ATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO DATI
(artt. 4, par. 8 e 28 del Regolamento UE 679/2016 "GDPR")

Tra

Il **Cliente,** identificato come in anagrafica (qui di seguito anche "Operatore" e/o "Titolare")

e

DIEFFEITALIA.IT S.R.L. (P.IVA & C. F. 02982940732), con sede legale in Martina Franca (TA), via Taranto n. 72, 74015, (P.IVA & C. F. 02982940732), in persona del legale rappresentante Donato Filomena (qui di seguito anche "Dieffe" e/o "Responsabile" e/o "Fornitore");

di seguito anche congiuntamente "Le Parti"

Premesso che

- tra le Parti è in essere un Accordo relativo alla fornitura, da parte di Dieffe e a favore dell'Operatore, della piattaforma "ISP Billing" e relativi servizi di assistenza e manutenzione (di seguito, "**Servizi**");
- l'esecuzione dei Servizi comporta il trattamento, da parte del Fornitore, di dati personali di cui l'Operatore è Titolare, ai sensi dell'art. 4 par. 7 del Regolamento Europeo 2016/679 (di seguito "**GDPR**");
- per mezzo del presente atto di nomina (di seguito "**nomina**"), l'Operatore e il Fornitore intendono disciplinare i trattamenti di dati personali che quest'ultimo, in qualità di Responsabile ai sensi degli artt. 4, par. 8 e 28 del GDPR, svolgerà nell'interesse del Titolare nel corso dell'esecuzione dei Servizi;
- L'Operatore ritiene che Dieffe presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che i trattamenti soddisfino i requisiti della normativa vigente in materia di protezione dei dati (GDPR, D. Lgs. 196/2003 "Codice Privacy" e *ss.mm.ii*., Provvedimenti dell'Autorità Garante in materia – di seguito "**Normativa Privacy**") e garantiscano la tutela dei diritti degli interessati

Tutto ciò premesso e considerato, si conviene e si stipula quanto segue:

1. Le Parti concordano che, ai sensi del GDPR, L'Operatore è il Titolare del trattamento dei dati che saranno messi a disposizione del Fornitore che quest'ultimo raccoglierà, per conto del Titolare, ai fini dell'esecuzione dei Servizi (di seguito, "**Dati condivisi**") nella veste di Responsabile qui espressamente conferita dal Titolare.
In particolare, i Dati condivisi riguardano:
- dati comuni (identificativi e di contatto quali ad es. nome, cognome, n. di telefono, e-mail ecc.);
- dati relativi alle fatturazioni e ai pagamenti;
- dati di traffico;

riferiti ai seguenti soggetti interessati
- utenti del Titolare;

che il Fornitore tratta attraverso le operazioni necessarie all'esecuzione dei Servizi.

2. Con la sottoscrizione della presente nomina, il Fornitore accetta la designazione quale Responsabile del trattamento e conferma di possedere i requisiti di esperienza, capacità ed affidabilità richiesti dalla Normativa Privacy, potendo dunque mettere in atto, tra l'altro, misure tecniche e organizzative adeguate a garantire che i trattamenti dei Dati condivisi saranno eseguiti in conformità ai principi di legge, con particolare riferimento alla tutela dei diritti degli interessati.

3. Il Fornitore si impegna ad osservare – e a fare in modo che tutti coloro che agiscono sotto la propria direzione a loro volta rispettino – gli obblighi stabiliti dalla Normativa Privacy e, in particolare, a fare quanto segue:

a) svolgere esclusivamente le operazioni di trattamento delegate da parte del Titolare e, per l'effetto, non utilizzare i Dati condivisi per finalità diverse da quelle collegate alla sola esecuzione dei Servizi.

b) Trattare i Dati condivisi in piena conformità alle istruzioni qui fornite da parte del Titolare, o di quelle ulteriori che quest'ultima dovesse in un secondo momento ritenere opportuno fornire per la migliore e più efficiente esecuzione dei Servizi.

c) Garantire che tutte le persone agenti sotto la propria autorità alle quali sia consentito di accedere o trattare i Dati condivisi abbiano sottoscritto idoneo impegno – o siano altrimenti comunque adeguatamente vincolate – a mantenere totale riservatezza rispetto a tali dati e che, a tal fine, gli stessi agiscano sotto il costante controllo del Responsabile ed in conformità alle istruzioni da quest'ultimo fornite.

d) Definire e mettere in atto, tenendo conto delle *best practices di settore,* dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità delle operazioni di trattamento connesse all'esecuzione dei Servizi, oltre che dei rischi che tali trattamenti possono determinare per i diritti e le libertà degli interessati, misure tecniche ed organizzative adeguate a garantire un idoneo livello di sicurezza dei Dati condivisi (*vedi allegato 1*).

e) Implementare misure e processi, nell'ottica di cui al punto che precede, che garantiscano l'attuazione dei principi di *privacy-by-design* e *privacy-by-default* e, più in generale, la minimizzazione dei trattamenti, come ad esempio:

- l'adozione di sistemi di pseudonimizzazione o cifratura dei dati condivisi;
- la capacità di assicurare con continuità la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, oltre che quella di ripristinare tempestivamente la disponibilità e l'accesso ai Dati condivisi in caso di incidente fisico o tecnico;
- l'attivazione di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative messe in atto al fine di garantire la sicurezza dei trattamenti.

f) Adottare le misure necessarie a prevenire, o quantomeno minimizzare, ogni rischio ragionevolmente prevedibile connesso alla distruzione, alla perdita, alla modifica, alla divulgazione non autorizzata o all'accesso, in modo accidentale o illegale, ai Dati condivisi.

g) Adottare idonee misure di gestione delle violazioni della sicurezza da cui derivino accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati condivisi (*Data breach management policy*), prestando in ogni caso la massima collaborazione nei confronti del Titolare al fine di eliminare o quantomeno minimizzare gli impatti derivanti da eventi di questo tipo qualora dovessero verificarsi.

h) Fermo l'obbligo di notificare senza ingiustificato ritardo all'Operatore ogni possibile evento qualificabile come *data breach* ai sensi della Normativa Privacy applicabile, informare prontamente il Titolare riguardo a qualsiasi ulteriore evento, fatto o circostanza prevedibile o meno, da cui possa derivare un rischio elevato per i diritti e le libertà fondamentali degli interessati convolti nelle operazioni di trattamento.

i) Adottare misure tecniche ed organizzative che, anche in considerazione della natura dei trattamenti svolti per conto e nell'interesse del Titolare, consentano al Fornitore di assistere l'Operatore nell'adempimento del proprio obbligo di fornire adeguato riscontro alle richieste di esercizio dei diritti avanzate da parte degli interessati, con particolare riferimento alle istanze di portabilità, di limitazione del trattamento e di cancellazione ("oblio") dei dati.

j) Ove applicabile, individuare e nominare, ai sensi del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, le figure di "amministratore di sistema" e ottemperare agli obblighi ivi contenuti;

k) Collaborare con il Titolare, limitatamente ai trattamenti relativi ai Dati condivisi, nell'assolvimento degli obblighi di:

- notifica delle violazioni di dati all'Autorità Garante per la protezione dei dati personali (il "**Garante**") o ad altre autorità di controllo competenti e, laddove richiesto in ragione dell'elevato livello di rischio per i diritti e le libertà degli interessati, anche a questi ultimi;

- esecuzione, in tutti i casi in cui ciò sia necessario, di idonea valutazione di impatto sulla protezione dei dati (*privacy impact assessment*), oltre che nello svolgimento delle procedure di consultazione preventiva con il Garante e le altre autorità competenti.

l) Predisporre e mantenere costantemente aggiornato, in formato elettronico o cartaceo, un registro di tutte le operazioni di trattamento svolte ai fini dell'esecuzione dei Servizi ai sensi dell'art. 30 del GDPR.

m) Fermo l'obbligo di collaborazione di cui alla precedente lett. k), mettere l'Operatore al corrente di qualsiasi richiesta di esercizio di diritti inviata da parte degli interessati, entro un termine massimo di 24 ore dal ricevimento della stessa.

n) Non trasferire i Dati condivisi al di fuori dello Spazio Economico Europeo se non previa autorizzazione da parte del Titolare ed in presenza di idonee garanzie ai sensi di legge (quali ad es. decisioni di adeguatezza della Commissione UE, Clausole Contrattuali Standard o *Binding Corporate Rules*).

o) Non comunicare a terzi, e più in generale, non diffondere i Dati condivisi, se non in presenza di adeguati presupposti di liceità per tali ulteriori trattamenti.

p) Prestare nei confronti del Titolare ogni necessaria collaborazione nell'assolvimento di richieste che dovessero pervenire dal Garante o da altre autorità competenti o in relazione a procedure o ispezioni che dovessero essere avviate nei confronti dell'Operatore, dando altresì immediata esecuzione alle istruzioni ricevute e fornendo copia di ogni documento richiesto.

4. Il Titolare autorizza espressamente che alcune operazioni di trattamento dei Dati condivisi siano affidate dal Fornitore a soggetti terzi quali altri responsabili del trattamento (di seguito "**sub-responsabili**").

Il Fornitore si impegna ad avvalersi di sub- responsabili che garantiscono misure tecniche e organizzative adeguate al trattamento e garantisce che l'accesso ai Dati Condivisi, e il relativo trattamento, sarà effettuato esclusivamente nei limiti di quanto necessario per l'erogazione dei Servizi.

L'elenco dei sub-responsabili è indicato all'allegato 2 della presente nomina, eventuali ulteriori informazioni sono a disposizione su richiesta.

5. Fermo tutto quanto sopra, il Responsabile dovrà mettere a disposizione del Titolare tutte le informazioni necessarie a dimostrare il rispetto dei propri obblighi, cooperando altresì ad eventuali attività di *audit*, revisioni o controlli che l'Operatore dovesse ritenere opportune per monitorare il mantenimento, da parte del Responsabile, dei dovuti livelli di sicurezza dei Dati condivisi per l'esecuzione dei Servizi. Qualsiasi inadempimento o violazione degli obblighi sopra stabiliti e di ogni ulteriore norma di legge applicabile, con particolare riguardo ai necessari livelli di sicurezza, anche in tema di *data breach management,* ricadrà sotto l'esclusiva responsabilità del Fornitore.

6. La presente nomina avrà la medesima durata dell'Accordo. Alla cessazione – per qualsiasi causa – del rapporto, il Fornitore dovrà restituire al Titolare tutti i Dati condivisi, provvedendo altresì alla definitiva cancellazione di ogni copia degli stessi, in qualsiasi formato (back-up, cartacea, su supporto mobile, in cloud, ecc.), tranne quando diversamente richiesto da norme di legge o in ragione di prescrizioni dettate dal Garante o da altre autorità competenti.

Allegati:

- **Allegato 1 – Descrizione delle misure tecniche e organizzative di sicurezza**
- **Allegato 2 – Elenco Sub Responsabili**

ALLEGATO 1

Descrizione delle misure tecniche e organizzative di sicurezza implementate dal Responsabile (e dai sub-responsabili).

CONTESTO	MISURE DI SICUREZZA A PROTEZIONE DEI DATI PERSONALI DESCRIZIONE
NETWORK E RETE	Firewall e router sono configurati al fine di verificare, limitare e convalidare il traffico, in entrata e in uscita, da reti "non attendibili" (incluse reti wireless).
	Per proteggere i dati personali durante la trasmissione su reti aperte, pubbliche o non attendibili, è previsto l'utilizzo di protocolli sicuri.
	Per proteggere la riservatezza e l'integrità dei dati, è prevista la crittografia SSL (Secure Sockets Layer) durante il transito dei dati tra il client e il server. Questo previene efficacemente l'intercettazione dei dati durante il loro trasferimento attraverso la rete.
	Sono installati e mantenuti in costante aggiornamento idonei software di protezione malware e antivirus nel sistema.
	La rete è protetta contro gli attacchi DDoS tramite soluzioni di mitigation fornite da OVH. Questo sistema aiuta a filtrare il traffico maligno e a garantire la continuità del servizio anche durante tentativi di attacco distribuito.
SICUREZZA E CONSERVAZIONE DEI DATI	Il periodo di conservazione dei dati personali è limitato nella misura necessaria per ogni singola attività di elaborazione, nel rispetto degli obblighi legali e/o regolamentari vigenti.
	I programmi utilizzati per compiere attività di trattamento sono aggiornati con i più recenti rilasci di sicurezza.
	Localizzazione dei Server: Unione Europea.
	Il numero degli archivi di dati personali (database, file, copie, archivi) è ridotto al minimo, evitando inutili duplicazioni.
DISPONIBILITA' E RIPRISTINO	Sono messe in atto procedure di backup adeguate a ripristinare la disponibilità dei dati personali in modo tempestivo e la resilienza dei sistemi con cui sono operati i trattamenti.
GESTIONE DEGLI ACCESSI INFORMATICI	I profili di autorizzazione per l'accesso ai sistemi informatici sono configurati considerando il principio del "privilegio minimo necessario" e di separazione dei compiti. La pertinenza dei profili è oggetto di revisione periodica.
	Sono previste tecniche di Strong Authentication per gli accessi ai dati.
	Il numero degli archivi di dati personali (database, file, copie, archivi) è ridotto al minimo, evitando inutili duplicazioni.

CONTESTO	MISURE DI SICUREZZA A PROTEZIONE DEI DATI PERSONALI
	DESCRIZIONE
	Gli access log di coloro che accedano ai sistemi informatici con privilegi amministrativi sono registrati per un periodo minimo sufficiente a permettere la ricostruzione di eventi anomali e in modi tali da garantire l'integrità e l'inalterabilità dei log raccolti, e, in ogni caso, nei modi e tempi previsti da obblighi normativi applicabili.
VIOLAZIONE DEI DATI PERSONALI	È mantenuto ed aggiornato uno specifico registro delle violazioni dei dati personali.
	È presente ed aggiornata una procedura per gestire i *data breach*.
SICUREZZA FISICA	Applicazione di misure adeguate a prevenire accessi fisici non autorizzati ai locali contenenti dati personali o in cui si operano attività di trattamento.
	Applicazione di misure adeguate a minimizzare i rischi di danneggiamenti accidentali e/o intenzionali ad archivi, banche dati elettroniche e apparecchiature dedicate al trattamento di dati.

ALLEGATO 2

Elenco Sub-Responsabili del trattamento (*ex* art.28 GDPR)

- ***Google Cloud SQL*** - Servizio di Hosting. Maggiori dettagli su: https://cloud.google.com/trust-center/;
- ***OVH Cloud***-Protezione DDoS – Attack Mitigation. Maggiori dettagli qui: https://www.ovhcloud.com/it/security/anti-ddos/ddos-attack-mitigation/.