ATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI (art. 28 Regolamento UE 2016/679 — GDPR)

Allegato al Contratto di Licenza d'Uso e Fornitura del Servizio Software ApphoPMS

TRA

Utilizzatore del software ApphoPMS (di seguito il "Titolare")

E

Adriatica Sistemi Società Cooperativa (P.IVA 01999590688), con sede legale in Pescara (PE) alla Strada Della Bonifica, 108/110, nella persona del Suo legale rappresentante pro tempore (di seguito il "Responsabile"),

di seguito congiuntamente definite le "Parti"

PREMESSO CHE

a) Le Parti hanno stipulato il "Contratto di Licenza d'Uso e Fornitura del Servizio Software

ApphoPMS" (di seguito il "Contratto");

b) nell'esecuzione delle prestazioni contrattuali — tra cui l'erogazione dei servizi Cloud, la conservazione e sincronizzazione del database, l'assistenza tecnica, la manutenzione preventiva e correttiva — il Responsabile tratta, per conto e nell'interesse del Titolare, dati personali di cui

quest'ultimo è Titolare del trattamento ai sensi dell'art. 4, n. 7, GDPR;

c) le Parti intendono con il presente atto (di seguito la "Nomina") dare attuazione a quanto

previsto dall'art. 28 GDPR; tutto ciò premesso, le parti convengono e stipulano quanto segue:

Art. 1 – Nomina e accettazione

Il Titolare nomina Adriatica Sistemi Società Cooperativa quale Responsabile del trattamento dei dati personali ai sensi e per gli effetti dell'art. 28 del GDPR per tutte le attività di trattamento eseguite tramite o in relazione al Software ApphoPMS. Il Responsabile accetta la nomina, confermando di disporre delle competenze e risorse tecniche e organizzative idonee ad assicurare

il rispetto del GDPR e della normativa vigente sulla protezione dei dati personali.

Art. 2 – Oggetto, natura e finalità

2.1 Il Software ApphoPMS (di seguito il "Software") è fornito in architettura tecnologica con applicativo locale e database in ambiente Cloud con backup giornaliero, comprendente una suite di moduli gestionali tra cui: PMS (gestione prenotazioni, check-in/out, conti, schede alloggiati, ISTAT, tassa di soggiorno), Fatturazione Elettronica e Corrispettivi (XML), Clienti e Preventivi, Ristorante (comande e trattamento HB/FB), Spiaggia (gestione ombrelloni/servizi), App

Smartphone per ospiti e operatività del personale, Channel Manager e Booking Engine.

2.2 Il trattamento consiste in operazioni di raccolta, registrazione, organizzazione, strutturazione, conservazione (tramite hosting cloud), consultazione, elaborazione, estrazione, sincronizzazione local-to-cloud, backup giornaliero, modifica, cancellazione e distruzione di dati personali nell'ambito dell'erogazione, gestione, manutenzione tecnica e assistenza del Software

ApphoPMS;

2.3 I dati sono trattati esclusivamente per consentire al Titolare l'utilizzo operativo delle funzionalità del Software ApphoPMS e per l'erogazione dei correlati servizi di assistenza e manutenzione da parte del Responsabile, oltre all'analisi di dati di telemetria di cui all'art. 16 del

Contratto.

Art 3 — Categorie di Dati Personali Trattati

Dati Anagrafici e di Contatto (nome, cognome, luogo e data di nascita, nazionalità, indirizzo di residenza, documenti di identità, codice fiscale, numeri di telefono, indirizzi e-mail), dati contabili e amministrativi (dati di fatturazione elettronica, metodi e dettagli di pagamento) nonché eventuali categorie particolari di dati (dati relativi alla salute espressamente inseriti nel modulo Ristorante o nella scheda cliente del PMS, con primario riferimento ad allergie alimentari, intolleranze, celiachia, regime dietetico per esigenze sanitarie, nonché eventuali specifiche esigenze legate a disabilità o ridotta mobilità necessarie per l'assegnazione delle camere o dei

servizi spiaggia).

Art 4- Categorie di Interessati Ospiti e clienti della struttura ricettiva, del ristorante e dello stabilimento balneare, potenziali clienti (richiedenti preventivi), dipendenti, collaboratori e fornitori del Titolare, nonché ulteriori

soggetti i cui dati siano trattati tramite il Software per conto del Titolare.

Art. 5- Istruzioni documentate del Titolare

Il Responsabile tratta i dati personali esclusivamente sulla base delle istruzioni documentate impartite dal Titolare tramite il presente Atto e il Contratto, salvo che lo richieda il diritto dell'Unione o dello Stato membro cui è soggetto il Responsabile. Qualora il Responsabile ritenga che un'istruzione violi il GDPR o altre disposizioni di legge relative alla protezione dei dati, ne

informa immediatamente il Titolare. Prima di effettuare un trattamento imposto dal diritto dell'Unione Europea o dello Stato membro cui è soggetto, il Responsabile informa il Titolare di tale obbligo, salvo che la legge vieti tale informazione per rilevanti motivi di interesse pubblico.

Art. 6— Obblighi del Responsabile del Trattamento

Il Responsabile si obbliga a:

a) trattare i dati riservati esclusivamente per le finalità contrattuali previste;

b) garantire che le persone autorizzate al trattamento dei dati personali (dipendenti e collaboratori del Responsabile) si siano impegnate alla riservatezza o siano soggette a un adeguato obbligo legale di riservatezza;

c) adottare tutte le misure di sicurezza richieste dall'art. 32 del GDPR;

d) rispettare le condizioni per il ricorso a Sub-responsabili di cui all'Art. 8 del presente Atto;

e) assistere il Titolare con misure tecniche e organizzative adeguate per consentire al Titolare di dare riscontro all'esercizio dei diritti degli interessati (artt. 15-22 GDPR);

f) assistere il Titolare nell'adempimento degli obblighi relativi alla sicurezza del trattamento, alla notifica delle violazioni di dati personali (Data Breach) e alla valutazione d'impatto sulla protezione dei dati (DPIA), tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile; Tale assistenza è limitata agli aspetti tecnici inerenti ai servizi prestati e non comprende attività di consulenza o rappresentanza legale del Titolare.

g) mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 GDPR e consentire le attività di verifica/audit secondo l'Art. 9 del

presente Atto.

Art. 7— Misure di sicurezza

Il Responsabile dichiara di aver adottato, e si impegna a mantenere nel tempo, misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte, dei costi di attuazione e della natura, dell'oggetto, del contesto e delle finalità del trattamento, ivi comprese, tra l'altro: misure di controllo degli accessi logici, cifratura e/o pseudonimizzazione ove applicabile, procedure di backup e disaster recovery, capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi, procedure di

test e valutazione periodica dell'efficacia delle misure adottate.

Art. 8— Personale autorizzato

Il Responsabile garantisce che l'accesso ai dati personali sia consentito esclusivamente ai propri dipendenti e collaboratori preventivamente designati quali soggetti autorizzati al trattamento,

formalmente istruiti e vincolati all'obbligo di riservatezza.

Art. 9— Gestione delle richieste degli interessati Qualora l'interessato/ gli interessati rivolgano direttamente al Responsabile istanze per l'esercizio dei diritti previsti dal GDPR, il Responsabile non fornisce riscontro autonomo, ma trasmette

tempestivamente la richiesta al Titolare, salvo diversa e specifica istruzione del Titolare stesso.

Art. 10— Sub-responsabili del trattamento

Il Titolare autorizza in via generale il Responsabile ad avvalersi di Sub-responsabili per l'erogazione di specifici servizi infrastrutturali e tecnici, come fornitori di server cloud, hosting datacenter e/o simili.

Il Responsabile informa il Titolare di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri sub-responsabili con un preavviso di 15 (quindici) giorni, concedendo al Titolare il diritto di opporsi per giustificati motivi legati alla protezione dati. Il Responsabile impone ai Sub-responsabili, mediante contratto, i medesimi obblighi di protezione dei dati

stabiliti nel presente Atto.

I sub-responsabili infrastrutturali utilizzati per il servizio sono:

- Aruba, per la fornitura dell'infrastruttura server sulla quale sono ospitati i database del servizio.

- Wasabi, per la fornitura dello spazio di archiviazione cloud S3 destinato alla conservazione dei backup, configurato nella regione di Milano (Italia).

Art. 11 — Verifiche e Ispezioni (Audit)

Il Titolare ha il diritto di verificare la conformità del Responsabile agli obblighi previsti dal presente Atto e dall'articolo 28 del GDPR.

Il Responsabile mette a disposizione del Titolare le informazioni necessarie a dimostrare il rispetto di tali obblighi e consente e contribuisce alle verifiche, comprese le ispezioni, effettuate dal Titolare o da un auditor indipendente da questi incaricato.

Le verifiche ordinarie sono concordate preventivamente, con un preavviso scritto di almeno 15 (quindici) giorni lavorativi, e sono svolte con modalità proporzionate, evitando interferenze ingiustificate con l'operatività del Responsabile e garantendo la sicurezza dei sistemi, la riservatezza delle informazioni aziendali e la protezione dei dati degli altri clienti.

In presenza di circostanze urgenti e documentate che rendano necessario un intervento tempestivo, le Parti concordano modalità e tempi di verifica adeguati alla situazione.

Il Responsabile può mettere a disposizione documentazione tecnica, certificazioni di terzi e report di audit indipendenti, ove disponibili, quali strumenti per dimostrare la conformità, ferma restando la possibilità di ulteriori verifiche quando legittimamente necessarie.

I costi delle verifiche ordinarie richieste dal Titolare sono a carico di quest'ultimo, salvo diversi obblighi inderogabili di legge o differenti accordi tra le Parti.

Le verifiche non comportano un diritto di accesso indiscriminato ai sistemi informatici, alle credenziali, al codice sorgente o ai dati personali di altri clienti.

Restano fermi i poteri di controllo e di accesso dell'Autorità di controllo previsti dalla normativa applicabile.

Art. 12— Violazioni dei dati personali (Data Breach)

In caso di violazione della sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trattati, il Responsabile si impegna a notificare l'evento al Titolare senza ingiustificato ritardo e, ove possibile, entro 48 ore da quando ne è venuto a conoscenza. La notifica sarà corredata da una descrizione della natura dell'evento, delle categorie di dati/interessati coinvolti e delle misure

correttive adottate o proposte.

Art. 13— Trasferimento dei dati al di fuori dello Spazio Economico Europeo

I dati personali non saranno trasferiti verso paesi terzi al di fuori dello Spazio Economico Europeo (SEE) o verso organizzazioni internazionali, salvo che il trasferimento avvenga sulla base di una decisione di adeguatezza della Commissione Europea o previa adozione delle garanzie adeguate

di cui agli artt. 45-46 del GDPR. Ogni eventuale trasferimento è inoltre effettuato sulla base delle istruzioni documentate del Titolare.

Art. 14 — Responsabilità

Le Parti rispondono dei danni causati a terzi o agli interessati dal trattamento in conformità con quanto stabilito dall'art. 82 del GDPR. Il Responsabile risponde dei danni cagionati dal trattamento unicamente qualora non abbia adempiuto agli obblighi del GDPR specificamente diretti ai responsabili del trattamento o abbia agito in modo difforme o contrario rispetto alle

legittime istruzioni del Titolare.

Art. 15 — Cessazione del Contratto e gestione dei dati personali

Alla cessazione, per qualsiasi causa, del Contratto, il Titolare può richiedere la restituzione dei propri dati personali nel formato tecnico originario del database (.sql), mediante trasmissione tramite PEC con adeguate misure di sicurezza, oppure impartire istruzioni documentate per la loro cancellazione, conformemente all'articolo 28, paragrafo 3, lettera g), del GDPR.

In assenza di differenti istruzioni documentate del Titolare, il Responsabile procede alla cancellazione dei dati presenti nei sistemi operativi decorso il periodo di disponibilità previsto dall'articolo 9 del Contratto, ordinariamente pari a 30 giorni dalla cessazione del servizio. Tale periodo può essere prorogato su richiesta documentata del Titolare, anche per consentire un eventuale rinnovo tardivo del servizio.

Le copie presenti nei sistemi di backup sono conservate secondo il ciclo tecnico di rotazione, per un periodo massimo di 100 giorni dalla loro creazione, durante il quale sono protette e non utilizzate per finalità operative ordinarie, salvo esigenze di ripristino o obblighi di legge. Alla scadenza del relativo ciclo, tali copie sono eliminate.

Il Responsabile conferma per iscritto, su richiesta del Titolare, l'avvenuto completamento delle operazioni di cancellazione, tenendo conto dei tempi di eliminazione delle copie di backup.

Restano salvi eventuali obblighi di conservazione previsti dal diritto dell'Unione Europea o dalla normativa nazionale applicabile.

Art. 16 — Durata

La presente Nomina ha efficacia per tutta la durata del Contratto e si intende automaticamente risolta alla cessazione dello stesso, fermi restando gli obblighi di riservatezza e di cancellazione/restituzione dei dati di cui agli articoli precedenti, che permangono anche

successivamente alla cessazione del Contratto.

Art. 17 — Legge applicabile e Foro competente Il presente Atto è disciplinato dalla legge italiana. Per qualsiasi controversia inerente alla validità, interpretazione, esecuzione o risoluzione della presente Nomina sarà competente in via esclusiva

il Foro di Pescara, in coerenza con quanto previsto dall'art. 21 del Contratto.