BOZZA DATA PROCESSING AGREEMENT (DPA)

Tra

La società Milano Ristorazione S.p.A. con sede in Via Quaranta n. 41 Milano (MI) (di seguito anche la "**Società**" o il "**Titolare**"), in persona del legale rappresentante *pro tempore*,

e

La società _____ con sede in _____ (di seguito anche il "**Fornitore**" o il "**Responsabile**"), in persona del proprio legale rappresentate *pro tempore*,

Premesso che

A. La Società ha stipulato con il Fornitore un contratto sottoscritto in data _____ (di seguito l'"**Accordo**") concernente _____ (di seguito l'"**Attività**").

B. Nell'esecuzione dell'Attività, il Fornitore può trovarsi a trattare dati personali della Società come di seguito definiti nell'Articolo 1.

C. La Società e il Fornitore hanno convenuto di stipulare il presente contratto (di seguito il "**Contratto**") allo scopo di disciplinare le modalità di trattamento dei dati personali della Società da parte del Fornitore.

1. <u>Definizioni</u>. I seguenti termini utilizzati nel presente Contratto e negli Allegati alla stessa avranno i seguenti significati:

a. "**Normativa applicabile**": l'insieme delle norme rilevanti in materia di privacy alle quali il Titolare è soggetto incluso il Regolamento (UE) n. 2016/679, il D.lgs. n. 196/2003 come novellato dal D.lgs. n. 101/2018 (di seguito, unitamente "**GDPR**"), nonché in ogni tempo, ogni linea guida, norma di legge, codice o provvedimento rilasciato o emesso dagli organi competenti o da altre autorità di controllo, ivi inclusi i Provvedimenti del Garante per la protezione dei dati personali che resteranno in vigore.

b. "**Titolare del trattamento**", "**responsabile del trattamento**", "**interessato**", "**dati personali**" e "**trattamento**" hanno il significato dato dalla Normativa applicabile.

c. **'Misure tecniche e organizzative di sicurezza'** sono le misure intese a proteggere i dati personali dalla distruzione accidentale o illegale o dalla perdita, alterazione, divulgazione o accesso non autorizzato, in particolare quando il trattamento comporta la trasmissione di dati su una rete, come previste dalla Normativa applicabile all'art.32 GDPR e tutte le ulteriori misure tecniche ed organizzative necessarie a garantire un livello di sicurezza adeguato al rischio, tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento posto in essere, come del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

d. **"Data breach"**: Si intende l'ipotesi in cui si verifica una violazione dei dati personali secondo l'art. 33 GDPR.

e. **"Garante"**: si intende l'autorità competente responsabile per la protezione dei dati.

f. **"Sub-responsabile/i"** Si intende qualsiasi responsabile del trattamento incaricato dal (i) Responsabile o (ii) da qualsiasi altro "sub-responsabile" di trattare dati personali per conto del Responsabile, sempre in conformità alle istruzioni del Titolare.

2. Oggetto del Contratto

Le premesse e gli Allegati costituiscono parte integrante e sostanziale del presente Contratto.

Le incombenze e le responsabilità oggetto del presente Contratto vengono affidate al Responsabile sulla base delle dichiarazioni dallo stesso fornite alla Società (e della successiva verifica da parte della Società, per quanto ragionevolmente possibile, della loro rispondenza al vero) circa le caratteristiche di esperienza, capacità e affidabilità che vengono richieste dalla legge (artt. 28 GDPR) per chi esercita la funzione di Responsabile del trattamento. Con la sottoscrizione del presente Contratto, il Responsabile si dichiara disponibile e competente per la piena attuazione di quanto ivi disposto, conferma la diretta ed approfondita conoscenza degli obblighi che assume in relazione al dettato del GDPR, conferma, altresì, di disporre di una propria organizzazione che dichiara idonea a consentire il trattamento dei dati nel pieno rispetto delle prescrizioni legislative, ivi compreso il profilo della sicurezza, e si impegna a procedere al trattamento dei dati personali attenendosi alle istruzioni impartite nel pieno rispetto di quanto imposto dall'art. 28, lettera a) del GDPR.

Nei limiti delle proprie competenze e attribuzioni, il Responsabile dovrà garantire l'osservanza degli obblighi di legge, sempre conformemente alle direttive e sotto la vigilanza del Titolare.

Onde consentire al Responsabile di espletare i compiti e le attribuzioni meglio specificati in seguito, con il presente Contratto vengono fornite le specifiche istruzioni per l'assolvimento del compito assegnato.

3. Misure tecniche ed organizzative - Audit e diritti di verifica del Titolare del Trattamento

Il Responsabile del Trattamento si obbliga ad adottare ed implementare le Misure tecniche ed organizzative di sicurezza, oltre a quanto previsto dall'art.5, numero 8, con l'obbligo di documentarle se richiesto dal Titolare del Trattamento.

Il Titolare si riserva la facoltà di effettuare, nei modi ritenuti più opportuni, anche tramite l'invio presso i locali del Responsabile di propri funzionari a ciò delegati, o tramite l'invio di apposite check list, verifiche tese a vigilare sulla puntuale osservanza delle disposizioni di legge e delle presenti istruzioni.

In alternativa a quanto sopra precisato, il Responsabile può fornire al Titolare copie delle relative certificazioni esterne (es. ISO 27001: 2013, SSAE 16 ecc.), audit report e/o altra documentazione sufficiente per il Titolare a verificare la conformità del Responsabile alle Misure tecniche e organizzative di sicurezza del presente Contratto.

Il Responsabile deve adottare misure tecniche ed organizzative adeguate per salvaguardare la sicurezza di qualsiasi rete di comunicazione elettronica o dei servizi forniti al Titolare o utilizzati per trasferire o trasmettere i dati personali (incluse, ad esempio, le misure intese a garantire la segretezza delle comunicazioni così da prevenire l'intercettazione di comunicazioni o l'accesso non autorizzato a qualsiasi computer o sistema), garantendo, in tal modo, la sicurezza delle comunicazioni

4. Correzioni, cancellazione o blocco di dati

Il Responsabile può solamente correggere, cancellare o bloccare il trattamento dei dati personali a beneficio del Titolare del Trattamento e quando ha avuto istruzioni dal Titolare del Trattamento in tal senso. Se l'interessato fa richiesta direttamente al Responsabile del Trattamento per la correzione o la cancellazione dei propri dati personali, il Responsabile deve indirizzare la predetta richiesta al Titolare del Trattamento senza ritardo alcuno.

Alla scadenza del Contratto il Responsabile si obbliga a restituire al Titolare del trattamento tutti i dati in suo possesso.

5. Istruzioni generali del Responsabile del Trattamento

Il Responsabile, sebbene non in via esaustiva, avrà i compiti e le attribuzioni di seguito elencate, oltre agli ulteriori obblighi previsti al successivo articolo 6, e dunque dovrà:

1. effettuare la ricognizione delle banche dati, degli archivi (cartacei e non) relativi ai trattamenti effettuati in esecuzione dell'Attività;
2. tenere un registro, come previsto dall'art. 30 del GDPR, in formato elettronico, di tutte le categorie di attività relative al trattamento svolte per conto della Società, contenente:
   - il nome e i dati di contatto del Responsabile e del Titolare e, laddove applicabile, del Responsabile della protezione dei dati;
   - le categorie dei trattamenti effettuati per conto del Titolare;
   - ove possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative adottate;
3. organizzare le strutture, gli uffici e le competenze necessarie e idonee a garantire il corretto espletamento dell'Attività;
4. astenersi dal contattare i nominativi trattati attraverso l'Attività così come dal trattarli per finalità proprie;
5. non diffondere o comunicare a terzi i dati trattati attraverso l'Attività;
6. garantire l'affidabilità di qualsiasi dipendente che accede ai dati personali del Titolare ed assicurare, inoltre, che gli stessi abbiano ricevuto adeguate istruzioni e formazione con riferimento alla protezione e gestione dei dati personali, e che siano vincolati al rispetto di obblighi di riservatezza non meno onerosi di quelli previsti nel presente Contratto;
7. tenere i dati personali trattati attraverso l'Attività e di cui è titolare la Società separati rispetto a quelli trattati per conto di altre terze parti, sulla base di un criterio di sicurezza di tipo logico;
8. adottare le Misure tecniche ed organizzative di sicurezza, come previste al precedente articolo 3, nonché le ulteriori misure di sicurezza previste dall'Allegato 2;
9. procedere alla nomina del proprio/i amministratore/i di sistema, in adempimento di quanto previsto dal provvedimento del Garante del 27.11.08, pubblicato in G.U. n. 300 del 24.12.2008, ove ne ricorrano i presupposti, comunicandolo prontamente al Titolare, curando, altresì, l'applicazione di tutte le ulteriori prescrizioni contenute nel suddetto provvedimento;

10. assistere tempestivamente il Titolare con misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo del Titolare di procedere ad un DPIA (Valutazione di impatto sulla protezione dei dati) ex art. 35 e ss del GDPR, con obbligo di notifica quando venga a conoscenza di un trattamento di dati che possa comportare un rischio elevato;

11. assistere il Titolare nel garantire il rispetto degli obblighi di cui agli artt. 32-36 GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile e garantire l'esercizio del diritto alla portabilità dei dati personali trattati attraverso l'Attività, ai sensi dell'art. 20 del GDPR, assicurando che gli stessi possano essere trasmessi in un formato strutturato, di uso comune e leggibile da qualsiasi dispositivo automatico;

12. notificare alla Società, senza ingiustificato ritardo e comunque non oltre le 24 ore da quando ne abbia avuto conoscenza, ai sensi dell'art.33 del GDPR, nel caso in cui si verifichi un *Data breach* anche presso i propri Sub-responsabili; la notifica deve contenere tutti i requisiti previsti dall'art. 33, 3° comma del GDPR (la natura delle violazioni, gli interessati coinvolti, le possibili conseguenze e le nuove misure di sicurezza implementate). Dovrà, inoltre, adottare, di concerto con la Società, nuove misure di sicurezza atte a circoscrivere gli effetti negativi dell'evento e a ripristinare la situazione precedente;

13. predisporre e aggiornare un registro che dettagli, in caso di eventuali *Data breach*, la natura delle violazioni, gli interessati coinvolti, le possibili conseguenze e le nuove misure di sicurezza implementate;

14. astenersi dal trasferire i dati personali trattati per conto della Società al di fuori dello Spazio Economico Europeo senza il previo consenso scritto della Società;

15. avvertire prontamente la Società, entro tre (3) giorni lavorativi, in merito alle eventuali richieste degli interessati che dovessero pervenire al Responsabile inviando copia delle istanze ricevute all'indirizzo e-mail: privacy@milanoristorazione.it e collaborare al fine di garantire il pieno esercizio da parte degli interessati di tutti i diritti previsti dalla Normativa applicabile;

16. adottare adeguati processi e ogni altra misura tecnica idonea ad attuare le istruzioni fornite dal Titolare, incluse:

    i. le procedure idonee a garantire il rispetto dei diritti e delle richieste formulate al Titolare dagli interessati relativamente ai loro dati personali, come indicato al precedente punto 15;

    ii. l'adozione di adeguate interfacce o sistemi di supporto che consentano di garantire e fornire informazioni agli interessati così come previsto dalla Normativa applicabile;

    iii. procedure atte a garantire l'aggiornamento, la modifica e la correzione, su richiesta del Titolare, dei dati personali di ogni interessato;

    iv. procedure atte a garantire la cancellazione o il blocco dell'accesso ai dati personali a richiesta del Titolare;

    v. misure che consentano di contrassegnare i dati personali o gli account, per consentire al Titolare di poter applicare particolari regole ai dati personali dei singoli interessati; il Responsabile, dietro richiesta scritta del Titolare, collaborerà con questo per garantire il diritto degli interessati alla portabilità dei dati e di limitazione di trattamento;

17. avvisare immediatamente, e comunque entro tre (3) giorni lavorativi, il Titolare del trattamento, di qualsiasi richiesta o comunicazione da parte dell'Autorità Garante o di quella Giudiziaria eventualmente ricevuta inviando copia delle istanze all'indirizzo e-mail: privacy@milanoristorazione.it per concordare congiuntamente il riscontro;

18. predisporre idonee procedure interne finalizzate alla verifica periodica della corretta applicazione e della congruità degli adempimenti posti in essere ai sensi della Normativa applicabile, attuate in accordo con il Titolare anche in applicazione delle Misure tecniche e organizzative di sicurezza;

19. mantenere un costante aggiornamento sulle prescrizioni di legge in materia di trattamento dei dati personali, nonché sull'evoluzione tecnologica di strumenti e dispositivi di sicurezza, modalità di utilizzo e relativi criteri organizzativi adottabili;

20. garantire la stretta osservanza dell'incarico ricevuto, escludendo qualsiasi trattamento o utilizzo dei dati personali non coerente con gli specifici trattamenti svolti in adempimento dell'incarico medesimo;

21. rispettare la Normativa applicabile e adempiere gli obblighi previsti dal presente Contratto in modo da evitare che il Titolare incorra nella violazione di un qualunque obbligo previsto dalla Normativa applicabile;

22. ottemperare tempestivamente alle richieste del Titolare;

23. inviare tutte le comunicazioni al Titolare previste nel presente atto all'indirizzo soprariportato o a quello diverso che verrà eventualmente comunicato;

24. prima di iniziare il trattamento e, ove occorra, in qualsiasi altro momento, informare il Titolare se, a suo parere:

    a) una qualsiasi istruzione fornita dal Titolare si pone in violazione di legge;

    b) il Responsabile è soggetto al rispetto di previsioni di legge, che potrebbero rendere per lo stesso, in tutto o in parte, impossibile o illegale agire conformemente alle istruzioni impartite da Titolare o nel rispetto di quanto previsto dalla Normativa applicabile.

6. Ulteriori obblighi del Responsabile

Il Responsabile del trattamento, compatibilmente con quanto previsto dal presente Contratto ed in conformità con le previsioni dell'art.28 del GDPR, sarà altresì soggetto al seguente obbligo di riservatezza; a tal fine ogni persona che abbia accesso ai dati personali appartenenti al Titolare del trattamento, sotto i termini del presente Contratto, si impegna a mantenere la riservatezza e deve essere informata di qualsiasi speciale necessità derivante dal predetto Contratto e della limitazione d'uso a specifici scopi. Se i dati personali relativi alla Società vengono conservati, trattati o usati come parte del presente Contratto, le persone coinvolte nel trattamento saranno obbligate a mantenere l'obbligo di riservatezza.

7. Sub-responsabili

a. Sub-responsabili autorizzati. I Sub-responsabili autorizzati dal Titolare, a decorrere dalla data effettiva del presente Contratto, sono elencati all'Allegato 3 della stessa.

b. **Designazione di nuovi Sub-responsabili.** Se il Responsabile desidera incaricare nuovi Sub-responsabili, in aggiunta a quelli di cui al punto precedente, deve chiedere la relativa autorizzazione alla Società e rispettare le seguenti condizioni:

(i) condurre e documentare un'appropriata due diligence nei confronti del Sub-responsabile proposto;

(ii) almeno trenta (30) giorni prima che il Responsabile autorizzi qualsiasi nuovo Sub-responsabile ad accedere ai dati personali del Titolare, il Responsabile fornirà al Titolare un report descrittivo per iscritto avente ad oggetto le attività di trattamento dei dati personali da devolvere al Sub-responsabile nonché gli eventuali risultati rilevanti della due diligence effettuata nei confronti dello stesso;

(iii) se il Titolare autorizza la designazione del nuovo Sub-responsabile, il Responsabile implementa in tal senso l'Allegato 3 e ne inoltra la versione aggiornata al Titolare, unitamente al contratto di incarico del Sub-responsabile;

(iv) se il Titolare non autorizza la designazione del nuovo Sub-responsabile, a causa di ragionevoli preoccupazioni per la protezione dei dati, questi comunicherà tale decisione al Responsabile, specificando le ragioni per cui l'autorizzazione non è stata concessa. In questo caso, il Responsabile non deve consentire alcun trattamento dei dati del Titolare da parte del Sub-responsabile finché non vi sia l'autorizzazione del Titolare.

c. **Obblighi verso il Sub-responsabile**. Nel momento in cui il Titolare autorizza l'incarico di uno o più Sub-responsabili, il Responsabile:

(i) limiterà l'accesso del Sub-responsabile ai dati personali a quanto strettamente necessario per soddisfare gli obblighi del Responsabile ai sensi del Contratto; al Sub-responsabile sarà vietato l'accesso ai dati personali per qualsiasi altro scopo;

(ii) imporrà per iscritto ad ogni Sub-responsabile il rispetto di obbligazioni ed istruzioni equipollenti a quelle previste nel presente Contratto nella sua totalità, ivi inclusi gli Allegati 1 e 2, nonché la possibilità di effettuare audit;

(iii) rimarrà pienamente responsabile nei confronti del Titolare per il rispetto degli obblighi derivanti dal presente Contratto per qualsiasi atto o omissione del Sub-responsabile che comporti una violazione degli stessi.

Il Sub-appalto nel significato della presente disposizione, non include servizi ausiliari richiesti dal Responsabile del trattamento da terze parti per assisterli nell'esecuzione dell'appalto. Questi possono essere ad esempio servizi di telecomunicazione, manutenzione e supporto agli utenti (se non è possibile l'accesso ai dati personali da parte del Titolare del trattamento), la pulizia, il controllo o l'eliminazione dei dati multimediali. Tuttavia, il Sub-appalto relativo all'eliminazione di documenti/dati multimediali deve essere comunicato al Titolare del trattamento se l'attività principale del trattamento commissionato comporta l'eliminazione di documenti/ dati multimediali. Per salvaguardare la protezione e la sicurezza dei dati personali del Titolare del trattamento, anche quando i servizi ausiliari sono resi da terze parti, il Responsabile del trattamento comunque stipula accordi contrattuali adeguati e legittimi e intraprende attività di monitoraggio.

8. Responsabilità

Il Responsabile tiene indenne e manlevata il Titolare 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 Responsabile degli obblighi della Normativa applicabile o delle disposizioni contenute nel presente Contratto. In particolare, il Responsabile tiene indenne il Titolare da qualsiasi perdita derivante: (a) da qualsiasi violazione (i) dei termini del presente Contratto o (ii) della Normativa applicabile, anche da parte di ogni Sub-Responsabile di cui si avvale; o (b) dalla subfornitura o all'esternalizzazione di qualsiasi Trattamento affidato a terzi soggetti.

9. Miscellanea

I dati devono essere trattati ed utilizzati esclusivamente nel territorio di uno Stato Membro dell'Unione Europea (EU) o di altro firmatario del presente Contratto nell'Area Economica Europea (AEE).

Il Responsabile non avrà diritto di rimborso delle eventuali spese che lo stesso potrebbe dover sostenere per essersi attenuto alle istruzioni impartite da Titolare per lo svolgimento dell'Attività, e/o di un qualsiasi altro suo obbligo previsto dal Contratto.

10. Durata - Legge e foro competente

Il Contratto decorre dalla data della sua sottoscrizione e rimarrà in vigore sino alla risoluzione o alla scadenza del Contratto o cessazione dei servizi da eseguirsi in relazione all'Attività.

Il Contratto o qualsiasi reclamo, pretesa o rivendicazione da esso derivante da o in relazione ai soggetti del Contratto deve esser governato dalla Legge italiana. Si stabilisce la competenza esclusiva del Tribunale di Milano per qualsiasi controversia derivante dal Contratto.

Le parti stabiliscono le seguenti persone di contatto per l'esecuzione del Contratto:

Per il Titolare del Trattamento: [____*____];

Per il Responsabile del Trattamento: [____*____]

Qualsiasi modifica relativa le sopramenzionate persone o la responsabilità delle persone di contatto deve essere immediatamente notificata all'altra parte.

Allegati:

1. Oggetto del trattamento dei dati personali
2. Misure tecniche e organizzative di sicurezza;
3. Elenco dei Sub-responsabili autorizzati.

Luogo e data _____

Il Titolare

_____

Il Responsabile

_____

Amministratore Unico
Fabrizio De Fabritiis

***

ALLEGATO 1

Oggetto del trattamento dei dati personali

Con riferimento al Contratto relativo al trattamento dei dati soprariportato, le parti consentono che i seguenti servizi relativi e/o che includano il trattamento dei dati personali vengano forniti dal Responsabile del Trattamento.

1. **Oggetto del servizio**

L'oggetto del servizio è il risultato dei seguenti compiti del Responsabile del trattamento:

Capitolato Speciale d'Appalto – CIG – Appalto per il Servizio di Call Center Milano Ristorazione SPA

2. **Dati relativi al servizio**

Scopo, natura della conservazione, trattamento ed uso dei dati personali

Il Contact Center verrà instradato tramite numero verde 800.710.980 di proprietà di Milano Ristorazione S.p.A. attestato tramite deviazione su procedura CRM che dovrà essere messa a disposizione dalla Società aggiudicataria.
Il servizio di Contact Center è il principale contatto tra la società Milano Ristorazione SpA e i City users (Utenti fruitori del servizio di refezione scolastica) e dovrà fornire informazioni, con le seguenti modalità:1) multicanale (telefono, web) da rete fissa, cellulare ed app mobile; 2) IVR (risponditore automatico) che fornisce le prime informazioni di carattere generale assistendo ed indirizzando il City User, attraverso un percorso guidato, verso la risposta attesa e registrata e dovrà essere strutturato su 2 (due) livelli:
I° Livello – opera con un insieme di risorse, tecnologie integrate di telecomunicazione e informatiche e di processi, che consentono di gestire i contatti telefonici tra Milano Ristorazione SpA e gli utenti del servizio di refezione scolastica inbound.
II° Livello - opera in co-sourcing con il personale interno della Società Milano Ristorazione in modalità off-line prendendo in carico le problematiche non risolte dal I° Livello, che richiedano un approfondimento informativo o richieste di assistenza per i relativi ambiti di competenza.

I dati personali debbono essere trattati ed utilizzati esclusivamente nel territorio di uno Stato membro dell'Unione Europea (UE) o di altro stato firmatario dell'Area Economica Europea (EEA).

Il Titolare del Trattamento fornirà al Responsabile del Trattamento le seguenti categorie di dati personali degli interessati relativi ai suddetti scopi:

Categorie di dati:

- Codice identificativo dell'utente/tutore
- Cognome/Nome
- Informazioni di contatto (numero di telefono, numero di cellulare, indirizzo email)
- Indirizzo
- Data di nascita
- Dati bancari (IBAN)
- Dati di fatturazione e di pagamento
- Situazione reddituale del nucleo (Dati ISEE)
- Dati sensibili (speciali categorie di dati personali ai sensi dell'art. 9 del GDPR: dati personali relativi alle origini raziali ed etniche, religiose o filosofiche, dati relativi alla salute)

- Informazioni che permettono la creazione di un profilo personali o tracciamento del profilo (es. Tracking Cookies)
- Dati di telecomunicazione (es. utilizzo di dati provenienti dall'uso dei servizi di telecomunicazioni, tracciamento delle call individuali nel contesto della legge relativa alle telecomunicazioni).

Interessati:

- Utenti (alunni/tutori)

3. Specifiche tecniche e misure organizzative ulteriori rispetto a quanto previsto dall'Allegato 2 ***(a cura del fornitore)***

- Nessuna specifica misura tecnica e organizzativa

- Se necessario per il Responsabile del Trattamento adottare ulteriori misure di sicurezza per questo specifico Contratto che vadano oltre le misure tecniche ed organizzative previste nell'allegato 2, queste misure debbono essere elencate di seguito.

  Se un adeguato livello di protezione può essere garantito dal Responsabile del Trattamento, il Titolare del Trattamento richiede l'autorizzazione dei dipendenti nominati dal Responsabile da questo contratto per il tele lavoro o accesso remoto. Se questo non può essere garantito, il Responsabile deve prevedere adeguate misure.

4. Sub-responsabili

- Nessun subappaltatore
- Subappaltatore in UE o EEA (*completare con dati societari ed indirizzo*)

5. Diritti di controllo del Titolare del Trattamento

Le regolari visite di controllo di cui all'art. 3 del presente Contratto, fatto salvo il diritto del Titolare del Trattamento di effettuare le visite non programmate nel caso di incidenti sospetti o non conformità con le misure tecniche ed organizzative, sono stabilite come segue: entro un anno dall'inizio del trattamento e successivamente su una base regolare di tre anni.

6. Persone di contatto

Le parti nominano le seguenti persone di contatto per l'esecuzione di un singolo ordine:

Per il Titolare del Trattamento: [*];

Per il Responsabile del Trattamento: [*]

Qualsiasi modifica relativa le sopramenzionate persone o la responsabilità delle persone di contatto deve essere immediatamente notificata all'altra parte.

***

ALLEGATO 2

Misure tecniche e organizzative di sicurezza

1. Sicurezza

Il presente Allegato 2 del Contratto fornisce i requisiti base per il rispetto dei livelli di sicurezza ritenuti necessari dal Titolare la cui realizzazione da parte del Responsabile è parte integrante del presente Contratto. Il Responsabile si obbliga a rispettare la Normativa applicabile.

Il Responsabile garantisce che:

- all'interno della propria organizzazione è individuata la struttura di Information Security ed il suo responsabile;
- nella struttura di Information Security sono adottate misure di sicurezza adeguate e che sono eseguite le opportune periodiche verifiche di sicurezza e gli audit;
- le terze parti con cui collabora (relativamente alle attività e alle infrastrutture fornite e utilizzate per la Società) sono qualificate e certificate 'sicure', restando in ogni caso a carico del Responsabile la responsabilità dell'affidabilità terze parti in termini di sicurezza.

Di seguito vengono riportate le attività che il Responsabile svolgerà.

1) Sviluppare e mantenere aggiornati gli standard di sicurezza, adottando una Information Security Policy in conformità alle best practices, periodicamente aggiornata. La Information Security Policy sarà a disposizione del Titolare con le altre procedure che tengano conto delle best practices del settore.
2) Rimanere aggiornato su norme, regole o vulnerabilità segnalate e relative alla sicurezza.
3) Mettere a disposizione una struttura di riferimento per il monitoring continuo della sicurezza e per la gestione degli assessment (su richiesta del Titolare).
4) Fornire costantemente personale specializzato a supporto dello staff del Titolare.
5) Fornire il piano di sicurezza IT e le infrastrutture necessarie in base ai requisiti di sicurezza, della Normativa applicabile e delle procedure.
6) Implementare i piani di sicurezza fisica e logica coerenti con le best practices (e.g. ISO 27001).
7) Recepire le richieste di abilitazione, di accesso, di pubblicazione di Applicazioni e Servizi, provenienti dal Titolare, formulate necessariamente ad alto livello, e trasformarle in Policy/Regole di implementazione e configurazione di dettaglio per tutti gli apparati in ambito (es. firewall, router, switch, IDS/IPS, antivirus, ecc.).
8) Stabilire la profilazione degli accessi relativi alle utenze e le policy per adding, changing, enabling/disabling.
9) Eseguire la profilazione degli accessi infrastrutturali relativi alle utenze.
10) Eseguire le modifiche di accesso a livello di sistema operativo e software di sistema.
11) Garantire che tutti i supporti di backup e di archiviazione che contengono informazioni riservate del Titolare siano conservati in aree di memorizzazione sicure e controllate a livello ambientale, detenute, gestite o contrattate dal Responsabile. Le aree di archiviazione utilizzate per memorizzare tali supporti dovranno essere programmate per ridurre ragionevolmente impatti derivanti da minacce ambientali.
12) Assicurare che i propri sistemi impediscano adeguatamente i tentativi di accesso da parte di utenti non autorizzati, ad esempio bloccando l'accesso dopo la ripetizione di un numero minimo di tentativi.
13) Garantire che le chiavi crittografiche e i certificati digitali siano gestiti in modo sicuro in qualsiasi momento, in conformità con i requisiti di controllo documentati e le procedure coerenti con le best practices.
14) Assicurare che tutte le connessioni esterne ai propri sistemi (inclusi, senza limitazione, reti o accesso remoto) siano individuate, verificate, registrate e approvate individualmente dallo stesso.
15) Assicurare che l'accesso wireless ai propri sistemi sia soggetto all'autorizzazione di autenticazione e ai protocolli di crittografia in linea con le best practices e siano consentiti solo dalle posizioni approvate dal Responsabile stesso.
16) Condurre Vulnerability assessment periodici (come da SLA) per identificare eventuali Security gaps, condividendo con il Titolare i risultati ed il piano di risoluzione. In particolare:

a) se il Vulnerability assessment dovesse identificare rischi critici, elevati o moderati, il Titolare presenterà una soluzione alternativa (remediation plan) entro dieci (10) giorni lavorativi dal termine dell'assessment. Il remediation plan sarà attuato tempestivamente e indicherà le azioni necessarie per la mitigazione dei rischi, con specificazione delle date entro le quali saranno completate le azioni di risoluzione dei rischi ad alto e medio livello. Il costo di attuazione del piano di bonifica sarà affrontato esclusivamente dal Responsabile.
b) Il Titolare si riserva il diritto di approvare le date e le azioni contenute nel remediation plan e, una volta completato, il Responsabile provvederà alla conferma dell'avvenuta implementazione delle azioni ivi indicate. Di conseguenza, il Titolare avrà il diritto di effettuare o far effettuare ad un terzo una Valutazione della Sicurezza (in entrambi i casi a spese del Responsabile), al fine di convalidare l'avvenuta mitigazione dei rischi.

17) Fornire log su connessioni e accessi, includendo adempimenti degli amministratori di sistema. L'attività di gestione del tracciamento e dei log file è demandata al Responsabile (salvo diverse indicazioni concordate) per i componenti che esso fornisce e di cui esegue la manutenzione tra sistemi operativi, database e applicativi.

Al proposito, il Responsabile farà sì che:

- sia realizzata l'implementazione di un sistema di registrazione e gestione dei log, comprensivo di funzionalità di non-ripudio dove necessario e previsto dalla normativa;
- I file di log siano resi disponibili al Titolare entro massimo tre (3) giorni dalla richiesta di quest'ultima;
- i file di log contengano il tracciamento relativo a chi ha avuto accesso (login, login denied e logout) ai dati ed il tracciamento relativo all'utente, la data, l'orario e l'IP che hanno eseguito l'operazione. Il Responsabile consegnerà un report con Time Stamp e login relativo a tali accessi.

18) Risolvere le violazioni di sicurezza fornendo adeguata reportistica al Titolare
19) Risolvere eventuali violazioni esterne (*Es.* denial-of-service attacks, spoofing, Web exploits, etc.).
20) Verificare tutte le patch di sicurezza rilevanti per l'ambiente e classificare la necessità e la priorità con cui le patch di sicurezza devono essere installate.
21) Installare le Security patches per il Titolare secondo le procedure di Change Management.
22) Mantenere aggiornata tutta la documentazione necessaria per i controlli di sicurezza e di controllo interno e per i test di controllo.
23) Posizionare i sistemi di supporto che contengono dati sensibili in aree ad accesso controllato e conformemente alla Normativa applicabile. Ai soli utenti con un accesso valido e autorizzato sarà permesso di entrare in queste aree.
24) Segregare il sistema informativo del Titolare da altri sistemi informativi, tra cui quello del Responsabile.

2. Sicurezza fisica

I servizi di sicurezza fisica sono associati ai controlli degli accessi fisici implementati per garantire la sicurezza degli apparati, impianti e sistemi di gestione del Titolare e del Responsabile.

Di seguito vengono riportate le attività garantite dal Responsabile:

- definire e mantenere aggiornate practices, policy e procedure per garantire la sicurezza fisica nei locali sotto il proprio controllo rimanendo aggiornati su norme, regole o vulnerabilità segnalate e fornendo servizi in conformità con quanto definito nel Contratto;
- rivedere e approvare i cambiamenti alle practices, policy e procedure congiuntamente al Titolare per l'approvazione;
- collaborare con il Titolare nella modifica delle practices, delle policy e delle procedure per colmare le lacune e contestualmente garantire la sicurezza fisica in modo efficiente ed efficace;
- proteggere le apparecchiature del data center e i servizi di gestione utilizzati per il Titolare dagli accessi non autorizzati e da eventuali rischi ambientali e avarie infrastrutturali (meccanico, elettrico, HVAC, cablaggi).

In particolare, il Responsabile garantisce che le infrastrutture di supporto IT (il sistema informativo) che contengono applicazioni e dati dei processi eseguiti per il Titolare saranno collocati all'interno di locali (il Data Center o assimilati) aventi le seguenti caratteristiche:

- monitoraggio degli ingressi/uscite tramite controllo degli ingressi fisici per il personale autorizzato (con tessera magnetica abilitata e tracciata sul sistema di controllo);
- controllo degli ingressi fisici tramite rilascio di badge di identificazione a fronte della fornitura delle credenziali di identità;
- presenza di adeguati sistemi di difesa passiva e, quanto meno, di inferriate o blindatura alle finestre e porte antisfondamento;
- presenza di controlli antintrusione fisica realizzati con telecamere interne o, in alternativa, anche sistemi volumetrici;
- presenza di adeguate misure di prevenzione ambientale e, quanto meno, di un sistema di rilevamento fumi e sistema antincendio allarmato, sistema di rilevamento allagamento allarmato, sistema di rilevamento temperatura allarmato;
- presenza di un sistema di continuità elettrica costituito da UPS di zona e gruppi elettrogeni;
- utilizzo di opportuno sistema di condizionamento.

Il Responsabile si impegna inoltre a:
- proteggere fisicamente e conservare i supporti portatili che contengono dati del Titolare assicurandosi che l'accesso agli stessi sia permesso solo al personale autorizzato.
- far sì che i sistemi informatici consentano la possibilità di revocare immediatamente l'accesso alle apparecchiature di elaborazione dati, ai servizi e ai supporti di memorizzazione;
- mantenere registri di controllo degli accessi informatizzati.

Il Responsabile garantisce che i locali in cui vengono eseguite le lavorazioni dei processi sono dotati di servizio di portineria o di videocitofono e controllo degli ingressi, registrazione e rilascio di badge di identificazione.

3. IT Identity e Access Management

I servizi di IT Identity e Access Management (IAM) sono le attività associate ad autorizzare, autenticare e fornire il controllo degli accessi a tutti i sistemi informativi che risiedono nell'infrastruttura del Titolare.

Di seguito vengono riportate le attività che il Responsabile deve svolgere:

- collaborare con il fornitore IAM per individuare / progettare e realizzare i collegamenti con lo IAM, l'ITSM e altri sistemi IT definendo le best practices, le policy e le procedure per l''IT Identity e Access Governance;
- fornire il servizio di IT Identity e Access Management in conformità con le policy, procedure e practices del Titolare (tra cui le policy di sicurezza);
- mantenere l'IT Identity e Access Management allineato alle practices, policy e procedure del Titolare soprattutto nel caso di modifiche al perimetro (*e.g.*, il cambiamento delle tecnologie, aggiunte o modifiche di ruoli);
- definire i ruoli, le attività autorizzate e i privilegi minimi concessi al personale del Responsabile e al personale del Titolare (inclusi gli account non-personali);
- definire e gestire il processo per la definizione, l'assegnazione, la modifica e la revoca degli account utente e per supportare gli accessi temporanei;
- definire, supportare implementare e manutenere la soluzione di IT IAM idonea al Sistema informativo del Titolare;
- fornire e implementare una soluzione per interfacciare i processi di IT Identity e Access Management del Titolare e del Responsabile;
- fornire le specifiche di registrazione dei log e l'archiviazione;

- utilizzare password complesse (minimo 8 caratteri di tipologia differente, reimpostazione password obbligatoria al primo accesso, scadenza password);
- assegnare ad ogni utente credenziali (user e password) personali, uniche e non assegnabili ad altri utenti;
- rimuovere gli account inattivi o non più necessari in accordo alle policy e norme del Titolare;
- rivedere periodicamente gli account IT e utente con tutti i privilegi e le autorizzazioni al fine di assicurare che tutti gli utenti abbiano gli appropriati privilegi in base al loro impiego lavorativo, in accordo alle policy e norme del Titolare;
- fornire al Titolare, entro sette (7) giorni, adeguato report sulle eventuali anomalie riscontrate.

4. Servizi di sicurezza di rete

Di seguito vengono riportate le attività garantite dal Responsabile e inerenti la gestione dei firewall, dei Servizi di Intrusion Prevention e Detection del datacenter e dei Security Vulneralibity assessment e Penetration testing:

- definire practices, policy e procedure per la gestione dei firewall, dei Servizi di Intrusion Detection, Intrusion Prevention, Security Vulnerability e Penetration;
- erogare i servizi in conformità con le policy e i requisiti definiti.

***

ALLEGATO 3

Elenco dei Sub-responsabili autorizzati alla data di firma del presente contratto. Eventuali modifiche andranno tempestivamente notificate al Titolare, laddove non siano previsti subfornitori già in fase di sottoscrizione l'allegato 3 non deve essere compilato.

Sub-responsabile	**Sede e dati di contatto / Luogo del trattamento**	**Attività di trattamento**