ACCORDO CONTRATTUALE DI NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI

(Art. 28 del Regolamento UE 2016/679)

TRA LE SOTTOSCRITTE PARTI

Società Cliente_____,
con sede in Via_____,
in persona del Legale Rappresentante_____
(di seguito, "Titolare del trattamento", oppure “Data Controller”, oppure “Cliente”)

E

Yes Ticket S.r.l., con sede operativa in Via Ippolito Rosellini, 12, 20123 Milano (MI), in persona del Legale Rappresentante (di seguito, "Responsabile del trattamento", oppure “Yes Ticket”, oppure “Fornitore”)

AI SENSI E PER GLI EFFETTI DELL’ART. 28 DEL REG.UE 2016/679 (DI SEGUITO GDPR), CONSIDERATO IL RAPPORTO PROFESSIONALE / CONTRATTUALE INSTAURATO, SI CONVIENE QUANTO SEGUE.

1. DEFINIZIONI

Ai fini del presente Accordo valgono le seguenti definizioni:

- Per “**Autorità di controllo**” si intende l’Autorità Garante e ogni autorità competente a vigilare ed assicurare l’applicazione delle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali con riferimento al Trattamento dei Dati Personali del Cliente;
- per “**Dati personali**” si intendono tutte le informazioni relative ad una persona fisica, identificata o identificabile (l’“**Interessato**”) che il Responsabile tratta per conto del Titolare allo scopo di fornire i Servizi;
- Per “**Diritti dell’interessato**” si intendono i diritti riconosciuti all’interessato dalle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali, come, a titolo di esempio, il diritto di chiedere al Titolare l’accesso, la rettifica o la cancellazione dei Dati Personali, il diritto alla limitazione dei Trattamento dei dati dell’interessato o il diritto di opposizione al Trattamento, nonché il diritto alla portabilità dei dati;
- per “**Misure di sicurezza**” si intendono le misure minime di sicurezza indicate dall’art. 32, GDPR e nei provvedimenti del Garante;
- per “**Operazioni di Trattamento**” si intende qualsiasi operazione o insieme di operazioni compiute con o senza l’ausilio di processi automatizzati applicati a Dati Personali come la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l’interconnesione, la limitazione, la cancellazione o la distruzione;
- per “**Legge applicabile**” si intende 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* (il “**Regolamento**” o “**GDPR**”), nonché qualsiasi altra normativa o atto avente forza normativa in materia di protezione dei dati personali applicabile in Italia, ivi compresi i provvedimenti del Garante;
- Per “**Responsabile**” si intende generalmente la persona fisica o giuridica, la pubblica autorità, l’organismo o altro ente che tratti Dati Personali per conto del Titolare. Ai fini del presente accordo contrattuale il Responsabile è la Società Yes Ticket S.r.l.;
- Per “**Sub-Responsabile**” si intende un organismo individuato dal Responsabile che assista quest’ultimo nel trattamento dei Dati Personali del Titolare;
- Per “**Titolare**” si intende generalmente la persona fisica o giuridica, la pubblica autorità, l’organismo o altro ente che, da solo o congiuntamente con altri soggetti, determini le finalità e le modalità del Trattamento dei Dati Personali. Ai fini del presente accordo contrattuale, il Titolare è il Cliente;
- Per “**Violazione dei dati personali**” si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la divulgazione non autorizzata o l’accesso ai Dati Personali trasmessi, conservati o comunque trattati.

2. OGGETTO

L'oggetto del presente Accordo (di seguito anche "Atto") è la definizione delle modalità operative in forza delle quali il Responsabile del trattamento si impegna ad effettuare, per conto del Titolare, le operazioni di trattamento dei dati personali di seguito definite. Nell'ambito dei loro rapporti contrattuali, le parti si impegnano a rispettare i regolamenti in vigore applicabili al trattamento dei dati personali e, in particolare, il Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 applicabile dal 25 maggio 2018 (GDPR).

3. DESCRIZIONE DEL TRATTAMENTO CHE VIENE SVOLTO PER CONTO DEL TITOLARE DEL TRATTAMENTO

3.1 Il Responsabile del trattamento è autorizzato ad accedere e/o trattare per conto del Titolare del trattamento i dati personali necessari alla fornitura e alla gestione operativa di buoni pasto e di buoni acquisto.
3.2 La finalità del trattamento è dunque l'erogazione, da parte del Responsabile e a favore del Cliente, di servizi sostitutivi di mensa aziendale a mezzo emissione e commercializzazione di buoni pasto cartacei ed elettronici, di buoni acquisto *full digital* - tra cui si annovera il buono spesa sociale e il buono regalo - e, in ultimo, della mensa diffusa elettronica aziendale.
3.3 Yes Ticket, in qualità di Responsabile, tratta, per conto del Titolare, dati di natura economica e di ubicazione quali:

- informazioni di spesa relative all'ammontare delle transazioni realizzate dagli utilizzatori del buono, alla data e all'ora dei movimenti in uscita;
- informazioni relative al saldo disponibile e al numero e valore complessivo delle ricariche percepite in favore dei beneficiari;
- la denominazione sociale dell'azienda a cui l'utilizzatore fa capo;
- dati relativi all'ubicazione in cui è avvenuta la consumazione del buono.

L'accesso a questi dati avviene nella sola e unica misura in cui la loro acquisizione risulti necessaria al corretto computo dei buoni associabili ed effettivamente spendibili da parte di ciascun utilizzatore, oltre che alla fruizione dei servizi di assistenza erogati dal Responsabile in favore di quest'ultimo.
3.4 La categoria di interessati è rappresentata dai dipendenti del Titolare, ivi compreso il personale direttivo.

4. DURATA DEL TRATTAMENTO

4.1 Il presente accordo rimane in vigore fino a quando il Fornitore effettua il trattamento di dati personali per conto del Cliente, o fino a quando l'Accordo scade oppure termina, indipendentemente dal fatto che sia sostituito da un accordo successivo.

5. OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO NEI CONFRONTI DEL TITOLARE DEL TRATTAMENTO

5.1 Adempimenti

Nell'esecuzione delle attività destinate alla puntuale erogazione dei Servizi, il Fornitore si impegna a porre in essere quanto segue:

- utilizzare i dati personali contenuti nei database forniti dal Titolare al solo fine di erogare i Servizi. Di tali dati personali potrà essere fatta una copia a fini esclusivi di svolgimento delle attività connesse ai Servizi ovvero per back–up, rimanendo vietato qualsiasi altro utilizzo, comunicazione, copia (parziale o totale) dei dati stessi senza il preventivo consenso scritto del Titolare;
- intraprendere nuove attività di trattamento rispetto a tali dati solo previo consenso scritto da parte del Titolare;
- predisporre politiche di sicurezza e procedure operative specifiche atte a garantire la sicurezza dei dati personali (quali, ad esempio: policy per la gestione dei diritti degli interessati, gestione dei *data breach*) che siano:
  - opportunamente documentate ed adeguatamente riviste e aggiornate;
  - approvate dalle Direzioni e/o Responsabili.
- formulare e mantenere costantemente aggiornato il Registro delle operazioni di trattamento di cui l'art. 30 comma 2 del GDPR fa espresso richiamo, relativamente alle operazioni di trattamento effettuate per conto del Titolare e, su richiesta, mettere detto Registro a disposizione di quest'ultimo e/o del Garante per la protezione dei dati personali;
- garantire un'adeguata politica di assistenza in favore del Cliente durante le operazioni di audit, secondo quanto espressamente previsto all'art. 5.8 del presente Atto;
- effettuare i controlli necessari ad accertare che i dati personali siano trattati dal proprio personale, nonché da ogni ulteriore responsabile del trattamento, nella sola misura strettamente necessaria ad eseguire i Servizi di cui al presente accordo, nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche;
- assicurare una coerente definizione e assegnazione di ruoli e, conseguentemente, predisporre una politica degli accessi ai dati personali che garantisca che questi ultimi siano sempre riservati al personale che ne ha la reale necessità;
- assistere e collaborare con il Titolare nel processo di eventuale valutazione d'impatto sulla protezione dei dati ("DPIA – *Data Protection Impact Assessment*") di cui all'art. 35 GDPR, nonché nella eventuale fase di consultazione preventiva con l'Autorità di controllo ai sensi dell'art. 36 GDPR, qualora la valutazione d'impatto

sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare per attenuare il rischio;

- comunicare tempestivamente al Titolare il report finale della DPIA svolta ove quest'ultima sia compiuta autonomamente in relazione a servizi, prodotti, asset che coinvolgano i trattamenti compiuti per conto del Titolare;
- trattare i dati personali in accordo con le istruzioni provenienti dal Cliente e informare immediatamente quest'ultimo qualora ritenga che un'istruzione costituisca una violazione del GDPR o di qualsiasi altra disposizione del diritto dell'Unione o della legge sulla protezione dei dati degli Stati membri;
- garantire l'esportazione di dati personali al di fuori dell'Unione Europea solo in presenza di apposita decisione di adeguatezza, o, in mancanza di quest'ultima, sotto la copertura di garanzie adeguate di natura contrattuale, tra cui norme vincolanti d'impresa e clausole contrattuali tipo di protezione dei dati personali;
- procedere, ove necessario, all'individuazione e nomina degli incaricati che operino quali Amministratori di Sistema, ai sensi del Provvedimento del Garante del 27 novembre 2008 in materia di Amministratori di Sistema, impartendo le relative istruzioni e vigilando, anche tramite verifiche periodiche (da eseguirsi almeno con cadenza annuale), sulla puntuale osservanza delle disposizioni ed istruzioni impartite

5.2 **Designazione da parte del Responsabile del trattamento di un altro Responsabile del trattamento ("Sub-Responsabile del trattamento")**

Il Fornitore può nominare un altro Responsabile del trattamento (in seguito denominato "Sub-Responsabile del trattamento") per svolgere specifiche attività (vedasi allegato al presente atto di nomina). In questo caso, il Fornitore informa per iscritto il Cliente dell'eventuale designazione del Sub-Responsabile del trattamento e di ogni ulteriore eventuale modifica e/o sostituzione, indicando espressamente le attività di trattamento svolte per suo conto, l'identità e le informazioni di contatto del Sub-Responsabile del trattamento.
Il Sub-Responsabile del trattamento è tenuto a rispettare gli obblighi del presente contratto per conto e in accordo con le istruzioni impartite dal Titolare del trattamento. Spetta al Fornitore assicurare che il Sub-Responsabile del trattamento presenti 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 dell'interessato. Se il Sub-Responsabile del trattamento non adempie ai propri obblighi di protezione dei dati, il Fornitore rimane pienamente responsabile nei confronti del Cliente.

5.3 **Esercizio dei diritti degli interessati**

Il Fornitore presterà al Cliente adeguata collaborazione ed assistenza al fine di permettergli di fornire un puntuale riscontro agli interessati in merito all'effettivo esercizio dei diritti di cui gli artt.15-22 del GDPR fanno espresso richiamo (a titolo esemplificativo: *diritto alla cancellazione, diritto di opposizione, diritto di rettifica, diritto di accesso*) mettendo a disposizione del Cliente, su richiesta di quest'ultimo, il supporto, i dati personali e le informazioni ritenute necessarie all'esercizio degli stessi. Qualora la richiesta di esercizio dovesse pervenire al Fornitore, quest'ultimo si impegna ad inviare tempestivamente tali richieste all'indirizzo legal@360-paymentsolutions.com. Resta inteso tra le Parti che tutte le attività del Fornitore, ai sensi del presente paragrafo, sono comprese nei corrispettivi previsti per l'esecuzione dei Servizi, fatta eccezione per eventuali richieste ulteriori da parte del Cliente, che le Parti concorderanno di volta in volta in forma scritta ed in buona fede.

5.4 **Notifica di violazioni dei dati personali (*Data breach*)**

Il Fornitore si impegna ad informare, senza ingiustificato ritardo, il Cliente di ogni violazione dei dati personali. Tale informazione deve essere accompagnata da tutta la documentazione pertinente al fine di consentire al Cliente, se necessario, di notificare tale violazione all'Autorità Garante competente.
L'informazione deve contenere:

- una descrizione della natura della violazione dei dati personali, comprese, ove possibile, le categorie e il numero approssimativo di persone interessate dalla violazione e le categorie e il numero approssimativo di record di dati personali interessati;
- il nome e i dati di contatto del Responsabile della Protezione dei Dati (c.d. DPO) o altro punto di contatto da cui possono essere ottenute informazioni aggiuntive;
- una descrizione delle probabili conseguenze della violazione dei dati personali;
- una descrizione delle misure adottate o proposte per porre rimedio alla violazione dei dati personali, comprese, se del caso, misure per attenuare eventuali conseguenze negative.

Se, e nella misura in cui non è possibile fornire tutte queste informazioni nello stesso momento, le informazioni possono essere comunicate in modo scaglionato senza indebito ritardo. Il Fornitore garantisce che non rilascerà commenti o dichiarazioni pubbliche relative alle violazioni di dati personali senza il consenso scritto del Cliente.

5.5 **Misure di sicurezza**

Il Fornitore, in caso di trasferimento di dati del Cliente presso la propria infrastruttura, oppure in caso di accesso ai sistemi del Cliente si impegna ad attuare le misure di sicurezza tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, che comprendano, tra le altre, se del caso:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Il Fornitore si impegna inoltre a:

- adottare tutte le misure necessarie a proteggere i dati personali e le informazioni rilevanti relative al presente accordo;
- prevedere sistemi di monitoraggio e di analisi dei log di sicurezza;
- implementare una procedura per la segnalazione, la risposta e la gestione degli incidenti legati alla sicurezza dei dati personali;
- garantire che i predetti sistemi di sicurezza siano adottati anche dai sub-responsabili che costituiscono la filiera di fornitura a cui il Titolare ricorre per l'offerta dei propri servizi;
- condurre attività verifica dei sistemi informativi aziendali che gestiscono i dati personali trattati per conto del Titolare, anche a mezzo di attività di *penetration test* e *vulnerability assessment*, al fine di verificarne la conformità con le politiche e gli standard di sicurezza adottati;
- mantenere costantemente aggiornati tutti gli strumenti software e hardware di cui dispone attraverso gli aggiornamenti di sicurezza pubblicati dai rispettivi produttori;
- garantire la puntuale identificazione delle risorse IT impiegate ai fini del trattamento dei dati di cui la Società Cliente è Titolare, al fine di permettere a quest'ultimo la tempestiva collocazione dei dati personali trasmessi;
- fornire adeguate istruzioni operative ai soggetti che eseguono materialmente operazioni di trattamento dei dati personali, con particolare riguardo ai dipendenti autorizzati ad accedere ai sistemi del Cliente con credenziali di admin.;
- non conservare copie, estratti, riassunti o sommari di dati personali, salvo ove richiesto a tal fine dagli obblighi dell'accordo o dalla legislazione applicabile;
- non divulgare, distruggere, sottrarre o manipolare il contenuto delle banche dati, salvo ove richiesto a tal fine dagli obblighi dell'accordo o dalla legislazione applicabile.

In particolare, per quanto concerne il servizio di *hosting* che presiede il regolare funzionamento delle reti dei portali web, le misure di sicurezza adottate prevedono:
a. la protezione offerta dal certificato SSL relativamente alle operazioni di navigazione sul portale;
b. l'archiviazione di tutti i dati personali in forma rigorosamente criptata;
c. la protezione della pagina login a mezzo Google reCAPTCHA v2 contro gli attacchi *brute force*;
d. il blocco di tutti gli utenti e relativi indirizzi IP in presenza di accesso consecutivo errato per un numero pari e superiore a 5 tentativi;
e. backup impostato ogni due ore volto a ricreare una versione criptata dei contenuti del database e a trasferirli in un'area non pubblica del server.

5.6 **Politica di fine rapporto**
Il Fornitore restituirà o cancellerà i dati personali forniti nell'ambito dell'erogazione dei Servizi alla scadenza o risoluzione anticipata del presente Atto, comprese eventuali copie di back-up, subordinatamente ad una richiesta scritta inviata con congruo preavviso, salvo che sussistano specifici obblighi di conservazione previsti dalla legge.
L'eventuale richiesta del Cliente volta alla restituzione dei dati personali sarà soddisfatta nei limiti del possibile, subordinatamente ai limiti tecnici ed organizzativi commercialmente ragionevoli, commisurati al volume, alla categorizzazione e alla quantità di dati personali oggetto di trattamento.
Ove alla conclusione dello svolgimento delle attività non siano pervenute indicazioni da parte del Cliente, il Fornitore, fatti salvi specifici obblighi normativi, potrà conservare i dati in forma anonimizzata.
Il Responsabile assicura che i medesimi principi siano applicati anche da parte di ciascuno dei Sub-responsabili con i quali intrattiene rapporti commerciali funzionali al perfezionamento dei Servizi.

5.7 **Responsabile della Protezione dei Dati (c.d. DPO)**
Il Fornitore comunica per iscritto al Cliente il nome e i dettagli di contatto del suo DPO, se è obbligato ai sensi dell'articolo 37 del Regolamento Europeo sulla Protezione Dei Dati oppure in tutti i casi in cui abbia ritenuto di procedere volontariamente alla designazione.

5.8 **Documentazione ed audit**
Il Responsabile si impegna a consentire al Titolare o a soggetti terzi da questo delegati, l'accesso ad uffici, sistemi e documenti informatici propri e dei propri subappaltatori o, alternativamente, la condivisione dello schermo guidata per quanto concerne il possibile accesso ai programmi relativamente alle Operazioni di trattamento, nella misura in cui detti accessi risultino necessari per verificare l'osservanza, da parte del Responsabile, degli obblighi pattuiti.
Il Fornitore e il Titolare valuteranno e concorderanno preventivamente l'identità dell'auditor. Successivamente, il Titolare comunicherà per iscritto al Fornitore - con un preavviso di 20 giorni lavorativi - la data di inizio dell'audit, l'ambito e la durata dell'audit.
Il Fornitore si impegna pertanto a fornire il proprio supporto alle attività di verifica che il Titolare potrà condurre nei suoi confronti, contribuendo a dette attività anche mediante colloqui e/o compilazione di questionari forniti dal Titolare.

Rimane inteso che qualsiasi attività di audit avrà luogo limitatamente alla verifica degli impegni assunti ai sensi dell'Atto.
Il Fornitore si riserva il diritto di addebitare costi e oneri per gli audit richiesti e svolti.

6. RESPONSABILITA' E INDENNIZZO

Ai sensi dell'art. 82 GDPR, la responsabilità delle Parti, nonché di eventuali altri Responsabili di cui eventualmente si avvalga il Fornitore ai sensi del precedente art. 5.2, è solidale per qualsiasi danno cagionato nei confronti degli Interessati nell'esecuzione delle attività di trattamento descritte nel presente Atto di Nomina. La Parte che abbia risarcito il danno per intero avrà diritto di rivalsa nei confronti dell'altra per la parte di risarcimento corrispondente alla propria responsabilità nella causazione del danno.
In caso di violazioni accertate dall'Autorità di controllo competente, ciascuna Parte sarà tenuta al pagamento dell'ammontare della sanzione contestata nei limiti della responsabilità rilevata a proprio carico dall'autorità di controllo.

7. DISPOSIZIONI FINALI

7.1 Le suddette prescrizioni, in ordine agli obblighi di riservatezza e non divulgazione, si ritengono applicabili a qualsiasi informazione di natura tecnica e/o commerciale (di cui il **Fornitore** può venire, anche accidentalmente, a conoscenza nell'esercizio delle sue mansioni) da mantenere per la loro importanza strategica in un regime di confidenzialità. A titolo esemplificativo si citano: processi/strumenti/metodologie di produzione, progetti ed iniziative strategiche, dati di business, dati contabili, listini, tariffe, ecc.).
7.2 L'invalidità, anche parziale, di una o più delle clausole del presente Accordo non pregiudica la validità dei contenuti del restante Atto.
7.3 L'incarico di Responsabile del trattamento dei dati è di carattere fiduciario e non è in alcun modo suscettibile di delega, fatta salva la nomina di Sub-Responsabile disciplinata all'art. 5.2 del presente Accordo.
7.4 L'osservanza dei principi fondamentali in materia di privacy in relazione alle informazioni di cui si è venuti a conoscenza presso la scrivente, si ritiene indispensabile anche successivamente all'eventuale cessazione del rapporto professionale.

Luogo e data ……..

Il Cliente

_____
Titolare del trattamento

Il Fornitore

_____
Responsabile del trattamento

ALLEGATO

SUB RESPONSABILI DEL TRATTAMENTO

Il Responsabile del trattamento in epigrafe si avvale dei seguenti Sub-Responsabili per la corretta e puntuale erogazione del servizio:

- **JDS – JD-Net**

Informazioni di contatto - privacy@jd-net.it

Attività di trattamento

- produzione, personalizzazione e spedizione delle chip card
- stampa dei buoni pasto cartacei, personalizzazione e relativa spedizione degli stessi
- emissione delle codline buono pasto, buono acquisto e buono sociale
- bruciatura delle codline

Tipologia di dati trattati

- Dati dei beneficiari nome, cognome, numero di matricola, organizzazione aziendale di appartenenza
- Dati di dettaglio spesa: nome, cognome, ammontare della transazione ed esercizio commerciale nella quale la transazione è avvenuta

- **Mosaikoweb**

Informazioni di contatto - privacy@mosaikoweb.com

Attività di trattamento

- portale azienda
- portale beneficiario/app mobile
- portale esercente/app mobile

Tipologia di dati trattati

- Dati dei beneficiari: nome, cognome, matricola e, occasionalmente, codice fiscale del beneficiario; indirizzo mail personale inserito facoltativamente da parte di quest'ultimo e finalizzato alla regolare gestione del recupero della sua password
- Dati di dettaglio spesa: ammontare della transazione e data in cui questa viene effettuata, numero di buoni complessivamente utilizzati ed esercizio commerciale nel quale la transazione è avvenuta

- **Solinf**

Informazioni di contatto - privacy@solinf.eu

Attività di trattamento

- anagrafiche/contratti aziende clienti e potenziali
- anagrafiche/contratti esercenti

Tipologia di dati trattati

- Dati di dettaglio spesa: valore complessivo dei buoni emessi e dei buoni ricaricati
- Dati dei beneficiari: accesso solo potenziale dei dati anagrafici a mezzo CRM con possibile controllo incrociato degli esercizi commerciali nei quali sono avvenute le transazioni.