DESIGNAZIONE DI RESPONSABILE DEL TRATTAMENTO
- Data Processing Agreement -
(Art. 28 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016)

PREMESSO CHE

a. Tra il CLIENTE e il FORNITORE indicato nel contratto cui il presente documento si riferisce (di seguito FORNITORE) è in essere un contratto per l'erogazione di servizi informatici e/o servizi ad essi collegati (di seguito SERVIZIO e/o SERVIZI), di cui la presente è parte integrante;

b. nel presente contratto le parti concordano di definire
- con il termine "GDPR" il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e
- con il termine "Normativa Privacy" le disposizioni del GDPR nonché tutte le altre disposizioni delle leggi dell'Unione o delle leggi degli Stati membri relative alla protezione dei dati personali e alla loro libera circolazione.

c. nello svolgimento del SERVIZIO, il Titolare del trattamento dei dati personali, ai sensi e per gli effetti dell'art. 4 co 1 n. 7 del GDPR, è il CLIENTE e incombe sullo stesso il compimento di tutti gli atti previsti dalla Normativa Privacy per il trattamento dei dati personali vale a dire l'informativa, la raccolta del consenso, l'adozione di tutte le misure autorizzative, di incarico e di conservazione e di altro tipo anche per realizzare il sistema di sicurezza, ivi comprese le relative misure;

Ciò premesso, tra le Parti,

SI CONVIENE E SI STIPULA

quanto di seguito riportato.

1. Designazione di Responsabile del trattamento

1.1 Per i compiti che, in base al contratto per il SERVIZIO, vengono affidati al FORNITORE, quest'ultimo ai sensi dell'art. 4 co 1 n. 8) e dell'art. 28 GDPR è designato Responsabile del trattamento.

1.2 Il Responsabile del trattamento precisa di essere in grado di offrire garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti degli interessati.

2. Oggetto del DPA

2.1 Oggetto della presente designazione è definire le modalità e le condizioni contrattuali con le quali il Responsabile del trattamento si impegna ad effettuare, per conto del Titolare del trattamento, le operazioni di trattamento dei dati personali quali definiti dal contratto e specificate nell'allegato tecnico "Registro del trattamento del servizio" messo a disposizione a richiesta del Titolare del trattamento.

2.2 Nel quadro delle loro relazioni contrattuali, le parti si impegnano a rispettare la regolamentazione in vigore applicabile al trattamento dei dati personali e, in particolare, il GDPR e la Normativa Privacy.

3. Durata del DPA

La presente designazione avrà la durata del contratto a cui si riferisce.

4. Descrizione delle prestazioni del Responsabile del trattamento

4.1 Il Responsabile del trattamento è autorizzato a trattare, per conto del Titolare del trattamento, dati personali necessari per fornire il SERVIZIO quale previsto dal contratto. Per i dati che il Titolare del trattamento ha già fornito e che fornirà, lo stesso garantisce di disporre di una base giuridica idonea ai sensi dell'art. 6 GDPR, come il contratto con l'ospite, gli obblighi di legge in materia di pubblica sicurezza, statistica e fiscale e, dove necessario, il consenso.

Il Titolare del trattamento garantisce il Responsabile del trattamento di disporre legittimamente di tutte le informazioni che affiderà al Responsabile del trattamento per il loro trattamento, assicurando altresì che dette informazioni non violano in alcun modo diritti di terzi.

Il Titolare del trattamento mantiene la titolarità delle informazioni che saranno comunicate al Responsabile del trattamento per il SERVIZIO ed assume espressamente ogni più ampia responsabilità in ordine al contenuto dei relativi dati personali e manleva il Responsabile del trattamento da ogni obbligo e/o onere di accertamento e/o di controllo diretto e indiretto al riguardo.

4.2 La natura delle operazioni realizzate sui dati è l'erogazione del SERVIZIO e/o dei SERVIZI indicati nel contratto, per cui il Titolare del trattamento dichiara di affidare il relativo trattamento dei dati al Responsabile del trattamento.

4.3 La finalità del trattamento, la natura e la tipologia dei dati trattati, le categorie di persone interessate sono quelle specificate nel "Registro del trattamento del servizio".

4.4 Per quanto di sua competenza il Responsabile del trattamento, nel trattare i dati per l'erogazione del SERVIZIO, effettuerà il trattamento in osservanza dell'art. 5 GDPR relativo ai "Principi applicabili al trattamento dei dati personali".

4.5 Per l'esecuzione dell'incarico oggetto del presente contratto, il Titolare del trattamento mette a disposizione del Responsabile del trattamento le informazioni necessarie all'esecuzione delle attività per il SERVIZIO, anche indirizzate all'utilizzo appropriato del sistema informativo.

4.6 Il Responsabile del trattamento, ai sensi dell'art. 28 co 3 lett. b) GDPR, individua e incarica per iscritto le proprie persone autorizzate, definendo puntualmente l'ambito di trattamento consentito. Il Responsabile del trattamento si dichiara edotto che le proprie persone autorizzate agiscono sotto la sua autorità.

5. Obblighi del Responsabile del trattamento

Il Responsabile del trattamento, nello svolgimento delle sue funzioni, si impegna ad assolvere ed osservare i seguenti obblighi.

5.1 <u>Osservanza delle istruzioni date dal Titolare</u>

a. Il Responsabile del trattamento dovrà trattare i dati solo per le finalità sopra specificate e per l'esecuzione delle prestazioni contrattuali.

b. Il Responsabile del trattamento dovrà trattare i dati in conformità a quanto previsto nel "Registro del trattamento del servizio" ed il Titolare del trattamento ritiene adeguate le misure di sicurezza ivi previste.

5.2 <u>Garantire la riservatezza</u>

a. Il Responsabile del trattamento garantisce l'osservanza della riservatezza dei dati personali trattati nell'ambito della presente designazione.

b. Il Responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza e che esse ricevano e che venga loro data la formazione necessaria in materia di trattamenti dei dati personali.

5.3 <u>Adozione delle misure di sicurezza del trattamento</u>

a. Il Responsabile del trattamento deve procedere al trattamento dei dati personali in presenza delle misure richieste ai sensi dell'art. 32 GDPR. Le misure di sicurezza adottate sono quelle dichiarate nel "Registro del trattamento del servizio". Il Titolare del trattamento prende atto che in alcuni casi il Responsabile del trattamento procederà al trattamento attraverso gli strumenti

predisposti e configurati dallo stesso e, pertanto, dovrà adottare ogni cautela necessaria solo qualora il trattamento sia effettuato fuori dal controllo dello strumento impostato e configurato dal Titolare del trattamento.

b. Se il Responsabile del trattamento ha aderito ad un codice di comportamento, o ha esibito una certificazione, deve operare in presenza delle misure di sicurezza previste dal codice di comportamento o dai protocolli di cui alla certificazione. In questo caso il Titolare del trattamento accetterà la certificazione come prova del fatto che il Responsabile del trattamento ha adottato misure adeguate rispetto al trattamento effettuato, rinunciando ad effettuare attività di audit sui sistemi e sulle procedure del FORNITORE.

c. Il Responsabile del trattamento, per i casi contemplati all'art. 37 del GDPR, opera avvalendosi del proprio Responsabile della protezione dei dati (RPD o DPO): se designato, i riferimenti sono indicati nel "Registro del trattamento del servizio".

d. In conformità dell'art. 30 GDPR il Responsabile del trattamento (e, ove applicabile, il suo rappresentante, se non rientrante nei casi di esonero di cui al paragrafo 5 di tale articolo) deve tenere un registro di tutte le categorie di attività relative al trattamento svolte per conto del Titolare del trattamento, contenente quanto indicato nel co 2 di detto articolo.

e. I registri indicati sono tenuti in forma scritta, anche in formato elettronico, e saranno messi a disposizione del Titolare del trattamento a richiesta dello stesso.

5.4 Nomina di Sub-responsabili

a. Ai sensi dell'art. 28 co 2 GDPR, con la presente designazione, il Titolare del trattamento fornisce al Responsabile del trattamento espressa autorizzazione scritta generale alla individuazione di altri soggetti che svolgano, per conto del Responsabile medesimo, il ruolo di Sub-responsabili. A fronte di tale autorizzazione il Responsabile del trattamento si impegna a comunicare al Titolare del trattamento l'elenco di tutti gli eventuali soggetti individuati in qualità di Sub-responsabili. Nel caso in cui nel tempo intervengano modifiche, aggiunte o sostituzioni dei Sub-responsabili inizialmente comunicati, tali nuove nomine dovranno essere comunicate al Titolare del trattamento che avrà a disposizione 15 giorni per eventuali opposizioni dal ricevimento della comunicazione, esprimendo le motivazioni poste a corredo della propria opposizione. Laddove non sia possibile addivenire ad una soluzione condivisa, il Cliente/Titolare del trattamento può recedere dal contratto relativo al Servizio utilizzato, nei termini dallo stesso previsti. Il Responsabile del trattamento dichiara e garantisce che i Sub-responsabili presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative idonee a garantire il rispetto delle disposizioni della vigente Normativa Privacy e si impegna a vincolare contrattualmente gli ulteriori responsabili al rispetto degli stessi obblighi in materia di protezione dei dati personali assunti dal Responsabile del trattamento nei confronti del CLIENTE.

b. Qualora il Sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile del trattamento conserva, nei confronti del Titolare del trattamento, l'intera responsabilità dell'adempimento degli obblighi del Sub-responsabile del trattamento.

c. Si precisa che, in tutti i casi in cui il SERVIZIO non sia erogato direttamente a favore del CLIENTE, ma a favore dei clienti finali dello stesso, il FORNITORE si configura come ulteriore Responsabile del trattamento, e sarà tenuto a trattare i dati alle medesime condizioni determinate nel presente atto di nomina per il Responsabile del trattamento.

5.5 Assistenza al Titolare per l'esercizio dei diritti degli interessati

a. Per quanto possibile, il Responsabile del trattamento – tenendo conto della natura del trattamento – deve assistere il Titolare del trattamento al fine di consentire allo stesso di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al Capo III GDPR.

Il Responsabile del trattamento, nella misura in cui ciò sia possibile, assisterà il Titolare del trattamento con misure tecniche e organizzative adeguate.

b. In relazione al diritto di informazione degli interessati, spetta al Titolare del trattamento fornire l'informativa di cui agli artt. 13 e 14 GDPR alle persone interessate per le operazioni del trattamento, al momento della raccolta dei dati.

Laddove riceva direttamente richieste da parte di un interessato concernenti il trattamento di dati personali effettuato per conto del CLIENTE, il Responsabile di tale trattamento invita l'interessato a rivolgersi al CLIENTE, quale Titolare del trattamento e comunica tempestivamente a quest'ultimo l'istanza ricevuta dall'interessato, entro 10 giorni lavorativi dalla loro ricezione.

5.6 Assistenza al Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR

a. Il Responsabile del trattamento, tenendo conto della natura del trattamento e delle informazioni a sua disposizione, deve assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli artt. da 32 a 36 del GDPR vale a dire:

- l'articolo 32. Sicurezza del trattamento;
- l'articolo 33. Notifica di una violazione dei dati personali all'autorità di controllo;
- l'articolo 34. Comunicazione di una violazione dei dati personali all'interessato;
- l'articolo 35. Valutazione d'impatto sulla protezione dei dati;
- l'articolo 36. Consultazione preventiva.

b. Assistenza per la Sicurezza del trattamento – Il Responsabile del trattamento ha l'obbligo di assistere il Titolare del trattamento nella realizzazione della sicurezza del trattamento, conformemente all'art. 32 GDPR.

Il Responsabile del trattamento, a richiesta del Titolare del trattamento, relazionerà sulle misure di sicurezza adottate, anche mediante eventuali questionari e liste di controllo, previa, se necessaria, valutazione a livello progettuale.

c. Particolari misure di sicurezza del Responsabile del trattamento già in atto – Il Titolare del trattamento prende atto che, per il SERVIZIO, il Responsabile del trattamento ha in essere misure di sicurezza adeguate in osservanza del GDPR.

Amministratori di sistema. In relazione alle attività svolte dal Responsabile del trattamento riferite alla conservazione dei dati personali e alle attività sistemistiche dirette alla manutenzione della rete e all'aggiornamento dei relativi data base e sistemi operativi, gli operatori del Responsabile del trattamento avranno la funzione di Amministratori di sistema.

Gli adempimenti previsti dal Garante per la privacy nel provvedimento del 27 novembre 2008 saranno gestiti dal Responsabile del trattamento; in particolare sarà il Responsabile del trattamento a valutare le caratteristiche soggettive degli amministratori di sistema, ad effettuare le designazioni individuali, a verificare le attività dagli stessi svolte ed a provvedere alla registrazione dei relativi accessi. In relazione a quanto previsto dal provvedimento stesso il Responsabile del trattamento si obbliga a comunicare al Titolare del trattamento l'elenco aggiornato degli Amministratori di sistema; la comunicazione di tali dati potrà avvenire in formato elettronico o cartaceo ed il Titolare del trattamento considera evaso tale adempimento anche con la semplice messa a disposizione dell'elenco aggiornato dei nominativi degli stessi Amministratori di sistema su richiesta del Titolare del trattamento.

5.7 Assistenza per l'obbligo di Notifica di una violazione dei dati personali all'autorità di controllo

Il Responsabile del trattamento ha l'obbligo di assistere il Titolare del trattamento nell'adempimento dei propri obblighi di notifica di una violazione dei dati personali all'autorità di controllo, conformemente all'art. 33 GDPR. Il Responsabile del trattamento notifica al Titolare del trattamento ogni violazione di dati personali nel tempo massimo di 48 ore dopo esserne venuto a conoscenza. Tale notifica è accompagnata da quanto espressamente indicato nel co 3 dell'art. 33, utile per permettere al Titolare del trattamento, se necessario, di notificare questa violazione all'autorità di controllo competente.

È, infatti, esclusivo onere del Cliente, ove Titolare del trattamento, stabilire se l'incidente è classificabile come Data Breach e se il rischio per gli interessati è tale da richiedere la notifica all'Autorità di controllo e la comunicazione agli interessati coinvolti ai sensi dei richiamati articoli 33 e 34 del Regolamento.

Il Responsabile del trattamento assicura il rispetto degli obblighi del presente articolo anche da parte dei Sub-responsabili di cui si avvale ai fini dell'erogazione del SERVIZIO al CLIENTE/Titolare del trattamento, vincolandoli a comunicare al Responsabile del trattamento in modo tempestivo e senza ingiustificato ritardo eventuali incidenti di sicurezza, non appena ne siano venuti a conoscenza, con le modalità e nei termini previsti dai rispettivi accordi.

5.8 Assistenza per l'obbligo di comunicazione di una violazione dei dati personali all'interessato

Il Responsabile del trattamento ha l'obbligo di assistere il Titolare del trattamento nell'adempimento degli obblighi di comunicazione di una violazione dei dati personali all'interessato, conformemente all'art. 34 GDPR; tale comunicazione andrà comunque sempre effettuata da parte del Titolare del trattamento.

5.9 Assistenza del Responsabile del trattamento, nell'adempimento dell'obbligo del Titolare del trattamento della valutazione d'impatto sulla protezione dei dati

Il Responsabile del trattamento assisterà il Titolare del trattamento nell'adempimento degli obblighi della analisi dei rischi e valutazione d'impatto sulla protezione dei dati, conformemente all'art. 35 GDPR, fornendo ogni informazione utile in suo possesso attraverso il "Registro del trattamento del servizio".

5.10 Assistenza del Responsabile del trattamento nell'adempimento dell'obbligo del Titolare del trattamento della consultazione preventiva

Il Responsabile del trattamento assiste il Titolare del trattamento nella consultazione preventiva dell'autorità di controllo, prevista dall'art. 36 del GDPR, fornendo al Titolare ogni informazione utile in suo possesso attraverso il "Registro del trattamento del servizio".

5.11 Assistenza del Responsabile del trattamento nel caso di ispezioni/richieste da parte dell'autorità competente.

Il Responsabile del trattamento assiste e collabora con il Titolare del trattamento in caso di ispezioni/richieste da parte dell'autorità pubblica che possano in qualche modo riguardarlo.

In caso di ispezioni presso il Responsabile del trattamento che riguardano il Titolare del trattamento, verrà data immediata comunicazione al Titolare del trattamento, qualora ciò sia possibile in relazione ai presupposti dell'indagine giudiziaria svolta.

5.12 Tempi di conservazione dei dati: cancellazione o restituzione di tutti i dati personali al termine dell'incarico

Dopo che è terminata la prestazione dei servizi relativi al trattamento il Responsabile del trattamento, su scelta del Titolare del trattamento, dovrà restituire o cancellare tutti i dati personali e cancellare le copie esistenti.

I dati in possesso del Responsabile del trattamento dovranno essere restituiti al Titolare del trattamento, su richiesta dello stesso, mediante le funzioni di esportazione della piattaforma, in formati strutturati di uso comune, prima della cessazione; e/o cancellati entro i termini definiti nel "Registro del trattamento del servizio".

Eventuali ulteriori copie dei dati stessi di backup potranno essere conservate, per l'ulteriore periodo indicato nel "Registro del trattamento del servizio" per fini esclusivamente di sicurezza e non destinati alla comunicazione e alla diffusione.

In deroga a quanto indicato ai punti precedenti, il Responsabile del trattamento dovrà conservare i dati nei casi in cui il diritto dell'Unione o degli Stati membri ne preveda la conservazione, nei termini imposti da detta normativa o da detti provvedimenti.

5.13 Messa a disposizione del Titolare del trattamento di tutte le informazioni necessarie per dimostrare il rispetto degli obblighi

Il Responsabile del trattamento metterà a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 GDPR e deve consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato – nei termini e nelle modalità meglio definite al successivo art. 8 – o dalle autorità.

5.14 Caso in cui un'istruzione al Responsabile del trattamento sia ritenuta in violazione del GDPR

Qualora il Responsabile del trattamento, a suo parere, ritenga che un'istruzione del Titolare del trattamento violi il GDPR o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati, dovrà informare immediatamente il Titolare del trattamento.

5.15 Osservanza dei principi di "privacy by design" e di "privacy by default"

Il Responsabile del trattamento nello svolgimento dell'incarico dovrà operare in osservanza dei principi di protezione dei dati a partire da quando questi vengono progettati (privacy by design) e della protezione dei dati di default. I SERVIZI sono erogati in forma standard, uguale per tutti i clienti, e sono progettati secondo questi principi.

6. Obblighi del Titolare del trattamento

6.1 Il Titolare del trattamento deve:

- fornire al Responsabile del trattamento i dati previsti all'art. 4 delle presenti clausole;
- documentare per iscritto tutte le istruzioni riguardanti il trattamento dei dati da parte del Responsabile del trattamento;
- 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;
- supervisionare il trattamento, effettuando audit e ispezioni.

7. Luoghi ove sono e saranno custoditi i dati

7.1 I dati saranno trattati dal Responsabile del trattamento nei luoghi indicati nel "Registro del trattamento del servizio". Qualora il trattamento dovesse essere eseguito in Paesi Extra UE, il Responsabile del trattamento metterà a disposizione del Titolare del trattamento le garanzie adottate in funzione del luogo in cui il trattamento sarà svolto.

7.2 Se il Responsabile del trattamento sarà tenuto ad effettuare 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 circa tale obbligo giuridico prima del trasferimento al fine di ottenere autorizzazione, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.

8. Controlli

8.1 Il Titolare del trattamento si riserva, anche tramite verifiche periodiche, di vigilare sulla puntuale osservanza delle disposizioni di legge sul trattamento dei dati stessi e sul rispetto delle proprie istruzioni indicate nel presente documento. Il Responsabile del trattamento dovrà consentire al Titolare del trattamento, dandogli piena collaborazione, periodiche verifiche circa l'adeguatezza delle misure di sicurezza adottate e il rispetto della Normativa Privacy e delle disposizioni del Titolare del trattamento stesso.

8.2 Ogni attività di audit da parte del Titolare del trattamento dovrà essere convenuta con il Responsabile del trattamento, con un preavviso di almeno 10 giorni lavorativi. Qualora tali attività comportino oneri e spese non previsti dal presente contratto, tutte le richieste del Titolare del trattamento dovranno essere concordate nelle modalità di esecuzione e gestite a livello progettuale, con la definizione di una valutazione anche economica per la loro attuazione (siano esse attività di penetration test, vulnerability assessment, altro).

8.3 Ogni informazione condivisa in adempimento degli obblighi del Responsabile del trattamento o del Titolare del trattamento è classificata come riservata, pertanto, non potrà essere diffusa, comunicata o pubblicata in rete se non previa autorizzazione scritta dell'altra parte. Ogni incaricato che tratterà l'informazione avrà sottoscritto un accordo di riservatezza che prevederà il divieto di comunicazione a soggetti non autorizzati anche dopo la cessazione del rapporto di lavoro e fino a quando le informazioni non saranno di dominio pubblico per cause agli stessi non imputabili. Ogni violazione della riservatezza di tali informazioni sarà punita nei termini di legge e contrattuali.

Autore	Ufficio Privacy Zucchetti Spa
Approvazione	Fabrizio Scuppa, legale rappresentante di Octorate S.r.l.

Versione Revisione

Versione	Autore	Consultazione DPO	Data emissione	Motivo della revisione
0	Ufficio Privacy		12/11/2026	Prima emissione

OCTORATE

RESPONSABILE DEL TRATTAMENTO					
Denominazione	Octorate Srl				
Partita Iva	13493861002				
Indirizzo	Via Filippo Caruso 23				
Città	Roma	**Cap**	00173	**PV**	RM
Legale Rappresentante	Fabrizio Scuppa				

INCARICATI DEL TRATTAMENTO
Personale di Octorate addetto al supporto clienti, all'onboarding e alla formazione, sviluppatori e sistemisti, autorizzato e istruito al trattamento, con accessi limitati alle mansioni. Per OctoAgent, il team di sviluppo (4 persone) e il team di supporto (3 persone) di iManager S.r.l., Sub-responsabile indicato tra i destinatari.

DATI DI CONTATTO			
Responsabile del trattamento	Octorate Srl	legal@octorate.com	06 4542 0568
Rappresentante del responsabile	N.A.		
Responsabile protezione dati (DPO)	DPO di Octorate	dpo@octorate.com	

DESCRIZIONE
Sistema di gestione delle prenotazioni, delle tariffe e delle disponibilità, distribuzione sui canali collegati, sito e booking engine, comunicazioni con gli ospiti, adempimenti verso Polizia di Stato, ISTAT e Agenzia delle Entrate, integrazioni di pagamento, operatività quotidiana della struttura e, dove attivo, gestione automatizzata delle conversazioni con OctoAgent.

FINALITA' DEL TRATTAMENTO
Erogazione dei Servizi Octorate per conto del Cliente, vale a dire gestione delle prenotazioni,

delle tariffe e delle disponibilità, distribuzione sui canali collegati, sito e booking engine, comunicazioni con gli ospiti, adempimenti verso Polizia di Stato, ISTAT e Agenzia delle Entrate, integrazioni di pagamento, operatività quotidiana della struttura e, dove attivo, gestione automatizzata delle conversazioni con OctoAgent, con l'assistenza e la manutenzione dei Servizi.

Natura del trattamento. Raccolta, registrazione, organizzazione, strutturazione, conservazione, consultazione, elaborazione, estrazione, comunicazione mediante trasmissione ai destinatari indicati dal Cliente, cancellazione. Per OctoAgent anche elaborazione automatizzata mediante modelli di intelligenza artificiale per generare risposte, traduzioni, riepiloghi, trascrizioni, classificazioni e segnalazioni.

Durata e frequenza. Per tutta la durata del rapporto contrattuale, in modo continuo. I tempi di conservazione per categoria sono indicati nei termini per la cancellazione dei dati.

CATEGORIA INTERESSATI

Ospiti e prenotanti, inclusi accompagnatori e ospiti minorenni nei limiti degli adempimenti di legge. Soggetti che contattano la struttura per informazioni o preventivi. Utenti dell'account del Cliente, cioè titolare, staff e collaboratori. Proprietari delle unità gestite, per i property manager che usano il portale proprietari. Fornitori e partner del Cliente eventualmente registrati in piattaforma.

CATEGORIE DI DATI PERSONALI

Dati di prenotazione e soggiorno. Nome e cognome, contatti, lingua, nazionalità, date di arrivo e partenza, unità e tipologia, numero e composizione degli ospiti, importi, canale di provenienza, preferenze e note inserite dal Cliente o dall'ospite.

Dati per gli adempimenti di legge. Per le schedine Alloggiati, dati anagrafici, luogo e data di nascita, cittadinanza, tipo, numero e luogo di rilascio del documento d'identità. Per l'ISTAT, dati statistici sui flussi. Per i documenti fiscali, dati fiscali degli ospiti, codice fiscale e partita IVA.

Dati di pagamento. Dati della carta di credito acquisiti come garanzia della prenotazione, conservati in forma cifrata secondo gli standard PCI-DSS e non decodificabili direttamente da Octorate, esiti delle transazioni comunicati dai gateway e dagli istituti di pagamento.

Comunicazioni. Contenuto e allegati dei messaggi scambiati con gli ospiti via email, messaggistica dei portali OTA, WhatsApp, SMS e chat del sito. Con OctoAgent anche le immagini inviate dagli ospiti, i riepiloghi, le trascrizioni e le registrazioni audio delle chiamate quando il modulo voce è attivo, le righe di ragionamento dell'agente e le lezioni approvate dal Cliente.

Check-in online con OctoAgent. Immagine del documento d'identità inviata dall'ospite per il check-in, dalla quale OctoAgent estrae i dati anagrafici. La fotografia del documento è

oscurata prima dell'invio al modello di intelligenza artificiale.
Sito e booking engine. Dati dei visitatori e dei prenotanti sul sito e sul booking engine del Cliente, secondo l'informativa e la cookie policy del Cliente.
Utenti dell'account. Nome, email, ruolo, credenziali, log di accesso e di attività, necessari all'operatività e alla sicurezza della piattaforma.
Categorie particolari di dati. Non previste dai Servizi. Le informazioni comunicate spontaneamente dagli ospiti, per esempio esigenze di salute, alimentari o religiose, sono trattate sotto la responsabilità del Cliente.

NESSUN USO PER FINALITÀ PROPRIE

Octorate non utilizza i Dati del Cliente per finalità proprie. Octorate può elaborare dati in forma aggregata e anonima, che non consentono di identificare né il Cliente né gli interessati, per finalità statistiche, di sicurezza e di miglioramento dei Servizi.

CATEGORIA DI DESTINATARI A CUI I DATI POTRANNO ESSERE COMUNICATI

Elenco dei Sub-responsabili autorizzati in via generale dal Cliente, con il Paese e le garanzie per il trasferimento dei dati di ciascun fornitore. I portali OTA, gli enti pubblici, i gateway e gli istituti di pagamento non sono Sub-responsabili e ricevono i dati come indicato tra i soggetti che ricevono i dati come titolari autonomi.

- Aruba S.p.A. (Italia). Hosting, database, storage e backup della piattaforma Octorate (PMS, Channel Manager, Booking Engine). Garanzia di trasferimento intra SEE.
- Complior AB (già 24 Solutions) (Svezia). Ambiente certificato PCI DSS collegato alla piattaforma per i dati delle carte di credito. Garanzia di trasferimento intra SEE.
- iManager S.r.l., Via del Muro Linari 31, 00173 Roma, C.F. e P. IVA 16082961000 (Italia). Sviluppo, gestione e hosting applicativo della piattaforma OctoAgent. Garanzia di trasferimento intra SEE.
- Google Cloud (Google Cloud EMEA Limited) (Irlanda, data center di Milano). Hosting di OctoAgent. Garanzia di trasferimento intra SEE, clausole tipo per eventuali accessi da paesi terzi.
- MongoDB Atlas (MongoDB Limited) (Irlanda, data center di Milano e Francoforte). Database di OctoAgent e backup. Garanzia di trasferimento intra SEE, clausole tipo per eventuali accessi da paesi terzi.
- OpenAI (OpenAI Ireland Limited, contraente per lo SEE) (Irlanda, trattamento anche negli Stati Uniti). Modelli di intelligenza artificiale di OctoAgent, generazione di risposte, riepiloghi, trascrizioni, estrazione dei dati dai documenti, tramite l'account di iManager. Modelli di intelligenza artificiale delle altre funzioni della piattaforma Octorate, tramite l'account di Octorate. Garanzia di trasferimento Clausole tipo incluse nel DPA di OpenAI, che non ha la certificazione DPF.
- Openapi S.r.l. (Openapi.com) (Italia). Invio di SMS agli ospiti da OctoAgent. Garanzia di

trasferimento intra SEE.

- Better Stack (UE). Monitoraggio della disponibilità e allarmi di OctoAgent, regione dati UE, solo se nei log transitano dati personali. Garanzia di trasferimento intra SEE.
- Microsoft Clarity (Microsoft) (Irlanda, USA). Analisi dell'uso della console di OctoAgent da parte degli utenti delle strutture, con mascheramento attivo. Garanzia di trasferimento Adeguatezza (DPF) o clausole tipo.
- Meta (WhatsApp Business Platform) (Irlanda, USA). Messaggistica WhatsApp tra strutture e ospiti. Garanzia di trasferimento Adeguatezza (DPF) o clausole tipo.
- Mailchimp Transactional (Mandrill, The Rocket Science Group LLC) e SparkPost (Bird) (USA, UE). Servizi di invio email autorizzati per il dominio octorate.com, per le email che non partono dai server di posta di Octorate. OctoAgent non ne utilizza. Garanzia di trasferimento Adeguatezza (DPF) o clausole tipo.
- Mailgun (Mailgun Technologies, Inc., gruppo Sinch) (USA, UE). Servizio di invio delle email dei Servizi. Garanzia di trasferimento Clausole tipo.
- Intercom (Intercom R&D Unlimited Company) (Irlanda, USA). Chat di supporto della piattaforma Octorate, solo se transitano dati degli ospiti. OctoAgent non ne utilizza. Garanzia di trasferimento Adeguatezza (DPF).

Il servizio telefonico del modulo voce di OctoAgent è fornito da Vonage con un contratto intestato al Cliente, attivato su indicazione di Octorate, per cui Vonage non è un Sub-responsabile di Octorate. Le modifiche a questo elenco sono comunicate al Cliente. La versione aggiornata è disponibile su richiesta a legal@octorate.com.

TRASFERIMENTO DATI ALL'ESTERO

I Dati del Cliente sono conservati in data center situati nell'Unione europea, indicati nelle misure di sicurezza relative al data center.

Octorate trasferisce Dati del Cliente verso paesi terzi, anche tramite Sub-responsabili, soltanto nel rispetto del Capo V del GDPR, in forza di una decisione di adeguatezza della Commissione europea, incluso il quadro EU-US Data Privacy Framework per i fornitori certificati, o delle clausole contrattuali tipo adottate con la decisione di esecuzione (UE) 2021/914 della Commissione, integrate dalle misure supplementari eventualmente necessarie. Le garanzie applicate a ciascun Sub-responsabile sono indicate nell'elenco dei destinatari. Per i modelli di intelligenza artificiale di OctoAgent e delle altre funzioni della piattaforma i dati necessari alla generazione dei contenuti sono trasmessi a OpenAI, che li tratta anche negli Stati Uniti in forza delle clausole contrattuali tipo incluse nel proprio accordo sul trattamento dei dati.

Le trasmissioni verso portali OTA, gateway di pagamento, software di terzi collegati dal Cliente tramite API, ospiti e altri destinatari indicati dal Cliente, anche situati in paesi terzi, avvengono su istruzione del Cliente, che ne è responsabile.

TERMINI PER LA CANCELLAZIONE DEI DATI

Dati di prenotazione, soggiorno e anagrafiche ospiti. Per tutta la durata del contratto e fino a 30 giorni dalla cessazione, salvo diversa istruzione del Cliente.
Messaggi e conversazioni con gli ospiti. Per tutta la durata del contratto, salvo cancellazione anticipata su istruzione del Cliente.
Trascrizioni, riepiloghi e registrazioni delle chiamate, lezioni e righe di ragionamento di OctoAgent. Per tutta la durata del contratto, salvo cancellazione anticipata su istruzione del Cliente.
Dati inviati ai modelli di intelligenza artificiale (OpenAI). Non memorizzati dal fornitore per usi successivi. OpenAI li conserva fino a 30 giorni per il controllo degli abusi e poi li cancella.
Dati per schedine Alloggiati, ISTAT e documenti fiscali. Per il tempo necessario alla trasmissione e per gli obblighi di conservazione previsti dalla legge.
Log tecnici e di sicurezza. Per la piattaforma Octorate, log delle richieste HTTP 45 giorni e log degli accessi degli amministratori di sistema almeno 6 mesi, salvo obblighi di legge. Per OctoAgent, log applicativi 90 giorni e log di audit 400 giorni. Nei log di OctoAgent non sono registrati i contenuti degli ospiti, cioè messaggi, email, telefono e documenti. I log tecnici delle richieste, conservati 400 giorni per la sicurezza, contengono l'indirizzo IP di chi si collega. Ai log accede solo il team di sviluppo di iManager.
Backup. Sovrascrittura automatica secondo i cicli indicati di seguito. Per OctoAgent, backup giornalieri conservati 7 giorni, settimanali 4 settimane e copia giornaliera a Francoforte conservata 90 giorni. Per la piattaforma Octorate, backup giornalieri conservati 30 giorni.
Prima della cessazione il Cliente può esportare i Dati del Cliente mediante le funzioni di esportazione della piattaforma, in formati strutturati di uso comune. Su richiesta scritta ricevuta prima della cessazione, Octorate fornisce assistenza per la restituzione dei dati non esportabili in autonomia, ai corrispettivi eventualmente concordati.
Entro 30 giorni dalla cessazione Octorate cancella i Dati del Cliente e le copie esistenti, salvo i backup, che sono sovrascritti a rotazione come indicato sopra, e salvo i dati che Octorate deve conservare per obblighi di legge, tra cui i documenti fiscali e i log richiesti dalla normativa, che sono conservati per il tempo prescritto e poi cancellati. Le richieste di cancellazione ricevute durante il rapporto sono eseguite entro 5 giorni lavorativi, come previsto dai Termini e condizioni. Su richiesta Octorate attesta per iscritto l'avvenuta cancellazione.

SOGGETTI CHE RICEVONO I DATI COME TITOLARI AUTONOMI

I portali OTA, i gateway e gli istituti di pagamento, la Polizia di Stato, l'ISTAT, l'Agenzia delle Entrate e gli altri soggetti verso cui i Servizi trasmettono dati su istruzione del Cliente trattano i dati come titolari autonomi o secondo i rispettivi accordi con il Cliente. Octorate si limita alla trasmissione tecnica e non risponde del trattamento svolto da tali soggetti. Lo stesso vale per Vonage, che fornisce il servizio telefonico del modulo voce di OctoAgent con un contratto intestato al Cliente.

Octorate S.r.l.
Via Filippo Caruso 23, 00173 Roma · C.F. e P. IVA 13493861002 · octorate.com

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Octorate tiene il registro delle categorie di attività di trattamento svolte per conto dei clienti ai sensi dell'articolo 30, paragrafo 2, del GDPR e lo mette a disposizione del Cliente su richiesta a legal@octorate.com.

DESCRIZIONE GENERALE DELLE MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

1. MISURE DI SICUREZZA IMPLEMENTATE NEI SOFTWARE

Misure di sicurezza adottate nella piattaforma Octorate e in OctoAgent.

- *Gestione delle credenziali di accesso*

• Credenziali personali per ogni utente, regole sulla robustezza delle password, blocco degli accessi non autorizzati e registrazione degli accessi.
• Autenticazione a due fattori con codice OTP per la piattaforma Octorate e per l'accesso a OctoAgent con credenziali Octorate.
• OctoAgent prevede anche un accesso interno per il personale operativo della struttura che non ha un'utenza Octorate, per esempio chi risponde al telefono, manutenzione e pulizie, senza autenticazione a due fattori e non destinato a utenti con poteri di amministratore. L'estensione dell'autenticazione a due fattori agli utenti interni è in valutazione con il fornitore.

- *Minimizzazione*

• Ruoli e permessi configurabili dal Cliente, per limitare l'accesso ai dati alle mansioni di ciascun utente.
- Identificazione di chi ha accesso al sistema
• Log tecnici che consentono di ricostruire le attività svolte in piattaforma. Per OctoAgent, log applicativi conservati 90 giorni, log di audit e log tecnici delle richieste conservati 400 giorni, senza i contenuti degli ospiti. I log tecnici contengono l'indirizzo IP di chi si collega e sono accessibili solo al team di sviluppo di iManager. Per la piattaforma Octorate, log delle richieste HTTP conservati 45 giorni. Gli accessi degli amministratori di sistema sono registrati in modo non modificabile e i relativi log sono conservati almeno 6 mesi, come previsto dal provvedimento del Garante sugli amministratori di sistema.
• Accessi del personale di assistenza all'account del Cliente secondo le misure per i servizi di assistenza indicate più avanti.

- *Tecniche di crittografia*

• Trasmissione dei dati con protocollo TLS su tutti i Servizi.
• Dati delle carte di credito conservati in forma cifrata secondo lo standard PCI DSS, non decodificabili direttamente da Octorate.
• Cifratura dei dati a riposo nei database della piattaforma Octorate e di OctoAgent.

- *Privacy by default*

• Servizi erogati in forma standard, uguale per tutti i clienti, e progettati secondo i principi di protezione dei dati fin dalla progettazione e per impostazione predefinita. Separazione logica dei dati dei diversi clienti nella piattaforma.

- *Diritti degli interessati*

• Il Cliente può esportare i dati dalla piattaforma in formati strutturati di uso comune. Octorate assiste il Cliente nel dare seguito alle richieste degli interessati. Le richieste di cancellazione ricevute durante il rapporto sono eseguite entro 5 giorni lavorativi.

2. RESPONSABILE DEL TRATTAMENTO: MISURE DI SICUREZZA IMPLEMENTATE PER I SERVIZI DI ASSISTENZA

Octorate presta assistenza ai Clienti da remoto, tramite la chat della piattaforma, l'email e il telefono, con personale autorizzato e istruito al trattamento. Le richieste ricevute tramite chat ed email sono tracciate come ticket in Intercom, indicato tra i destinatari. Quando serve per risolvere la richiesta, il personale di assistenza accede all'account del Cliente dal pannello interno di Octorate, con credenziali personali e senza usare la password del Cliente. Octorate non si collega ai dispositivi del Cliente con programmi di controllo remoto.
Il personale di assistenza tratta i dati del Cliente solo per risolvere la richiesta. File ed esportazioni per l'assistenza sono ricevuti dal Cliente come allegati nella chat della piattaforma e sono usati solo per quella richiesta. Restano allegati alla conversazione in Intercom per la durata del contratto. Sono cancellati nei termini indicati in questo Registro per i Dati del Cliente, cioè entro 30 giorni dalla cessazione salvo gli obblighi di conservazione previsti dalla legge, o prima su richiesta del Cliente.

3. RESPONSABILE DEL TRATTAMENTO: MISURE DI SICUREZZA RELATIVE AL DATA CENTER

Piattaforma Octorate. Infrastruttura presso Aruba S.p.A. in data center in Italia certificati ISO/IEC 27001, 27017, 27018 e ANSI/TIA-942 Rating 4. Backup giornalieri del database conservati 30 giorni, con procedure di ripristino.
Carte di credito. Dati delle carte di credito in ambiente certificato PCI DSS presso Complior AB, Svezia.
OctoAgent. Dal 20 ottobre 2026 hosting su Google Cloud a Milano con database MongoDB Atlas a Milano e copia dei backup a Francoforte, al posto di Scaleway a Parigi, dove i dati sono stati cancellati dopo la migrazione. Fornitori con certificazioni ISO/IEC 27001 e SOC 2. Backup giornalieri conservati 7 giorni, settimanali 4 settimane e copia giornaliera a Francoforte conservata 90 giorni.
Email di sistema. Le email di sistema della piattaforma partono dai server di posta di Octorate ospitati da Aruba o dai servizi di invio email indicati tra i destinatari.

4. MISURE DI SICUREZZA DI BASE NIS2

Octorate fa parte del Gruppo Zucchetti, soggetto essenziale ai sensi della Normativa NIS2, e applica le misure di sicurezza di base definite dall'ACN secondo il modello del Gruppo. Le voci seguenti riportano, per ciascuna area prevista dal modello, le misure adottate da Octorate per i Servizi.

Affidabilità dei fornitori. Octorate tratta i Dati del Cliente soltanto con i Sub-responsabili indicati tra i destinatari, vincolati da accordi conformi all'articolo 28 e scelti tra fornitori con certificazioni di sicurezza riconosciute (ISO/IEC 27001, SOC 2, PCI DSS). Ogni nuovo fornitore è valutato prima dell'uso e comunicato al Cliente. Octorate partecipa al processo di qualifica dei fornitori del Gruppo Zucchetti tramite il referente di gruppo.

Ruoli e responsabilità. Responsabile della protezione dei dati raggiungibile a dpo@octorate.com. Referenti interni per la sicurezza e gli incidenti indicati nella procedura di gestione degli incidenti. Per gli obblighi NIS2 Octorate fa riferimento al punto di contatto NIS e al referente CSIRT designati dal Gruppo Zucchetti per il settore hospitality, con il relativo sostituto, indicati nella procedura di gestione degli incidenti.

Affidabilità delle risorse umane. Personale autorizzato al trattamento, istruito sulla Normativa applicabile e vincolato alla riservatezza, con accessi limitati alle mansioni e revocati alla cessazione del rapporto.

Conformità e audit. Informazioni e verifiche a disposizione del Cliente su richiesta. Infrastrutture presso fornitori certificati e sottoposti ad audit di terza parte, in particolare Aruba S.p.A. (ISO/IEC 27001, 27017, 27018 e ANSI/TIA-942 Rating 4), Complior AB (PCI DSS), Google Cloud e MongoDB (ISO/IEC 27001 e SOC 2).

Gestione delle vulnerabilità. Aggiornamenti e correzioni di sicurezza applicati con priorità. Per OctoAgent, scansione delle vulnerabilità e revisione della configurazione della nuova infrastruttura entro il 30 novembre 2026, primo penetration test esterno entro il 31 marzo 2027 e poi una volta l'anno, con gestione degli esiti e delle correzioni. Per la piattaforma Octorate, test di vulnerabilità e penetration test nell'ambito del programma del Gruppo Zucchetti, nel quale Octorate è inserita tramite il referente di gruppo.

Continuità operativa e disaster recovery. Backup della piattaforma Octorate giornalieri e conservati 30 giorni, con procedure di ripristino. Per OctoAgent, backup giornalieri conservati 7 giorni, settimanali 4 settimane e copia giornaliera a Francoforte conservata 90 giorni. Data center certificati ANSI/TIA-942 Rating 4 per la piattaforma Octorate. Monitoraggio continuo della disponibilità dei Servizi.

Gestione di identità e accessi. Credenziali personali, minimo privilegio con ruoli e permessi configurati dal Cliente, regole sulla robustezza delle password, blocco degli accessi non autorizzati, registrazione degli accessi e revisione delle utenze. Autenticazione a due fattori con codice OTP per la piattaforma Octorate e per l'accesso a OctoAgent con credenziali Octorate. Accesso interno a OctoAgent per il personale operativo della struttura con i limiti indicati nelle misure di sicurezza implementate nei software. Accessi tecnici e amministrativi all'infrastruttura di OctoAgent tramite la console del fornitore cloud con autenticazione a due fattori, su rete privata non esposta su internet, con il server di accesso al database acceso solo quando necessario. Accessi e modifiche amministrative registrati e monitorati.

Sicurezza fisica. Dati conservati esclusivamente nei data center dei fornitori indicati in questo Registro, con il controllo degli accessi fisici previsto dalle certificazioni dei fornitori.

Formazione e consapevolezza. Formazione del personale sulla protezione dei dati personali e sulla sicurezza informatica, con contenuti differenziati per personale generico, tecnico e direzione secondo il programma del Gruppo Zucchetti, nel quale Octorate è inserita tramite il referente di gruppo.
Sicurezza dei dati. Trasmissione con protocollo TLS, cifratura dei dati a riposo nei database della piattaforma Octorate e di OctoAgent, dati delle carte di credito in ambiente certificato PCI DSS, separazione logica dei dati dei clienti, backup conservati nell'Unione europea, cancellazione sicura alla cessazione.
Protezione delle reti e delle comunicazioni. Protezione perimetrale dei fornitori di hosting, infrastruttura di OctoAgent serverless su rete privata non esposta su internet, firewall applicativo su OctoAgent con registrazione dei blocchi, canali di comunicazione ufficiali verso il Cliente (email dell'account e avvisi in piattaforma) usati anche per le comunicazioni sugli incidenti.
Monitoraggio degli eventi. Per OctoAgent, controllo ogni minuto della disponibilità del servizio dall'esterno, degli errori applicativi, dei tempi di risposta, degli errori verso Octorate e verso i fornitori dei modelli, di memoria e code di lavoro, dei blocchi del firewall applicativo e degli accessi e delle modifiche amministrative, con allarmi al team tecnico. Log applicativi conservati 90 giorni, log di audit e log tecnici delle richieste 400 giorni, senza i contenuti degli ospiti. I log tecnici contengono l'indirizzo IP di chi si collega e sono accessibili solo al team di sviluppo di iManager. Per la piattaforma Octorate, log delle richieste HTTP conservati 45 giorni e log degli accessi degli amministratori di sistema, non modificabili, conservati almeno 6 mesi.
Gestione e segnalazione degli incidenti. Procedura scritta per rilevare, valutare, contenere e comunicare gli incidenti. Il fornitore che gestisce OctoAgent avvisa Octorate entro 12 ore dal rilevamento di un incidente che tocca i dati o il servizio, anche con informazioni parziali, con aggiornamento e analisi entro 48 ore e relazione finale entro 20 giorni, così che il Gruppo possa rispettare i termini di 72 ore e di un mese verso il CSIRT Italia. Octorate notifica la violazione al Cliente entro 48 ore da quando ne viene a conoscenza e, per gli incidenti significativi ai sensi della Normativa NIS2, attiva il referente del Gruppo Zucchetti per la segnalazione al CSIRT Italia, con pre-notifica entro 24 ore e notifica entro 72 ore.
Sviluppo sicuro. Sviluppo secondo pratiche di sicurezza fin dalla progettazione, aggiornamenti e correzioni di sicurezza, ambienti di sviluppo e di produzione separati e rilasci controllati.
Manutenzione ordinaria ed evolutiva. Aggiornamenti e nuove funzionalità rilasciati con un processo di gestione delle modifiche e comunicati al Cliente secondo la sezione Evoluzione e modifica dei servizi dei Termini e Condizioni. Per OctoAgent, migrazione dell'infrastruttura completata il 20 ottobre 2026, con revisione della configurazione entro il 30 novembre 2026.
Dismissione. Cancellazione dei Dati del Cliente entro 30 giorni dalla cessazione ed entro 5 giorni lavorativi su richiesta, come indicato nei termini per la cancellazione dei dati, con sovrascrittura dei backup a rotazione. Dismissione sicura dei supporti a cura dei fornitori di infrastruttura secondo le rispettive certificazioni.
Subappalto e catena di fornitura. Elenco dei Sub-responsabili tra i destinatari, con obblighi contrattuali equivalenti a quelli della designazione di responsabile del trattamento, incluse le misure di sicurezza di base NIS2 applicabili, e con la possibilità per il Cliente di opporsi alle

modifiche entro 15 giorni dalla comunicazione.