COMUNE DI GENOVA

Direzione Stazione Unica Appaltante

ACCORDO SUL TRATTAMENTO DEI DATI

ai sensi dell'art. 28 del Regolamento generale (UE) 2016/679

per il servizio di facchinaggio presso uffici e sedi comunali, scuole comunali e statali site nel territorio di Genova – CIG A04393F694

Accordo tra la Civica Amministrazione (di seguito "Amministrazione"), nella sua veste di titolare del trattamento ai sensi dell'art. 4, par. 1, n. 7 del Regolamento generale (UE) 2016/679, con sede legale in via Garibaldi, 9, 16124, Genova, P.IVA/C.F. 00856930102, rappresentata per il presente atto dal Dottor/Dottoressa Angela Ilaria Gaggero della Direzione Stazione Unica Appaltante

E

la Società/Associazione/etc. (di seguito "Fornitore") _____, nella sua qualità di responsabile del trattamento ai sensi dell'art. 4, par. 1, n. 8 del Regolamento generale (UE) 2016/679, con sede legale in _____, P.IVA/C.F. _____ rappresentata per il presente atto dal Dottor _____, munito degli idonei poteri.

Visti:

- il Regolamento generale (UE) 2016/679 (in seguito "GDPR");
- il D.lgs. 196/2003 (di seguito "Codice"), modificato dal D.lgs. 101/2018;
- il Regolamento in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati (d'ora innanzi "Regolamento") approvato con deliberazione del Consiglio Comunale n. 78 del 21 settembre 2021;

Premesso che:

- in esecuzione della determinazione dirigenziale _____, numero GIG …….. in data ……. è stato stipulato il contratto _____, numero repertorio _____ che ha come oggetto la stipula di un Accordo Quadro avente ad oggetto il servizio di facchinaggio presso uffici e sedi comunali, scuole comunali e statali site nel territorio di Genova;
- il Fornitore ai sensi dell'art. 6 c. 1 del Regolamento è stato scelto in virtù dei requisiti di esperienza, capacità e affidabilità in relazione alle peculiarità della materia di che trattasi;
- il Fornitore ai sensi dell'art. 6 c. 2 del Regolamento è stato contrattualizzato e, con il presente atto, verrà nominato responsabile del trattamento perché è in possesso di caratteristiche professionali e organizzative in relazione alle peculiarità del servizio o del lavoro affidato tali da mettere in atto misure tecniche e organizzative adeguate a tutelare i dati personali degli interessati dai rischi del trattamento e consentire l'esercizio dei diritti degli interessati previsti dal Capo III del GDPR con le modalità disciplinate dall'art. 4 del Regolamento;

Nomina del responsabile del trattamento

Tutto ciò premesso:

- con la sottoscrizione del presente Accordo, che forma parte integrante e sostanziale del/della contratto/convenzione/etc. di cui sopra, l'Amministrazione, titolare del trattamento, in persona del dirigente, nomina il presente Fornitore, quale responsabile del trattamento sulla base dell'art. 28 del GDPR e degli artt. 5, c. 3, lett. g) e 6 del Regolamento;
- il Fornitore si impegna ad assicurare il rispetto dei principi di liceità, correttezza, trasparenza, minimizzazione dei dati, limitazione della finalità e della conservazione, integrità e riservatezza, nonché favorire l'esercizio dei diritti degli interessati, specificando che le comunicazioni di dati personali diversi da quelli di cui agli artt. 9 e 10 del GDPR devono essere effettuate nel rispetto dell'art. 2-ter del Codice;
- il Fornitore, nella sua qualità di responsabile del trattamento, conferma di conoscere gli obblighi di conformità alle norme (*compliance*) al GDPR e al Codice;
- il Fornitore, con la sottoscrizione del presente Accordo, accetta la nomina quale responsabile del trattamento;
- il Fornitore si impegna ad effettuare tutti i trattamenti per conto dell'Amministrazione nel pieno rispetto dei principi dell'art. 5 e dell'art. 32 del GDPR in piena autonomia gestionale, anche sotto il profilo economico, ivi incluse le attività o parte delle attività di trattamento effettuate da soggetti TERZI, quali ad esempio, SOCIETÀ COLLEGATE, SUBAPPALTATORI, SUBFORNITORI, etc. (cd. SUB-RESPONSABILI) sulla base dell'art. 28, par. 2 e 4 del GDPR e dell'art. 6, c. 3 del Regolamento;
- il Fornitore si impegna a segnalare tempestivamente al titolare del trattamento qualsiasi mutamento dei requisiti di cui al citato art. 6, commi 1 e 2 del Regolamento che possa sollevare incertezze sul loro effettivo mantenimento, scrivendo all'indirizzo e-mail del referente privacy di direzione e per conoscenza al DPO: dpo@comune.genova.it
- il Fornitore, in veste di responsabile del trattamento, si impegna ad attenersi alle seguenti **ISTRUZIONI DOCUMENTATE** e a quelle ulteriori che gli potranno essere conferite nel corso del tempo in relazione ai rischi di *compliance* alla disciplina in materia di protezione dei dati personali (artt. 5, 24, 25, 30, 32, 33, par. 2, 82 e 83 del GDPR).

ISTRUZIONI DOCUMENTATE

a. descrizione del trattamento
a.1. banche dati degli ambiti di competenza Il dirigente ai sensi dell'art. 5, c. 3 del Regolamento mette a disposizione del Fornitore i seguenti sistemi e banche dati degli ambiti di competenza: dati afferenti i dipendenti, utenti e referenti per le sedi interessate dal servizio richiesto.
a.2. finalità del trattamento La stipula di un Accordo Quadro avente ad oggetto il servizio di facchinaggio interno ed esterno alle sedi comunali.
a.3. categorie degli interessati Le categorie degli interessati sono i dipendenti, utenti e referenti per le sedi interessate dal servizio richiesto.
a.4. tipologia dei dati Il Fornitore - in applicazione del principio di minimizzazione dei dati di cui all'art. 5, par. 1, lett. c) del GDPR - raccoglie: **dati comuni** (es. nome e cognome, indirizzo e-mail, numero di cellulare, codice fiscale, luoghi di lavoro, taglie, altezza, peso etc.).
a.5. informativa sul trattamento dei dati personali ai sensi degli artt. 13 e 14 del GDPR Il Fornitore definisce con l'Amministrazione i contenuti delle informative privacy e si impegna ai sensi dell'art. 12 del GDPR a rendere le informazioni in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio chiaro e semplice. Il Fornitore prima della raccolta dei dati personali informa l'interessato sulle modalità del trattamento e cura il costante aggiornamento delle informative privacy.
a.6. consenso al trattamento Il Fornitore informa l'interessato quando il trattamento dei dati è subordinato all'acquisizione del consenso, facoltativo ai sensi dell'art. 6, par. 1, lett. a) del GDPR nonchè sulla possibilità di revoca in qualsiasi momento ai sensi dell'art. 7, par. 3 del GDPR. A titolo di esempio, occorre il consenso dell'interessato nella raccolta di foto e video (solamente se diffusi), nel trattamento dei dati di minori (per il minore il consenso lo esprime il genitore/tutore), nell'attività di marketing diretto, nella profilazione, etc. Il Fornitore rende facilmente accessibile il diritto alla revoca del consenso prestato e l'opposizione al trattamento di cui agli artt. 7, 21 e 22 del GDPR.
b.7. rappresentante in Italia Il Fornitore non stabilito nell'U.E. ai sensi dell'art. 27, par. 3 del GDPR designa un rappresentante in Italia (*indicare, se previsto, il nominativo del rappresentante in Italia*).
b.8. trasferinento dei dati al di fuori dell'U.E. (preventiva autorizzazione)

Il Fornitore - in applicazione del Capo V del GDPR - si impegna a NON trasferire dati personali in paesi al di fuori dello Spazio Economico Europeo (SEE) che non garantiscano il livello adeguato di tutela previsto dal GDPR.

Il Fornitore che intende trasferire al di fuori dell'U.E. dati personali si impegna a inoltrare una ***preventiva autorizzazione scritta*** all'indirizzo e-mail del referente privacy di direzione e per conoscenza al DPO: dpo@comune.genova.it

b - istruzioni per i sub-responsabili

b.1. garanzie sui profili tecnici e di sicurezza

Il Fornitore ai sensi dell'art. 28, par. 4 può avvalersi di sub-responsabili che prestino 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.

Il Fornitore, qualora intenda avvalersi di soggetti TERZI che trattano dati personali e potenzialmente hanno accesso a tali dati, regola i rapporti interni con detti sub-responsabili, mediante un contratto o altro atto giuridico ai sensi dell'art. 28, par. 4 del GDPR. A titolo esemplificativo ma non esaustivo, attività sistemistica dell'infrastruttura IT dei servizi, manutenzione e assistenza sugli applicativi, etc.

Il Fornitore si impegna, senza costi aggiuntivi per l'Amministrazione, e in linea con gli artt. 25 e 32 del GDPR, a fornire istruzioni ai sub-responsabili sull'adozione delle misure di sicurezza:

Il Fornitore si impegna verso l'Amministrazione affinchè i sub-responsabili ai sensi dell'art. 6 del Regolamento offrano garanzie in termini di requisiti di esperienza, capacità e affidbilità NON inferiori a quelle garantite con l'accettazione della presente nomina.

b.2. autorizzazione preventiva (elenco dei sub-responsabili)

Qualora il Fornitore intenda avvalersi di TERZI, sub-responsabili, per le attività (o parte delle attività) di trattamento - già in sede di sottoscrizione del presente Accordo - trasmette via e-mail al referente di direzione e per conoscenza al DPO: dpo@comune.genova.it un elenco con i nominativi dei sub-responsabili ai fini *dell'autorizzazione preventiva* da parte del titolare del trattamento.

Il Fornitore inoltra al titolare del trattamento - in ogni momento - una richiesta scritta di *autorizzazione preventiva* ad avvalersi di sub-responsabili ai sensi dell'art. 28, par. 2 e 4 del GDPR con le modalità previste dall'art. 6 c. 3 del Regolamento.

b.3. autorizzazione preventiva al di fuori dello Spazio Economico Europeo (SEE)

Nella scelta dei sub-responsabili, il Fornitore considera in via prioritaria, a parità di garanzie, soggetti situati sul territorio nazionale e dell'U.E., istruendoli sulla necessità di trattare i dati all'interno dello spazione economico europeo (SEE).

Laddove ciò non fosse possibile, il Fornitore può ricorrere a sub-responsabili situati in paesi al di fuori dell'U.E., richiedendo *l'implementazione di misure supplementari* al fine di garantire la protezione dei dati personali degli interessati. In tal caso il Fornitore si impegna a trasmettere una richiesta via e-mail al referente privacy di direzione e per conoscenza al DPO: dpo@comune.genova.it diretta a ottenere un'*autorizzazione preventiva* a ricorrere a sub-responsabili stabiliti al di fuori dello spazio SEE.

c - istruzioni sulle misure di sicurezza

c.1. livello di sicurezza dei dati

Il livello di sicurezza dei dati personali dipende da vari elementi, quali ad esempio, tipologia dei dati trattati, contesto di riferimento, sistemi utilizzati dal Fornitore e la presenza di sub-responsabili.

Ai fini del presente Accordo il livello di sicurezza atteso è quello volto a garantire la confidenzialità, l'integrità, la disponibilità e la resilienza degli strumenti tecnologici.

Il Fornitore si impegna a trattare i dati per conto dell'Amministrazione con la medesima cura con la quale tratta i dati personali dei propri clienti in modo da garantire un'adeguata protezione a detti dati.

c.2. decisioni sul livello di sicurezza

Il Fornitore e i sub-responsabili hanno il diritto e l'obbligo di prendere decisioni sulle misure di sicurezza tecniche e organizzative che sono finalizzate a garantire il livello di sicurezza dei dati adeguato al rischio in linea con gli artt. 25 e 32 del GDPR.

Nel valutare l'adeguato livello di sicurezza si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Tali misure comprendono 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, nonchè una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative messe in atto.

c.3. misure tecniche e organizzative applicate ai DATI COMUNI

Per la protezione dei DATI COMUNI il Fornitore si obbliga ad applicare le seguenti misure tecniche e organizzative adeguate ai rischi del trattamento:

1. valutare le misure minime di sicurezza della circolare AgID 2/2017 per quanto applicabili.
2. obbligo di segnalare - entro entro 24 ore - qualsiasi minaccia e/o evento di una ***violazione di dati*** alla Direzione Stazione Unica Appaltante contattando immediatamente il DPO: tel. 010 5572665, e-mail dpo@comune.genova.it e il referente privacy di direzione, mettendo fin da subito in atto misure tecniche e organizzative al fine di mitigare le conseguenze della minaccia/violazione a tutela degli interessati coinvolti e attuando altresì tempestive azioni correttive in stretto coordinamento con la direzione e il DPO dell'Amministrazione;
3. obbligo di segnalare - entro le 24 ore - alla Direzione Stazione Unica Appaltante qualsiasi malfunzionamento o **violazione di piattaforme software** e dei **suoi sistemi di sicurezza.** Tale obbligo segue le modalità indicate al precedente punto 1. per consentire, anche in questo caso, all'Amministrazione di notificare all'autorità di controllo e, ove necessario, effettuare la comunicazione agli interessati;
4. garantire che ***le persone autorizzate al trattamen***to accedano ai dati personali solo dopo che sono state individuate, formate e formalmente designate con istruzioni all'utilizzo dei dati e siano obbligate alla riservatezza sui dati trattati, ai sensi degli artt. 28, par. 3, lett. b), 29 e 32 ultimo paragrafo del GDPR con le modalità previste dall'art. 2-quaterdecies del Codice;

5. agevolare l'***esercizio dei diritti dell'interessato*** informando tempestivamente - entro 2 giorni lavorativi - via e-mail il referente privacy di direzione e per conoscenza il DPO: dpo@comune.genova.it con le modalità previste dall'art. 4 del Regolamento;
6. assolvere agli ***obblighi informativi*** di cui agli artt. 13 e 14 del GDPR;
7. predisporre, aggiornare e conservare un ***registro*** di tutte le categorie di attività relative al trattamento svolte per conto dell'Amministrazione, salvo i casi di esenzione disciplinati dal par. 5 dell'art. 30 del GDPR;
8. assistere la Direzione Stazione Unica Appaltante nello svolgimento di una valutazione di impatto sulla protezione dei dati e nella consultazione preventiva in relazione ai trattamenti caratterizzati da un rischio elevato e in assenza di misure di attenuazione di tale rischio;
9. utilizzare protocolli di sicurezza previsti dallo standard TLS 1.2. o superiori nei vari contesti applicativi (es. protocollo di rete HTTPS) secondo le raccomandazioni AgID del 03/11/2020;
10. considerare le raccomandazioni dell'autorità di controllo 25.10.2021 sull'impostazione e gestione pasword sicure nel quadro delle attività di educazione digitale di base [doc-web 9709765];
11. impostare l'obbligo di cambio password al primo accesso, alla luce delle raccomandazioni citate al precedente punto 9. [doc-web 9709765];
12. aggiornare in modo periodico e costante i sistemi allo scopo di prevenire la loro vulnerabilità.

c.4. misure tecniche e organizztive applicate a CATEGORIE PARTICOLARI DI DATI

Per aumentare la protezione dei DATI SENSIBILI disciplinati dall'art. 9 del GDPR e dall'art. 2-septies del Codice, il Fornitore si obbliga ad applicare, oltre alle misure tecniche e organizzative concordate per i DATI COMUNI, le seguenti ulteriori misure, considerato il conteso, lo stato dell'arte e i costi di attuazione:

1. utilizzare tecniche di *strong authentication*, consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione (user ID e password) e codici OTP (one-time-password), cioè una password generata automaticamente da un token e usabile una sola volta;
2. utilizzare tecniche di cifratura dei dati (TLS 1.3) nei vari contesti applicativi (es. protocollo di rete HTTPS), raccomandazioni AgID del 03.11.2020;
3. implementare la crittografia end-to-end (E2EE);
4. mettere in atto policy restrittive sull'accesso ai dati che prevedano un profilo con credenziali di accesso selettivo ai dati, nonchè un livello diversificato di visibilità e di trattamento correlato ai compiti degli autorizzati al trattamento e agli Admin di sistema;
5. concordare l'eventuale istituzione di un security TEAM (Admin di sistema e DPO).

c.5. misure tecniche e organizzative applicate a CONDANNE PENALI E REATI

Per aumentare la protezione dei DATI GIUDIARI disciplinati dall'art. 10 del GDPR e dall'art. 2-octies del Codice, il Fornitore si obbliga ad applicare, oltre alle misure tecniche e organizzative concordate per i DATI COMUNI, le seguenti ulteriori misure, considerato il conteso, lo stato dell'arte e i costi di attuazione:

1. utilizzare tecniche di *strong authentication*, consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione (user ID e password) e codici OTP (one-time-password), cioè una password generata automaticamente da un token e usabile una sola volta;
2. utilizzare tecniche di cifratura dei dati (TLS 1.3) nei vari contesti applicativi (es. protocollo

di rete HTTPS), raccomandazioni AgID del 03.11.2020;

3. implementare la crittografia end-to-end (E2EE);
4. mettere in atto policy restrittive sull'accesso ai dati che prevedano un profilo con credenziali di accesso selettivo ai dati, nonchè un livello diversificato di visibilità e di trattamento correlato ai compiti degli autorizzati al trattamento e agli Admin di sistema;
5. concordare l'eventuale istituzione di un security TEAM (Admin di sistema e DPO).

c.6. codici di condotta/certificazioni

Ai fini della dimostrazione della propria idoneità alla presente nomina, è valutata l'adesione a codici di condotta o a meccanismi di certificazione approvati ai sensi degli artt. 40 e 42 del GDPR.

c.7. sicurezza fisica

Il Fornitore comunica all'indirizzo e-mail del referente privacy di direzione le procedure per l'accesso fisico ai locali del Data Center.

Il dirigente può concordare con il Fornitore l'ispezione fisica dei luoghi del trattamento; di tale sopraluogo viene redatto verbale a cura del referente privacy di direzione.

c.8. audit e ispezioni

Il Fornitore contribuisce alle attività di audit esterno con la Direzione Stazione Unica Appaltante sulla base di quanto previsto dall'art. 5, c. 3, lett. f) del Regolamento.

Il Fornitore agisce tempestivamente e in autonomia nei casi di ispezione disposte dall'autorità di controllo informando via e-mail il referente privacy di direzione e per conoscenza il DPO: dpo@comune.genova.it

Il rapporto di audit e quello di ispezione sono presentati - senza ritardo - all'indirizzo e-mail del referente privacy di direzione e per conoscenza al DPO: dpo@comune.genova.it

c.9. piano per la gestione dei rischi

Il Fornitore verifica periodicamente la rispondenza dei sistemi alle misure tecniche e organizzative nonchè la corretta conservazione dei file di log applicatvi e di sistema.

Le attività di controllo e di aggiornamento devono essere adeguatamente documentate nel piano per la gestione dei rischi, in modo che sia sempre possibile risalire ai sistemi verificati, alle operazioni tecniche su di essi effettuate, alle risultanze delle analisi e alle eventuali criticità riscontrate.

Il Fornitore comunica annualmente gli aggiornamenti al piano di gestione dei rischi e comunica senza ritardo eventuali criticità riscontrate, entrambi all'indirizzo e-mail del referente privacy di direzione e per conoscenza al DPO: dpo@comune.genova.it

c.10. elenco Admin di sistema

Per quanto riguarda gli accessi degli Admin, il Fornitore deve assicurare la puntuale adozione delle misure previste dall'autorità di controllo con il provvedimento del 2008, aggiornato nel 2009 [doc. web 1626595].

Il Fornitore in un'ottica di *accoutability* trasmette - con cadenza annuale - all'indirizzo e-mail del referente privacy di direzione e per conoscenza al DPO: dpo@comune.genova.it l'elenco completo e aggiornato degli Admin di sistema.

c.11. periodo di conservazione dei dati personali (criteri per la deterninazione previsti dagli

artt. 13 e 14, par. 2, lett. a) del GDPR

Il Fornitore conserva i dati personali per il periodo di tempo strettamente necessario al conseguimento delle finalità per le quali sono stati raccolti.

Il Fornitore si obbliga a gestire l'intero periodo di conservazione dei dati consentendone l'accesso solamente a persone individuate, formate, designate e istruite, in possesso di specifici profili di autenticazione e autorizzazione.

A tale riguardo tutti i dati personali devono confluire nei log applicativi e di sistema e devono essere:

- tracciati, prevedendo meccanismi di verifica delle operazioni effettuate;

- protetti da credenziali di autenticazione univoche e assegnate individualmente, con il cambio password al primo accesso;

- conservati per un tempo non inferiore a 6 mesi (provvedimento dell'autorità di controllo [doc. web 1626595]).

Fatta eccezione per i tempi di conservazione dei log che tracciano gli accessi degli Admin di sistema (per i quali è previsto un periodo minimo di conservazione di 6 mesi), in assenza di disposizioni normative, si ritiene congruo stabilire che il Fornitore conservi i dati personali per il periodo massimo di 10 anni dalla raccolta - limitatamente - alle informazioni necessarie per adempiere a obblighi legali e consentire all'Amministrazione l'eventuale accertamento, esercizio e difesa di un diritto in sede giudiziaria e/o in sede di accertamento fiscale.

Alla cessazione per qualsiasi causa del servizio/attività oggetto del presente Accordo, e decorsi i termini di conservazione obbligatoria, tutti i dati personali saranno distrutti, cancellati o resi anonimi e comunque resi inutilizzabili in maniera irreversibile, comprese le copie esistenti, mediante tecniche adeguate e sicure, tenuto conto dello stato dell'arte e dei costi.

Il Fornitore, entro un tempo congruo, comunica all'indirizzo e-mail del referente privacy di direzione e per conoscenza al DPO: dpo@comune.genova.it l'avvenuta distruzione, cancellazione o anonimizzazione e inutilizzabilità dei dati personali, comprese le copie esistenti.

Durata e cessazione del trattamento

La durata del trattamento corrisponde alla durata del servizio.

Una copia datata e firmata digitalmente del presente Accordo viene trasmessa dal referente privacy di direzione al Fornitore per integrale accettazione. L'Accordo si perfeziona al momento della reciproca sottoscrizione mediante firma digitale.

IL TITOLARE DEL TRATTAMENTO
Genova, __.__.____

La Dott.ssa Angela Ilaria Gaggero
Direzione Stazione Unica Appaltante
Comune di Genova

_____

IL RESPONSABILE DEL TRATTAMENTO
per integrale accettazione

Genova, __.__._____

Il Dott.
Società/Associazione/etc.
_____

DATI DI CONTATTO per le comunicazioni

PER IL TITOLARE DEL TRATTAMENTO
Il referente privacy di direzione
nome e cognome Angela Ilaria Gaggero
numero di cellulare/fisso _____
indirizzo e-mail igaggero@comune.genova.it

PER IL RESPONSABILE DEL TRATTAMENTO
Il dipendente indicato dal Fornitore
nome e cognome _____
numero di cellulare/fisso _____
indirizzo e-mail _____

PER IL RESPONSABILE DEL TRATTAMENTO
Il DPO del Fornitore, se nominato
nome e cognome _____
numero di cellulare/fisso _____
indirizzo e-mail _____