DPA TablePlan

Questo Accordo sul Trattamento dei Dati ("Accordo") è stipulato tra

> te, in qualità di cliente del servizio TablePlan
>
> ***— il Titolare —***
>
> e
>
> TablePlan, marchio di TheDrink S.r.l.s.
> Sede legale: Via Odorico da Pordenone 11, 50127 Firenze (FI), Italia
> C.F. e P. IVA 07474140485 — Registro delle Imprese di Firenze, REA FI-705748
> PEC: thedrink@pec.it
>
> nella persona del rappresentante legale pro tempore, Francesco Scopelliti
>
> ***— il Responsabile —***

1. Oggetto, durata, dati personali trattati e categorie di interessati

(1) Oggetto

- Il presente accordo ha per oggetto la nomina del Responsabile ed il conferimento allo stesso delle istruzioni relative al trattamento dei dati personali. Le attività di trattamento che il Responsabile potrà effettuare sono limitate a quelle strettamente necessarie per il raggiungimento dello scopo del contratto principale sottoscritto dalle parti.
- Il Responsabile svolgerà, per conto del Titolare, le seguenti attività di trattamento:
  - dati di contatto e per le comunicazioni;
  - dati di pagamento e fatturazione;
  - dati forniti dall'utente nell'utilizzo del programma, inclusi dati aziendali ed i Dati Personali di funzionari e dipendenti;
  - dati forniti relativamente al prodotto "Registro delle attività di trattamento dei dati";
  - dati relativi all'utilizzo del sito, quali dati riguardanti il supporto, analitici, ecc.;
  - dati relativi agli utenti del cliente, incluse informazioni sulle loro interazioni con gli strumenti di tableplan nel sito web del cliente e informazioni di tracciamento del consenso raccolte tramite Privacy Controls and Cookie Solution, Consent Database, Whistleblowing Management Tool, Newsletter, Data Subject Rights Management Tool, WayWidget o il Registro delle attività di trattamento dei dati;
  - dati dei clienti finali del Ristoratore raccolti tramite il widget di prenotazione TablePlan, tramite l'import automatico da provider esterni (TheFork, Quandoo, E-restaurants, DISH) e — per i Titolari che attivano l'addon "Prenota con Google" — tramite l'integrazione Google Reserve / Odoo Appointment.

(2) Durata

- La durata di questa nomina è pari alla durata del contratto principale.

(3) Categorie di dati personali

- Le categorie di dati personali trattati sono:
  - dati identificativi (e.g. nome, cognome, email, p.iva, indirizzo)
  - dati statistici o altri dati di navigazione in rete (e.g. dati trattati tramite strumenti analitici etc.)
  - storico acquisti
  - dati di fatturazione, contabilità e pagamenti
  - dati di prenotazione (data, ora, numero persone, note libere, allergeni) ricevuti dai clienti finali del Ristoratore
  - indirizzo postale del cliente finale (limitatamente alle prenotazioni ricevute tramite l'addon "Prenota con Google", per le quali Google Maps fornisce l'indirizzo validato)
  - prova del consenso GDPR (testo verbatim mostrato all'utente, timestamp, indirizzo IP, User-Agent) per i consensi raccolti tramite widget pubblico, modulo offline o pagina booking Odoo
  - log di invio email (delivery, bounce, open, unsubscribe) gestiti dal sub-responsabile Resend
  - eventuali dati relativi alla salute (allergie, intolleranze alimentari, restrizioni dietetiche) forniti spontaneamente dal cliente finale nelle note libere della prenotazione. Il trattamento avviene sulla base del **consenso esplicito dell'interessato** ai sensi dell'art. 9 par. 2 lett. a) GDPR, raccolto dal Titolare nell'ambito del proprio modulo di prenotazione. Il Responsabile non sollecita né richiede attivamente tali dati e li tratta esclusivamente per consentire al Titolare di offrire un servizio adeguato.
  - credenziali di accesso IMAP/POP3 della casella email aziendale del Titolare, conferite volontariamente dal Titolare per consentire l'import automatico delle prenotazioni provenienti dai portali esterni (TheFork, Quandoo, E-restaurants, DISH e simili). Tali credenziali sono cifrate a riposo con algoritmo AES-256-GCM e derivazione chiave PBKDF2 (100.000 iterazioni).

(4) Categorie di interessati

- I dati personali raccolti e trattati si riferiscono a:
  - clienti
  - clienti potenziali
  - utenti internet
  - dipendenti, collaboratori
  - terze parti che agiscono per conto del cliente
  - clienti finali del Ristoratore che effettuano prenotazioni o ricevono comunicazioni transazionali e di marketing tramite la piattaforma

2. Definizioni

A meno che il contesto non richieda diversamente, i seguenti termini nel presente Accordo avranno il significato attribuito di seguito:

1. "Accordo" il presente Accordo sul trattamento dei Dati e relativi Allegati e modifiche.
2. "Leggi sulla Protezione dei Dati Applicabili" si riferisce — a seconda delle circostanze — a qualsiasi legge e regolamento sulla privacy e protezione dei dati applicabile, quali, a titolo esemplificativo: (i) il Regolamento Generale sulla Protezione dei Dati dell'UE (Regolamento 2016/679) ("GDPR");
3. "Titolare" l'entità che, da sola o unitamente ad altri, determina le finalità e le modalità di Trattamento dei Dati Personali.
4. "Interessato(i)" l'individuo a cui si riferiscono i Dati Personali.
5. "Dati Personali" qualsiasi informazione relativa a una persona fisica identificata o identificabile; una persona fisica identificabile è quella che può essere identificata, direttamente o indirettamente, in particolare mediante un identificativo come un nome, un numero di identificazione, dati di localizzazione, un identificativo online o uno o più elementi relativi all'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di tale persona naturale.
6. "Trattamento" qualsiasi operazione o insieme di operazioni eseguite su Dati Personali o su insiemi di Dati Personali, con o senza l'uso di mezzi automatizzati, come la raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o alterazione, recupero, consultazione, uso, divulgazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, allineamento o combinazione, restrizione, cancellazione o distruzione.
7. "Responsabile" una persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che elabora Dati Personali per conto del Titolare.
8. "Sub-responsabile" qualsiasi responsabile del trattamento impiegato dal Responsabile che accetti di ricevere dal Responsabile Dati Personali esclusivamente destinati alle attività di trattamento da svolgere per conto del Titolare e previa autorizzazione di quest'ultimo.
9. "Misure tecniche ed organizzative" tutte le misure volte a proteggere i Dati Personali da distruzione accidentale o illecita o da perdita accidentale, alterazione, divulgazione o accesso non autorizzati e contro tutte le altre forme illecite di Trattamento.

I termini in maiuscolo non definiti nel presente Accordo avranno il significato attribuito nel GDPR, e qualsiasi altra Legge sulla Protezione dei Dati Applicabile.

3. Trattamento all'interno della UE e dello SEE

Alla data di stipula del presente accordo, il Titolare riconosce di essere stato informato che le seguenti attività di trattamento effettuate dal Responsabile per suo conto, avverranno al di fuori dello SEE. Tali trattamenti, in questa sede specificamente autorizzati dal Titolare, avranno luogo negli stati di seguito elencati e secondo le basi di legittimità del trasferimento stabilite agli artt. 45 e ss. RGPD, come di volta in volta applicabili a ciascun trattamento.

Stato	Trattamento	Base giuridica per il trasferimento
USA	Sincronizzazione, database	Adeguatezza del servizio (art. 45 par. 3); Standard Contractual Clauses
USA	Pagamenti, sicurezza	Adeguatezza del servizio (art. 45 par. 3); Standard Contractual Clauses
USA	Invio email transazionali e di marketing	Adeguatezza del servizio (art. 45 par. 3) — EU-US Data Privacy Framework + Standard Contractual Clauses
USA	Frontend "Prenota con Google" (solo per Titolari che attivano l'addon)	Adeguatezza del servizio (art. 45 par. 3) — EU-US Data Privacy Framework + Standard Contractual Clauses

I sub-responsabili che operano interamente all'interno dell'UE/SEE (vedi Sezione 7) non richiedono ulteriori meccanismi di trasferimento.

4. Misure tecniche ed organizzative

(1) Prima di dare esecuzione alla presente nomina, il Responsabile sarà tenuto ad implementare tutte le misure tecniche ed organizzative adeguate per la protezione dei dati personali ed a consegnare al Titolare un documento che descrive dettagliatamente tutte le misure di sicurezza adottate dallo stesso Responsabile, anche con specifico riferimento all'esecuzione del presente contratto. Tali misure sono soggette allo scrutinio del Titolare ed alla sua previa approvazione. Se approvate dal Titolare, tali misure, cristallizzate nel documento di cui al paragrafo precedente, divengono parte integrante e sostanziale di questo contratto di nomina e s'intendono integralmente richiamate nello stesso. Qualora mediante ispezione o revisione il Titolare dovesse constatare la necessità di modificarle, le modifiche saranno apportate di concerto tra le parti.

(2) Il Responsabile garantisce la sicurezza del trattamento ai sensi degli artt. 28 par. 3 punto c) e 32 RGPD, in particolare ai sensi dell'art. 5 par. 1 e par. 2 RGPD. Tali misure devono garantire la sicurezza dei dati ed un livello di protezione adeguato al rischio per la confidenzialità, integrità, disponibilità e resilienza dei sistemi. Ai sensi dell'art. 32 par. 1 RGPD, nel valutare il livello di adeguatezza delle misure di sicurezza deve tenersi conto dello stato dell'arte, i costi di realizzazione, la natura, l'oggetto e gli scopi del trattamento, così come la probabilità di una violazione di dati personali e la gravità dei rischi da essa potenzialmente derivanti per i diritti e le libertà delle persone fisiche.

(3) Le misure tecniche ed organizzative sono soggette a evoluzione e progresso tecnico e tecnologico. Pertanto, il Responsabile può adottare opportune misure alterative adeguate al mutato contesto tecnologico. In tali casi, il livello di sicurezza del trattamento non può essere ridotto. Ogni modifica sostanziale dev'essere documentata.

5. Diritti degli interessati

(1) Il Responsabile s'impegna a cooperare con il Titolare ed a fornire la più ampia assistenza, nei limiti in cui ciò è ragionevole o possibile, al fine di agevolare il Titolare nel riscontro delle richieste

degli interessati per l'esercizio dei loro diritti.

(2) In particolare, il Responsabile s'impegna a (i) comunicare immediatamente al Titolare ciascuna richiesta pervenutagli dagli interessati in merito all'esercizio dei loro diritti e, se fattibile o del caso, ad (ii) assistere il Titolare nel progettare e implementare tutte le misure tecniche ed organizzative necessarie per rispondere a tali richieste.

(3) Fermo restando che la responsabilità di riscontrare e soddisfare le richieste degli interessati grava esclusivamente sul Titolare, il Responsabile può essere incaricato di evadere alcune specifiche richieste, sempre che ciò non richieda sforzi sproporzionati e su istruzioni specifiche fornite per iscritto dal Titolare.

(4) Per agevolare il Titolare nell'evasione delle richieste degli interessati, il Responsabile mette a disposizione i seguenti strumenti self-service all'interno della piattaforma TablePlan: `GET /api/account/export` (diritto di portabilità, Art. 20), `DELETE /api/account/delete` (diritto all'oblio, Art. 17 — cancellazione a cascata), token unsubscribe single-click in ogni email marketing (diritto di opposizione, Art. 21 — effetto immediato), funzionalità di rettifica via CRM (Art. 16).

6. Altri obblighi del Responsabile

In aggiunta alle previsioni di questo contratto, il Responsabile è tenuto a rispettare tutti i requisiti di legge previsti dagli artt. 28-33 RGPD. A tal fine, il Responsabile garantisce quanto segue:

Il Responsabile segnalerà al Titolare senza indebito ritardo ogni cambio di DPO.

The Drink S.r.l.s. — 366 21 44 074 — tableplan.original@gmail.com — Francesco Scopelliti

- **Confidenzialità**
  Le attività di trattamento regolate da questo contratto di nomina dovranno essere svolte solo da dipendenti, collaboratori o incaricati previamente istruiti dal Responsabile sul corretto trattamento di dati personali e contrattualmente soggetti ad obbligo di confidenzialità ai sensi degli artt. 28 par. 3 (b) e 32 RGPD. Il Responsabile, così come chiunque agisca sotto la sua autorità ed abbia accesso a dati personali, non deve trattare dati personali se non è stato istruito in tal senso dal Titolare, anche a mezzo della presente nomina, salvo che per espressa previsione di legge.
- **Misure tecniche ed organizzative**
  Attuazione e rispetto di opportune misure tecniche ed organizzative nel contesto di questo contratto di nomina, ai sensi di quanto specificato dall'art. 32 RGPD. Il Responsabile controlla periodicamente i processi interni e le misure tecniche e organizzative per assicurare che il trattamento nella sua area di competenza sia conforme ai requisiti della normativa sulla protezione dei dati personali e dei diritti degli interessati. Il Responsabile garantisce al Titolare la verificabilità delle misure tecniche e organizzative nell'ambito dei suoi poteri di controllo di cui al punto 8 del presente contratto.
- **Collaborazione con le autorità di controllo**
  Il Titolare ed il Responsabile cooperano, su richiesta, con l'autorità di controllo. Il Titolare è immediatamente informato di tutte le ispezioni e misure eseguite dall'autorità di controllo, nella misura in cui esse si riferiscono alle attività svolte in base a questo contratto. Ciò vale anche nel caso in cui il Responsabile sia sottoposto a o coinvolto in una indagine da parte di

un'autorità competente in relazione a violazioni di qualsiasi disposizione in materia di trattamento di dati personali nello svolgimento di attività ai sensi di questo contratto. Nella misura in cui il Titolare sia soggetto a ispezione da parte dell'autorità di controllo, sanzione amministrativa pecuniaria, misura cautelare o procedimento penale, pretesa da parte di un interessato o di terzi o qualsiasi altra azione legale in collegamento con il trattamento di dati da parte del Responsabile ai sensi della presente nomina, il Responsabile farà tutto il possibile per sostenere il Titolare.

7. Altri responsabili del trattamento

(1) Il Titolare autorizza fin d'ora il Responsabile a ricorrere a terzi responsabili del trattamento. I sub-responsabili come richiesto dalla normativa, dovranno essere soggetti ai medesimi obblighi contrattuali contenuti nel presente contratto ai sensi dell'art. 28 par. 4 RGPD.

(2) Alla data di sottoscrizione del presente accordo, le parti si danno reciprocamente atto che il Responsabile si avvale dei seguenti sub-responsabili, con i quali s'impegna a concludere accordi contrattuali conformi al dettato dell'art. 28, par. 4 RGPD:

#	Sub-responsabile (società)	Attività di trattamento delegata
1	Vercel Inc.	Sincronizzazione
2	Stripe Inc.	Pagamento
3	Sentry.io	Sicurezza
4	Supabase Inc.	Cloud database
5	Resend (Drip Email Inc.)	Invio email transazionali e di marketing per conto del Titolare
6	Upstash Inc.	Cache e rate limiting (server UE — Frankfurt)
7	Google LLC *(solo per Titolari con addon "Prenota con Google" attivo)*	Frontend prenotazione su Google Maps e Google Search tramite il programma Reserve with Google
8	Odoo S.A. *(solo per Titolari con addon "Prenota con Google" attivo)*	Booking server e motore appuntamenti certificato Google (server UE — Belgio)

(3) Resta inteso che la comunicazione dei dati ad un terzo responsabile potrà avvenire solo una volta che tutte le condizioni per la nomina di cui al punto (1) del presente paragrafo siano realizzate.

(4) Il Responsabile dovrà mantenere aggiornato un elenco dei sub-responsabili. Qualsiasi modifica a tale elenco deve essere segnalata al Titolare senza indebito ritardo, dando al Titolare la facoltà di opporsi. In caso di opposizione, il Responsabile ha diritto di recedere dal contratto con il Titolare senza preavviso.

(5) Il Responsabile risponde integralmente dell'operato dei sub-responsabili nei confronti del Titolare.

(6) Qualora un sub-responsabile presti la propria opera al di fuori della UE/SEE, il Responsabile deve garantire la liceità del trasferimento dati al di fuori dello SEE, come descritto al punto 3 del

presente contratto.

8. Poteri di controllo del Titolare

(1) Il Titolare ha il diritto di svolgere ispezioni o farle svolgere ad un revisore di volta in volta incaricato. Il revisore dovrà valutare il rispetto di questo contratto di nomina da parte del Responsabile nel corso delle proprie attività d'impresa per mezzo di verifiche causali, le quali dovranno di regola essere notificate in anticipo.

(2) Il Responsabile deve permettere al Titolare di verificare l'adempimento alle proprie obbligazioni, come previsto dall'art. 28 RGPD. Su richiesta, il Responsabile fornisce al Titolare ogni informazione necessaria nonché, segnatamente, la prova di aver adottato le misure tecniche ed organizzative.

(3) La prova dell'adozione di tali misure, che potranno riferirsi anche ad attività non rientranti nell'ambito di questo contratto, potrà essere fornita anche per mezzo di:

- conformità a codici di condotta approvati ai sensi dell'art. 40 RGPD;
- certificazioni emesse in base ad un meccanismo di certificazione approvato ai sensi dell'art. 42 RGPD;
- attuali certificazioni di revisori, relazioni o estratti di relazioni redatte da organismi indipendenti (p. es. revisori, responsabili della protezione dei dati personali, dipartimento della sicurezza IT, revisori della protezione dei dati);
- idonee certificazioni emesse da revisori della sicurezza IT o della protezione dei dati personali.

(4) Il Responsabile può addebitare al Titolare un compenso di entità ragionevole per l'esecuzione delle ispezioni.

9. Violazioni dei Dati (Data Breaches)

Il Responsabile del trattamento si impegna ad adottare e mantenere idonee procedure e tecnologie per rilevare, prevenire e rispondere alle violazioni dei dati.

In caso di violazioni dei Dati Personali, il Responsabile ne informerà prontamente e senza indebito ritardo il Titolare e comunque entro 48 ore dalla scoperta. La comunicazione dovrà includere:

- una descrizione della natura della violazione, inclusi, ove possibile, il numero approssimativo e le categorie di Interessati coinvolti e le categorie ed il numero approssimativo di registri di dati interessati;
- il nome e i recapiti del responsabile della protezione dei dati del Responsabile o di un altro contatto cui rivolgersi per ottenere ulteriori informazioni;
- una descrizione delle probabili conseguenze della violazione;
- una descrizione delle misure adottate o proposte dal Responsabile per affrontare la violazione, comprese, eventualmente, le misure per mitigare i suoi possibili effetti avversi.

Il Responsabile è tenuto a documentare tutte le violazioni dei Dati Personali, incluse le circostanze in cui si è verificata la violazione, i suoi effetti e le contromisure adottate. Il Responsabile assiste il Titolare nell'osservanza degli obblighi imposti allo stesso dalle Leggi sulla Protezione dei Dati Applicabili in materia di notifiche alle autorità competenti ed agli Interessati.

Il Responsabile non potrà comunicare la violazione dei Dati Personali a terzi o agli Interessati coinvolti senza aver previamente ottenuto il consenso scritto del Titolare, a meno che tale comunicazione non sia richiesta dalle Leggi sulla Protezione dei Dati Applicabili.

Sono ad ogni modo fatti salvi i diritti e rimedi riconosciuti al Titolare in virtù di questo Accordo e delle Leggi sulla Protezione dei Dati Applicabili.

10. Assistenza al Titolare

(1) Il Responsabile assiste il Titolare nell'adempimento degli obblighi relativi alla sicurezza dei dati personali, nella segnalazione di violazioni dei dati, nelle valutazioni d'impatto sulla protezione dei dati e nelle consultazioni preventive di cui agli articoli da 32 a 36 RGPD, tra l'altro:

- garantendo adeguati standard di protezione mediante misure tecniche e organizzative, tenendo conto della natura, delle circostanze e delle finalità del trattamento, della probabilità di violazioni dei dati e della gravità del rischio per le persone fisiche che ne può derivare;
- garantendo l'immediata individuazione delle violazioni;
- riferendo senza indebito ritardo al Titolare ogni violazione di dati;
- assistendo il Titolare nell'evadere le richieste degli interessati di esercizio dei loro diritti.

(2) Il Responsabile può richiedere al Titolare un compenso ragionevole per servizi di assistenza che non sono compresi nella descrizione dei servizi e che non sono dovuti a errori, violazioni o condotte imputabili al Responsabile.

11. Poteri direttivi del Titolare

(1) Il Responsabile non tratta alcun dato personale ai sensi della presente nomina se non su istruzione documentata del Titolare, salvo che sia obbligato a farlo dal diritto dell'Unione o degli Stati membri.

(2) Nel caso in cui il Titolare richieda una modifica del trattamento dei dati personali previsto dalle istruzioni documentate di cui al punto 1, il Responsabile informa immediatamente il Titolare qualora ritenga che tale modifica possa comportare violazioni delle disposizioni in materia di protezione dei dati. Il Responsabile può astenersi dallo svolgere qualsiasi attività che possa dar luogo a tale violazione.

12. Responsabilità

(1) Ciascuna parte del presente contratto si impegna a risarcire l'altra parte per danni o spese derivanti dal proprio inadempimento colposo del presente contratto, compreso qualsiasi inadempimento colposo commesso dal proprio rappresentante legale, sub-contraenti, dipendenti o altri agenti. Inoltre, ciascuna parte si impegna a tenere indenne l'altra parte da qualsiasi pretesa fatta valere da terzi a causa di o in relazione a qualsiasi violazione colposa commessa dall'altra parte.

(2) Resta ferma la previsione dell'art. 82 RGPD.

13. Distruzione e restituzione dei dati personali

(1) Il Responsabile non crea copie o duplicati dei dati ad insaputa e senza il consenso del Titolare, fatta eccezione per le copie di sicurezza, nella misura in cui siano necessarie a garantire la corretta elaborazione dei dati, nonché per i dati la cui conservazione è prevista dalla legge.

(2) A conclusione della prestazione di servizi, a scelta del Titolare, il Responsabile cancella in maniera conforme alla protezione dei dati o restituisce al Titolare tutti i dati personali raccolti ed elaborati ai sensi della presente nomina, a meno che le disposizioni di legge applicabili non richiedano un'ulteriore conservazione dei dati personali.

(3) In ogni caso, il Responsabile può conservare tutte le informazioni utili a dimostrare la corretta e conforme esecuzione delle attività di trattamento anche oltre la cessazione del contratto.

(4) La documentazione di cui al punto (3) che precede, deve comunque essere conservata dal Responsabile in ottemperanza ai periodi di conservazione previsti dalla legge o altrimenti stabiliti. Il Responsabile può consegnare tale documentazione al Titolare al termine della durata del contratto per sollevarsi dall'obbligo contrattuale di conservazione.

14. Allegato I — Misure tecniche ed organizzative

Il Responsabile adotta le seguenti Misure tecniche ed organizzative:

1. **Policy sulla Sicurezza delle Informazioni**: il Responsabile ha definito, e procede ad un riesame regolare di, una policy contenente informazioni ed indicazioni di supporto sulla sicurezza delle informazioni, in conformità ai requisiti aziendali ed ai regolamenti e leggi applicabili.
2. **Organizzazione della Sicurezza delle Informazioni**: il Responsabile attribuisce le responsabilità per compiti specifici per garantire una gestione efficace della sicurezza delle informazioni.
3. **Sicurezza delle Risorse Umane**: il Responsabile ha adottato procedure di sicurezza per dipendenti e fornitori di servizi durante l'intero corso del loro impiego ed incarico di lavoro.
4. **Gestione delle Risorse**: il Responsabile effettua e conserva un inventario delle risorse disponibili ed ha assegnato opportune responsabilità con riferimento alla sicurezza.
5. **Controllo degli Accessi**: il Responsabile garantisce che dipendenti e fornitori di servizi abbiano accesso solo alle informazioni ed alle risorse necessarie per lo svolgimento della propria funzione.
6. **Crittografia**: il Responsabile utilizza la crittografia e la gestione delle credenziali d'accesso per la protezione delle informazioni.
7. **Sicurezza Fisica e Ambientale**: il Responsabile predispone misure di sicurezza per uffici, locali e strutture al fine di prevenire accessi fisici non autorizzati, danneggiamenti e disturbi alle sedi del e alle informazioni conservate dal Responsabile.
8. **Sicurezza delle Operazioni**: il Responsabile garantisce il corretto e sicuro funzionamento delle strutture in cui avviene il trattamento dei dati.
9. **Sicurezza delle Comunicazioni**: il Responsabile ricorre a reti e metodi di trasferimento dei dati sicuri.

10. **Acquisizione, Sviluppo e Manutenzione del Sistema**: il Responsabile garantisce la sicurezza dei dati quale parte integrante dei sistemi durante tutto il loro ciclo di vita.
11. **Relazioni con i Fornitori**: il Responsabile predispone misure di sicurezza per gli asset che sono accessibili ai fornitori.
12. **Gestione degli Incidenti**: il Responsabile gestisce gli incidenti relativi alla sicurezza dei dati ed apporta costanti miglioramenti.
13. **Gestione della Continuità Operativa**: il Responsabile garantisce continuità nella gestione della sicurezza delle informazioni in caso di interruzione delle attività aziendali.
14. **Conformità**: il Responsabile garantisce di aderire ai requisiti legali, statutari, regolamentari e contrattuali ed alle proprie policy e procedure.
15. **Sicurezza degli Archivi Cloud**: il Responsabile ha adottato ulteriori misure di sicurezza degli archivi cloud per proteggere l'integrità, accessibilità e riservatezza dei dati. Queste misure includono, ad esempio, il trasferimento sicuro dei dati, le interfacce software sicure, l'archiviazione sicura dei dati, la gestione dell'identità degli utenti e degli accessi e la sicurezza dell'infrastruttura. Il Responsabile conduce, inoltre, regolari verifiche della sicurezza dell'ambiente cloud per identificare e superare potenziali vulnerabilità.

15. Clausole specifiche per gli addon di TablePlan

Le seguenti clausole si applicano in aggiunta a quanto precede, e sono operative solo nei confronti dei Titolari che hanno attivato l'addon corrispondente. La loro accettazione è automaticamente raccolta all'atto di acquisto dell'addon all'interno della piattaforma.

15.1 Addon "Email Reminder + Marketing" (€19.90/mese)

Quando attivo, il Responsabile invia per conto del Titolare email transazionali (conferma prenotazione, reminder a 24 ore e 4 ore dalla prenotazione, post-visita) e — su istruzione del Titolare — campagne di marketing diretto verso i clienti finali che hanno espresso consenso esplicito (Art. 6.1.a GDPR). Per tali finalità il Titolare riconosce e accetta che:

- l'invio è eseguito tramite il sub-responsabile **Resend (Drip Email Inc.)**, già autorizzato in Sezione 7;
- è responsabilità del Titolare verificare la liceità del contenuto delle campagne marketing;
- il Responsabile filtra automaticamente i destinatari sulla base del consenso marketing attivo e include in ogni invio un link di unsubscribe single-click;
- il Responsabile rispetta le quiet hours (22:00–09:00 ora locale del ristorante) posticipando automaticamente gli invii al primo slot utile;
- i log di invio (delivery, bounce, open, unsubscribe) sono conservati per 12 mesi per finalità di prova e diagnostica (Art. 7.1 GDPR — onere della prova del consenso).

15.2 Addon "Prenota con Google" (€19.90/mese)

L'attivazione di questo addon comporta l'integrazione della piattaforma TablePlan con il programma **Reserve with Google** tramite il booking server certificato **Odoo Appointment**. Ai sensi dell'art. 28 par. 2 GDPR, l'attivazione dell'addon costituisce **autorizzazione scritta specifica** del Titolare all'aggiunta dei sub-responsabili **Google LLC** e **Odoo S.A.** (vedi Sezione 7,

righe 8 e 9). L'autorizzazione è raccolta tramite checkbox dedicato al momento dell'attivazione e archiviata insieme a timestamp e indirizzo IP.

Per l'addon in questione il Titolare riconosce e accetta che:

- il flusso dati segue il percorso: Cliente Google Maps/Search → Google LLC → Odoo S.A. → webhook TablePlan → database del Titolare;
- oltre ai dati elencati in Sezione 1.3, vengono trattati anche l'indirizzo postale del cliente finale (validato da Google Maps) e l'eventuale risposta a una domanda custom sul consenso marketing posta sulla pagina di prenotazione Odoo;
- è onere del Titolare disporre di un Google Business Profile verificato e configurare correttamente il proprio *privacy_policy_url* nei settings dell'addon, in modo che venga linkato sulla pagina di prenotazione Odoo;
- i tempi tecnici di apparizione del pulsante "Prenota" su Google Maps e Google Search dipendono integralmente da Google e non sono garantiti dal Responsabile;
- il record di idempotenza delle prenotazioni provenienti da Google (tabella `odoo_rwg_bookings`) è conservato per 12 mesi e successivamente cancellato automaticamente;
- in caso di disattivazione dell'addon il Responsabile esegue il deprovisioning dei dati merchant da Odoo entro 30 giorni dalla cessazione, fatti salvi i dati prenotazione già acquisiti dal Titolare nella propria banca dati TablePlan, soggetti alla retention ordinaria.

Il Titolare ha facoltà di opporsi all'aggiunta dei sub-responsabili Google LLC e Odoo S.A.: in tal caso non potrà attivare l'addon, restando peraltro impregiudicato l'utilizzo delle altre funzionalità della piattaforma.

15.3 Addon "Mappa Sala + Tavoli" (€14.90/mese)

L'addon gestisce esclusivamente metadati interni del ristorante (layout tavoli, zone, regole di auto-assegnazione) e non comporta alcun trattamento aggiuntivo di dati personali dei clienti finali rispetto a quanto già previsto dal contratto principale.

15.4 Funzionalità "Email Sync" (sincronizzazione IMAP)

Su istruzione del Titolare e previo conferimento volontario delle credenziali della propria casella di posta aziendale, il Responsabile si connette tramite protocollo IMAP/IMAPS o POP3/POP3S alla casella stessa con l'unica finalità di scaricare ed elaborare le email contenenti conferme di prenotazione provenienti da portali di terzi (TheFork, Quandoo, E-restaurants, DISH e altri provider analoghi). Il Titolare riconosce e accetta che:

- il conferimento delle credenziali è facoltativo: la mancata attivazione di Email Sync non pregiudica le altre funzionalità della piattaforma;
- le credenziali sono cifrate a riposo (AES-256-GCM con derivazione PBKDF2) e accessibili in chiaro solo durante l'esecuzione della singola sessione di sincronizzazione;
- la sincronizzazione è limitata, per default, alle ultime 7 giornate solari di posta in arrivo, con un budget di tempo per esecuzione e un numero massimo di email processate per ciascuna esecuzione, allo scopo di minimizzare l'accesso ai dati;

- il Responsabile applica protezione SSRF (blocco di indirizzi IP privati e whitelist di porte IMAP/POP3 standard) per impedire abusi del canale di connessione;
- il Responsabile non legge, archivia o utilizza email diverse da quelle riconosciute come conferme di prenotazione tramite parser dedicati. Le email non riconosciute sono scartate senza essere persistite;
- è onere esclusivo del Titolare verificare che il proprio provider di posta consenta l'accesso IMAP da terze parti e che il conferimento delle credenziali non violi i termini contrattuali con tale provider;
- il Titolare può revocare in qualsiasi momento l'accesso disattivando la connessione dal pannello di configurazione, con eliminazione immediata delle credenziali cifrate.

15.5 Funzionalità "Backfill" (import storico prenotazioni)

Su richiesta del Titolare, il Responsabile importa nella piattaforma prenotazioni storiche del Ristoratore a partire da file forniti dal Titolare stesso (archivi `.eml`, `.zip`, file `.csv`, report `.pdf` esportati da TheFork o da altri portali, oppure tramite una connessione IMAP "one-shot" a una casella o cartella archivio). Il Titolare riconosce e accetta che:

- è onere esclusivo del Titolare aver raccolto i dati personali oggetto del backfill in conformità al GDPR e di disporre di idonea base giuridica per il trattamento e per il loro trasferimento al Responsabile;
- il Titolare manleva il Responsabile da ogni pretesa di terzi derivante da carenze di base giuridica o di informativa relative ai dati conferiti tramite backfill;
- i file di origine caricati dal Titolare sono trattenuti dal Responsabile per il solo tempo necessario all'elaborazione e cancellati al termine della stessa, salvo il mantenimento delle prenotazioni estratte nella banca dati del Titolare con la retention ordinaria;
- le prenotazioni importate sono soggette alle medesime tempistiche di conservazione e ai medesimi diritti dell'interessato previsti per le prenotazioni native della piattaforma.

15.6 Funzionalità "Risk Score" (indicatore di affidabilità del cliente)

Il Responsabile mette a disposizione del Titolare un indicatore di affidabilità del cliente finale (di seguito "Risk Score") calcolato in via puramente **deterministica** sulla base di un unico parametro oggettivo: il numero di mancate presentazioni (*no-show*) precedentemente registrate sulla piattaforma per quel cliente presso il medesimo ristorante. La scala è statica e priva di componenti di intelligenza artificiale, apprendimento automatico o ponderazione probabilistica.

Le parti danno atto che:

- il Risk Score costituisce mero **strumento informativo** a supporto del Titolare e **non determina alcuna decisione automatizzata** che produca effetti giuridici o incida in modo analogo significativamente sull'interessato ai sensi dell'art. 22 par. 1 GDPR;
- ogni decisione operativa nei confronti del cliente finale (conferma o rifiuto della prenotazione, richiesta di carta di garanzia, gestione della sala) rimane sempre e integralmente in capo al Titolare, che può discostarsi dall'indicazione fornita dal Risk Score senza alcun vincolo;
- la logica di calcolo (numero di no-show → soglie 0/35/65) è semplice, trasparente e documentata, e può essere comunicata all'interessato che ne faccia richiesta tramite il Titolare;

- il Titolare si impegna a non utilizzare il Risk Score come unico criterio di accettazione o rifiuto sistematico di prenotazioni e a garantire in ogni caso un intervento umano nella valutazione, ove rilevante;
- il Responsabile non condivide il Risk Score con soggetti terzi diversi dai sub-responsabili strettamente necessari all'erogazione del Servizio.

Documento accettato per rinvio all'atto di accettazione dei Termini e Condizioni di tableplan.tech.

The Drink S.r.l.s. — Via Odorico da Pordenone 11, Firenze — tableplan.original@gmail.com — 366 21 44 074
Versione 2.1 del 9 Giugno 2026 (rimosso il sub-responsabile Iubenda S.r.l. a seguito della dismissione del servizio). Sostituisce la versione 2.0 del 15 Maggio 2026 (consultabile su `https://tableplan.tech/dpa-v2-2026-05.pdf`) e la versione 1.0 del 2 Gennaio 2026 (consultabile su `https://tableplan.tech/dpa-v1-2026-01.pdf`).