

ACCORDO DI NOMINA A SUB RESPONSABILE DEL TRATTAMENTO DEI DATI
Ai sensi dell'art. 28 del Reg. UE 2016/79

Il presente Accordo di nomina a sub responsabile del trattamento dati (di seguito denominato “**Accordo**”) è concluso tra:

Milano Ristorazione S.p.A. con sede in Milano, via Quaranta, 41 CF/P.IVA 13226890153 in persona del legale rappresentante pro tempore, [Dott. Bernardo Notarangelo], (di seguito denominata “**Milano Ristorazione**” o il “**Responsabile**”)

[] e
[] con sede legale in [] CF/P.IVA [] telefono [] email [] Pec
[]

in persona del legale rappresentante pro tempore

di seguito denominata (di seguito “ [] ” o il “**Sub Responsabile**”)

Il Responsabile e il Sub Responsabile, di seguito congiuntamente denominati le “**Parti**” e ciascuno una “**Parte**”.

PREMESSO CHE

- In data 20/03/2019 con idoneo contratto di nomina, il Comune di Milano – nella sua qualità di Titolare del trattamento (di seguito, il “**Titolare**”) – ha nominato Milano Ristorazione quale responsabile del trattamento ai sensi dell’articolo 28 del Regolamento UE 2016/679 (di seguito “GDPR”), in virtù del trattamento dati effettuato per conto del Titolare al fine di garantire la gestione del servizio di refezione scolastica per le scuole pubbliche dell’infanzia (comunali e statali), le scuole primarie, le scuole secondarie di primo grado e nidi d’infanzia nel territorio comunale e la gestione del servizio di refezione nei Centri Estivi e le Case Vacanza extraurbane (di seguito il “**Servizio**”);
- Per l’esecuzione del Servizio Milano Ristorazione si avvale di fornitori. In particolare, in data [] Milano Ristorazione ha sottoscritto con la società [] un contratto avente ad oggetto il servizio di “[Supporto all’iscrizione per il servizio di refezione scolastica](#)” (di seguito, il “**Contratto**”);
- L’adempimento delle attività oggetto del Contratto da parte della società [] comporta il trattamento dei dati personali (così come definiti dall’art. 4 punto 1 del GDPR, di seguito “**dati personali**”) di cui Milano Ristorazione è Responsabile per conto del Titolare;
- Ad esito di autorizzazione scritta del Titolare del [], circa l’idoneità della società [] a trattare dati per conto del Titolare stesso, con la sottoscrizione del presente Accordo, Milano Ristorazione intende nominare la società [], Sub Responsabile dati nell’esecuzione del Contratto.

Ciò premesso le Parti convengono e stipulano quanto segue.

Le premesse e gli allegati costituiscono parte integrante e sostanziale dell’Accordo.

Con il presente Accordo Milano Ristorazione S.p.A.

NOMINA

la società | quale **SUB RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI** per l'esecuzione di specifiche attività di trattamento per conto del Titolare in virtù dell'esecuzione del Contratto.

1. Oggetto dell'accordo

Il presente Accordo disciplina il trattamento dei dati personali da parte del Sub Responsabile per conto del Titolare sulla base delle istruzioni del Responsabile, nonché gli obblighi e i diritti delle Parti. Il Sub Responsabile fornisce i servizi al Responsabile in relazione al Contratto citato in premessa.

2. Requisiti di professionalità

Secondo l'art. 28 del GDPR, quando un trattamento viene effettuato per conto del Titolare quest'ultimo e il Responsabile ricorrono, rispettivamente, a Responsabili o Sub Responsabili del trattamento che forniscano piena garanzie del rispetto delle vigenti normative in materia e che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate. Le incombenze oggetto del presente Accordo sono affidate al Sub Responsabile sulla base delle dichiarazioni da esso fornite al Responsabile in merito alle caratteristiche di esperienza, capacità e affidabilità previste dalla normativa applicabile.

Per **normativa applicabile** si intende l'insieme delle norme rilevanti in materia di protezione dei dati personali, incluso il GDPR e inoltre, in ogni tempo, ogni linea guida, norma di legge, compresa la normativa nazionale di adeguamento al citato GDPR, nonché i provvedimenti del Garante per la protezione dei dati, codice o provvedimento rilasciato o emesso dagli organi competenti o da altre autorità di controllo.

Il Sub Responsabile designato, con la sottoscrizione del presente Accordo si dichiara disponibile e competente e dotato di una propria organizzazione, per dare attuazione a quanto previsto, nonché in possesso dei requisiti di esperienza e capacità tali da fornire garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ed in particolare in termini di conoscenze specialistiche, affidabilità e risorse, per attuare misure tecniche e organizzative che soddisfino i requisiti del GDPR, compresa la sicurezza del trattamento per garantire la riservatezza e la protezione dei diritti degli interessati.

3. Ambito e limiti del trattamento dei dati

Il Sub Responsabile è autorizzato ad effettuare esclusivamente le operazioni di trattamento necessarie per lo svolgimento delle attività concordate e descritte in premessa che sinteticamente si riportano di seguito con l'indicazione delle categorie di dati:

Attività	Categorie di dati
----------	-------------------

- Servizio di assistenza compilazione domanda di iscrizione al servizio di refezione	Principali dati personali
--	---------------------------

Si rinvia all'**allegato 1** del presente atto il dettaglio delle tipologie di dati trattati e alle categorie di interessati per l'esecuzione del servizio

A tal proposito, il Sub Responsabile riconosce che le finalità del trattamento sono esclusivamente quelle individuate nel Contratto. Il Sub Responsabile ha accesso ai dati di cui Milano Ristorazione è Responsabile, esclusivamente per le attività necessarie e connesse allo svolgimento delle attività previste nel Contratto, nei limiti di legge e di eventuali prescrizioni da parte del Titolare sulla base delle istruzioni del Responsabile medesimo.

4. Dichiarazioni e compiti del Responsabile

Il Responsabile sulla base delle istruzioni ricevute dal Titolare, affida al Sub Responsabile le operazioni di trattamento dei dati necessarie per dare esecuzione al Contratto e gli comunica qualsiasi variazione che dovesse rendersi necessaria nelle operazioni di trattamento.

Il Responsabile, sulla base delle istruzioni del Titolare, precisa che i dati personali messi a disposizione del Sub Responsabile, ivi compresi i dati e le categorie particolari di dati, sono esclusivamente quelli connessi e strumentali all'esecuzione del compito svolto in qualità di Sub Responsabile e che la raccolta dei dati personali da parte del Sub Responsabile deve avvenire nel rispetto delle disposizioni di legge ed in particolare del GDPR; i dati dovranno essere esatti ed aggiornati, pertinenti, completi e non eccedenti le finalità per le quali sono trattati.

Nell'ambito delle attività oggetto del presente Accordo, il Responsabile esercita funzioni di controllo utilizzando gli strumenti di verifica più opportuni rispetto all'attività: es. check list e verifiche periodiche tramite propri addetti presso la sede del Sub Responsabile. A tal fine il Responsabile informa il Sub Responsabile con un preavviso minimo di tre giorni lavorativi, fatta comunque salva la possibilità di effettuare controlli a campione senza preavviso.

5. Obblighi e dichiarazioni del Sub Responsabile

Il Sub Responsabile nell'espletamento della propria funzione, in forza del presente Accordo, è tenuto a collaborare con il Responsabile, fornendo le informazioni e i documenti richiesti, ed eventuali relazioni sui livelli di sicurezza dei sistemi e dei dati, sullo stato di attuazione della normativa, nonché sul modello organizzativo adottato e su certificazioni di sicurezza acquisite. Il Sub Responsabile dichiara - con la sottoscrizione del presente Accordo - la conformità alle norme in materia e alle misure richieste.

Il Sub Responsabile si impegna a rispettare in ogni fase del trattamento le disposizioni previste dal GDPR e dalle norme in materia di protezione dei dati applicabili, in particolare le finalità, le modalità, le misure di sicurezza e gli ambiti di comunicazione dei trattamenti.

Tenendo conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Sub Responsabile al fine di proteggere

i dati personali, siano essi trattati con strumenti elettronici che cartacei, mette in atto misure tecniche e organizzative per garantire un livello di sicurezza adeguato ai rischi, inclusi quelli di:

- distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati;
- trattamento dei dati non consentito o non conforme alle finalità delle operazioni di trattamento definite dal Titolare.

Il Sub Responsabile si impegna altresì a trattare i dati personali del Responsabile solo per suo conto e limitatamente alle attività di trattamento strettamente necessarie per l'esecuzione del Contratto, in conformità con le istruzioni impartite dal Responsabile. Qualora il Sub Responsabile non sia in grado di garantire la conformità per qualsiasi motivo, informa tempestivamente il Responsabile che ha il diritto di sospendere il trattamento dei dati e/o risolvere il Contratto.

Il Sub Responsabile in relazione a quanto previsto dal precedente punto 4 – ultimo paragrafo - riconosce al Responsabile il diritto di accedere ai locali ove hanno svolgimento le operazioni di trattamento o dove sono custoditi dati o documenti relativi al presente accordo. Per contro il Responsabile si impegna ad utilizzare le informazioni raccolte durante le operazioni di verifica solo per tali finalità.

Fermo restando quanto previsto ai precedenti punti, il Sub Responsabile dichiara di aver ricevuto, esaminato, condiviso e compreso le istruzioni impartite dal Responsabile con i documenti contrattuali, nonché quelle di seguito indicate alle quali dovrà attenersi nell'esecuzione dell'incarico.

6. Ulteriori obblighi e istruzioni per il Sub Responsabile

Il Sub Responsabile nell'esercizio delle proprie funzioni è tenuto, anche con riguardo alle persone autorizzate al trattamento che collaborano con la sua organizzazione, ad osservare gli obblighi inerenti le misure di sicurezza previste dalle norme in materia e a fornire assistenza al Responsabile sulla base delle istruzioni del Responsabile per garantirne il rispetto.

Il Sub Responsabile nell'ambito dei trattamenti effettuati presso le proprie sedi o presso i locali nella sua piena ed esclusiva disponibilità e/o con propri strumenti informatici, implementa le misure di sicurezza definite puntualmente **nell'Allegato 1** al fine di garantire:

- 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.

Nell'ambito dei trattamenti effettuati presso le proprie sedi e/o con propri strumenti, Il Sub Responsabile rende disponibile la documentazione relativa alla propria policy per la gestione degli eventi di "Data Breach", predispone e aggiorna un registro che dettagli, in caso di eventuali "Data Breach", la natura delle violazioni, gli interessati coinvolti, le possibili conseguenze.

Il Sub responsabile è inoltre tenuto ad informare il Responsabile, senza ingiustificato ritardo e comunque **entro 24 ore** da quando ne viene a conoscenza, in ordine a qualsiasi violazione di dati personali, anche se intervenuta presso i propri sub-Responsabili qualora nominati.

Il Sub Responsabile dovrà assicurare il pieno supporto al Responsabile e all'Autorità di controllo per ottemperare alle obbligazioni previste dalle norme vigenti (ad esempio notifica delle violazioni di dati

personali all'Autorità di controllo; laddove applicabile, comunicare la violazione di dati personali agli interessati).

Il Sub Responsabile è tenuto inoltre ad adottare, in accordo con il Responsabile, ulteriori misure finalizzate a circoscrivere gli effetti negativi dell'evento e ripristinare la situazione precedente.

Il Sub Responsabile inoltre:

1. adotta le misure di cui all'art. 25 del GDPR rubricato "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (cd." Privacy by Default" e "by Design") ovvero misure tecniche ed organizzative adeguate garantendo che, per impostazione predefinita, vengano raccolti e trattati solo i dati strettamente necessari al raggiungimento delle finalità stabilite e limitando l'accesso ad un numero definito di persone preventivamente autorizzate;
2. applica, se del caso, misure come l'anonimizzazione, la cifratura la pseudonimizzazione intesa come modalità di "riduzione della correlabilità di un insieme di dati all'identità originaria di una persona interessata";
3. garantisce il rispetto degli obblighi di cui agli articoli 32-36 del GDPR tenendo conto della natura del trattamento e delle informazioni a propria disposizione;
4. tiene un registro ai sensi dell'art. 30 del GDPR di tutte le categorie di attività relative al trattamento svolte per conto del Responsabile;
5. non comunica a terzi né diffonde i dati di cui viene a conoscenza, salvo che tali operazioni siano autorizzate dal Responsabile o previste da norme di legge o di regolamento nazionali o dell'Unione Europea;
6. concorda con il Responsabile le modalità con cui fornire agli interessati l'informativa ai sensi dell'art. 13 e 14 del GDPR;
7. non effettua di propria iniziativa alcuna operazione di trattamento diversa da quelle previste se non autorizzata Responsabile;
8. non trasferisce i dati trattati per conto del Responsabile al di fuori dello Spazio Economico Europeo senza autorizzazione scritta da parte del Responsabile, al quale vanno fornite tutte le informazioni riguardanti il rispetto delle condizioni di cui al Capo V del GDPR;
9. adotta adeguati sistemi per assicurare i diritti riconosciuti agli interessati dal GDPR;
10. informa tempestivamente il Responsabile, entro 2 giorni, in merito ad eventuali richieste inviate da parte degli interessati;
11. garantisce al Responsabile - se da questo richiesto - la tutela dei diritti innanzi al Garante per la protezione dei dati personali in caso di eventuali contenziosi rispetto al servizio offerto;
12. collabora con il Responsabile per il rispetto di eventuali prescrizioni emesse dall'Autorità Garante o dall'Autorità Giudiziaria in relazione al trattamento dei dati;
13. informa tempestivamente il Responsabile di qualsiasi richiesta legalmente vincolante per la divulgazione dei dati personali da parte di un'Autorità Giudiziaria salvo laddove diversamente vietato per rilevanti motivi di interesse pubblico;
14. informa immediatamente il Responsabile a mezzo e-mail: dpo@milanoristorazione.it, in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità Garante;
15. realizza tutto quanto sia utile e/o necessario per garantire gli adempimenti di tutti gli obblighi previsti dal GDPR.

Inoltre, qualora i trattamenti dovessero presentare un rischio elevato per la dignità e la libertà delle persone, il Sub Responsabile collabora con il Responsabile nelle attività di supporto al Titolare nella valutazione di

impatto (*data protection impact assessment* – DPIA) e nell’eventuale consultazione preliminare all’Autorità di Controllo, laddove applicabile.

Il Responsabile, in funzione di eventuali evoluzioni tecnologiche e/o normative, può richiedere ulteriori misure di sicurezza rispetto a quelle adottate dal Sub Responsabile. In tal caso il Responsabile fornirà al Sub Responsabile adeguate istruzioni con sufficiente preavviso per permettere allo stesso di attuarle.

Il Sub Responsabile al termine delle attività connesse alla propria funzione e delle prestazioni contrattualmente previste:

- consegna al Responsabile o distrugge su sua indicazione tutte le informazioni raccolte con qualsiasi modalità, cartacea e/o elettronica;
- consegna i supporti rimovibili eventualmente utilizzati in cui sono memorizzati i dati;
- distrugge tutte le informazioni registrate su supporto fisso, documentando per iscritto l’adempimento di tale operazione. Il Responsabile si riserva il diritto di effettuare controlli e verifiche al fine di accertare la veridicità delle dichiarazioni rese.

7. Persone autorizzate al trattamento

Il Sub Responsabile nell’ambito della propria organizzazione individua e autorizza le persone a trattare i dati e contestualmente fornisce loro, per iscritto, le istruzioni in merito ai trattamenti, con particolare riferimento alle modalità e alle operazioni che possono essere svolte sui dati in attuazione a quanto previsto dalle norme in materia e dal presente accordo. I nominativi delle persone autorizzate al trattamento saranno forniti al Responsabile se richiesto.

Il Sub Responsabile mette in atto le relative misure per consentire alle persone autorizzate di accedere ai soli dati la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati e avrà cura di fornire a tali persone che, per mansioni e funzioni, avranno accesso ai dati personali, categorie particolari di dati e dati personali relativi a condanne penali e reati, tutte le indicazioni e le specifiche regole comportamentali affinché i trattamenti effettuati siano conformi ai principi di pertinenza, non eccedenza e indispensabilità.

Al riguardo, il Sub Responsabile verifica che le persone autorizzate:

- a) applichino tutte le disposizioni in materia di sicurezza relativa alla custodia delle parole chiavi (trattamenti elettronici);
- b) conservino in luogo sicuro i supporti non informatici contenenti atti o documenti con categorie particolari di dati o la loro riproduzione, adottando contenitori con serratura (trattamenti cartacei categorie particolari di dati e dati personali relativi a condanne penali e reati).

Il Sub Responsabile vincola le predette persone alla riservatezza e al rispetto di tale obbligo anche per il periodo successivo all’estinzione del rapporto di collaborazione intrattenuto con il Sub Responsabile, in relazione alle operazioni di trattamento da esse eseguite.

Il Sub Responsabile sottopone le persone incaricate ad interventi formativi e di aggiornamento periodico o approfondimento per renderle edotte dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure adottate.

8. Ulteriori Sub-Responsabili

Il Responsabile non autorizza la nomina di Sub-Sub Responsabili

9. Amministratori di sistema

Laddove il trattamento sia effettuato con strumenti elettronici, il Sub Responsabile si obbliga a rispettare il provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e successive modifiche ed integrazioni recante disciplina in materia di amministratori di sistema, in particolare, a conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte alle funzioni di amministratore di sistema e a fornirli prontamente al Responsabile su richiesta del medesimo. Il Sub Responsabile si obbliga altresì a verificare, con cadenza almeno annuale e comunque ogni qualvolta lo richieda il Responsabile, l'operato degli amministratori di sistema al fine di controllare la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti previsti dalle norme vigenti.

10. Responsabilità

Il Sub Responsabile tiene indenne e manlevato il Responsabile da ogni perdita, costo, spesa, multa e/o sanzione, danno e da ogni responsabilità di qualsiasi natura (sia essa prevedibile, contingente o meno) derivante da o in connessione con una qualsiasi violazione da parte del Sub Responsabile degli obblighi della normativa applicabile o delle disposizioni contenute nel Contratto. In particolare, il Sub Responsabile tiene indenne il Responsabile, ai sensi dell'art. 2043 e 2049 c.c., da qualsiasi danno cagionato al Titolare o a terzi derivante da atti, fatti o omissioni posti in essere in violazione delle disposizioni del GDPR e delle altre disposizioni in materia di protezione dei dati personali, anche da parte delle persone autorizzate e dagli amministratori di sistema, se presenti. In particolare il Sub Responsabile risponde per i danni derivanti dal trattamento qualora abbia agito in modo difforme o contrario alle legittime istruzioni ricevute dal Responsabile in violazione dei termini del presente Accordo.

11. Comunicazioni tra le parti

Il Sub Responsabile informerà il Responsabile di ogni provvedimento dell'Autorità Garante di Controllo connesso al presente Accordo. In particolare il Sub Responsabile avvisa immediatamente il Responsabile in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità di Controllo.

Le parti stabiliscono le seguenti persone di contatto per tutte le comunicazioni relative all'esecuzione dell'Accordo:

Per il Responsabile del Trattamento: Nome Delegato Privacy MiRi; [Sig. Flavio Cuomo -3457851853-0288464665 flavio.cuomo@milanoristorazione.it];

Per il Sub Responsabile del Trattamento: [] [Qualsiasi modifica relativa le sopramenzionate persone o la responsabilità delle persone di contatto deve essere immediatamente notificata all'altra parte.

12. Richieste degli interessati

Su espressa richiesta del Responsabile, nella misura in cui ciò sia possibile, il Sub Responsabile fornisce riscontro alle eventuali istanze degli interessati nei termini previsti dal GDPR. Il Sub Responsabile prima di provvedere sottopone al Responsabile la richiesta che intende fornire in merito al trattamento dei dati.

13. Corrispettivo e spese

Nessun corrispettivo è dovuto dal Responsabile al Sub Responsabile per l'espletamento della funzione.

14. Decorrenza Cessazione e Revoca

Il presente Accordo decorre dalla data di sottoscrizione e cesserà automaticamente con la conclusione del Contratto. Il Titolare può revocare l'incarico in caso di svolgimento delle funzioni non conformi alle istruzioni fornite, nonché per la sopravvenuta perdita dei requisiti di cui all'art. 28 del GDPR

Per quanto non espressamente previsto nel presente Accordo, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

Letto, approvato e sottoscritto.

Milano, data []

Il Responsabile del Trattamento
Milano Ristorazione S.p.A.
Dott. Bernardo Notarangelo
|

Il Sub Responsabile del Trattamento
|

Allegato 1 Misure di sicurezza

Il presente Allegato costituisce parte integrante e sostanziale dell'Accordo.

Le attività di trattamento sono effettuate al fine di garantire la gestione dei servizi affidati (cfr. punto 3 del presente Accordo) di seguito riportate:

Attività
Servizio di assistenza compilazione domanda di iscrizione al servizio di refezione

I dati personali trattati riguardano le seguenti categorie di Interessati

Categorie di Interessati:
- Genitori/tutori di minori e scolari
- Utenti refezione studenti c/o scuole dell'infanzia, primarie e secondarie I grado
-

I dati personali trattati per conto del Responsabile riguardano le seguenti categorie di dati personali relativi agli Interessati

Tipologia di dati personali:
- Dati anagrafici e di contatto
- Dati finanziari
- Composizione del nucleo familiare
- Informazioni sulla scuola (istituto, classe) frequentata dal minore
- Stato di bambino in affido presso nuclei familiari, Comunità e/o Associazioni

In relazione al contesto e ai rischi analizzati il Sub Responsabile, effettuando questi trattamenti nell'ambito delle attività contrattualmente previste garantisce di applicare le seguenti misure di sicurezza:

Sicurezza applicativa:

- PROFILAZIONE DEGLI ACCESSI IN RELAZIONE AL RUOLO
- UTILIZZO CREDENZIALI UNINOMINALI
- AUTENTICAZIONE DELLE UTENZE USERNAME/PASSWORD
- UTILIZZO DI PASSWORD SICURE
- PROTEZIONE DEI DATI TRATTATI
-

Sicurezza infrastrutturale:

- PROFILAZIONE DEGLI ACCESSI IN RELAZIONE AL RUOLO
- UTILIZZO CREDENZIALI UNINOMINALI
- AUTENTICAZIONE DELLE UTENZE USERNAME/PASSWORD
- UTILIZZO PASSWORD SICURE
- PROTEZIONE DA MALWARE SIGNATURE BASED
- ISOLAMENTO DELLA RETE DA ALTRI SISTEMI
- PROTEZIONE DEL TRAFFICO
- PROGRAMMA DI PROTEZIONE DISCHI RIMOVIBILI
- FORMAZIONE DEL PERSONALE SULLA PROTEZIONE DEI DATI

Sicurezza fisica:

- LIMITAZIONE DI ACCESSO AI LOCALI DESTINATI AL TRATTAMENTO
- PROFILAZIONE DEGLI ACCESSI IN RELAZIONE AL RUOLO
- PRESENZA DI SISTEMI ANTI EFFRAZIONE