamento.

VI. I diritti di ispezione del Cliente

1) Il Cliente dovrà avere il diritto di attuare ispezioni previa consultazione con il Fornitore o di attuarle mediante ispettori designati nei casi individuali.
Il Cliente dovrà avere il diritto di verificare il rispetto di questo Accordo da parte del Fornitore nelle sue attività commerciali mediante ispezioni in loco, che dovranno come regola generale essere annunciate per tempo.

2) Il Fornitore dovrà assicurare che il Cliente possa verificare il rispetto del Fornitore con gli obblighi dell'Articolo 28 del GDPR. Il Fornitore è obbligato a fornire al Cliente le necessarie informazioni su richiesta e in particolare fornire la prova dell'implementazione delle misure Tecniche e organizzative.

3) L'evidenza di tali misure che riguardano non solo questo specifico Accordo o Contratto potranno essere fornite in conformità con codici di condotta approvati ai sensi dell'Articolo 40 del GDPR; certificazione secondo una procedura di certificazione approvata in conformità con l'Articolo 42 del GDPR; certificati di un attuale revisore, relazioni, o estratti di relazioni pubblicate da organi indipendenti (es. un revisore, il Responsabile della Protezione dei Dati, il dipartimento di sicurezza informatica, il revisore della riservatezza dei dati, revisore della qualità); o una adeguata certificazione rilasciata da sicurezza informatica o audit sulla protezione dei dati.

4) Il Fornitore potrà far valere il diritto di richiesta di remunerazione per consentire le ispezioni del Cliente.

VII. Altri accordi

1. Rimborso

   Non è richiesto un compenso per questo contratto.
   Se il Cliente richiede assistenza per rispondere alle richieste dalle Persone Interessate come descritto nella sezione IV di questo Accordo, al Cliente potrà essere richiesto di rimborsare il Fornitore per tale assistenza.
   Se il Cliente esercita i diritti di monitoraggio come descritto nella sezione VII di questo Accordo, l'importo del compenso da concordare sarà basato sulla tariffa oraria fissa dell'addetto del Fornitore che è incaricato di supervisionare il revisore.
   Se il Cliente fornisce istruzioni al Fornitore al Cliente potrà essere richiesto di pagare ogni costo derivante da queste istruzioni.

2. Durata del contratto
   Questo Accordo dipende dall'esistenza di un rapporto contrattuale principale come descritto nella sezione I di questo documento. La cancellazione o altri termini del contratto principale come descritto nella sezione I invalideranno allo stesso tempo questo Accordo.
   Il diritto di eccezionale singola notifica della rinuncia pertanto rimane intatto così come il legale diritto di recesso.

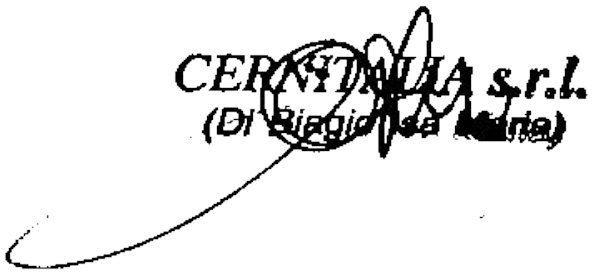
3. Scelta della legge
   Si applica la legge della Repubblica Italiana

4. Foro competente Le parti convengono che il foro competente dovrà essere l’ubicazione del tribunale competente per Sondrio(SO).

Firme, data

Milano, 2018-07-13 09:49:10

Cliente (il Titolare del Trattamento) Cernitalia s.r.l.



Fornitore (il Responsabile del Trattamento) Nereal srl