Accordo sul trattamento dell'Ordine in base all'Articolo 28 del Regolamento Generale sulla Protezione dei Dati [GDPR]

- di seguito definito "**Ordine**" -

tra

- Titolare del trattamento – di seguito denominato "Contraente" -

e

ista Italia s.r.l., via Lepetit 40, 20020 Lainate (Mi)

- Responsabile del trattamento – di seguito denominato "Commissionario"

1. Oggetto e durata dell'Ordine

(1) Oggetto dell'Ordine

L'oggetto dell'Ordine e i recapiti del Contraente risultano dai rispettivi accordi in base ai quali il Commissionario fornisce determinati servizi al Contraente come sopra individuato (di seguito definito "Contratto di Servizio").

(2) Durata

La durata del presente Ordine coincide con la durata del Contratto di Servizio.

2. Descrizione del contenuto dell'Ordine

(1) Tipologia e scopo del trattamento dei dati personali forniti

La tipologia e lo scopo del trattamento di dati personali del Contraente, da parte del Commissionario, sono specificamente descritti nel Contratto di Servizio.

Le disposizioni riferite al trattamento dei dati come contrattualmente concordate hanno validità esclusivamente in uno Stato membro dell'Unione Europea o in un altro stato facente parte dell'Area Economica Europea. Qualsiasi trasferimento in uno stato terzo richiede il preventivo consenso del Contraente e può essere effettuato solo in conformità di quanto stabilito dall'Articolo 44 e seguenti GDPR.

(2) Tipologia dei dati

Il contenuto del trattamento dei dati personali riguarda i seguenti tipi/categorie di dati (enumerazione/descrizione della categoria di dati)

- Dati anagrafici personali
- Recapiti (es.: telefono, e-mail)
- Estremi contrattuali (relazioni contrattuali, prodotti o interessi contrattuali)
- La storia del Contraente
- Dati riferiti alla fatturazione e ai pagamenti
- Dati relativi alla pianificazione e controllo
- Dati relativi ai proprietari, locatari, conduttori, ecc,. di abitazioni (es.: nome, indirizzo, ripartizioni, consumi)

(3) Categorie di persone interessate

Le categorie di persone interessate al trattamento includono:

- Clienti
- Potenziali acquirenti
- Partner di servizio di ista (es.: letturisti, installatori)
- Dipendenti
- Fornitori
- Contatti

- Proprietari, locatari, conduttori ecc. di abitazioni.

3. Misure tecnico-organizzative

(1) Il Commissionario deve implementare le misure tecnico organizzative di cui all'**Allegato 1**. Le misure così come elencate sono elementi essenziali dell'Ordine. Se a seguito dell'ispezione/valutazione eseguita da parte del Contraente risultasse la necessità di una correzione, questa deve essere implementata in accordo fra le parti.

(2) Il Commissionario deve garantire la sicurezza in osservanza dell'Articolo 28 (3) lett. c, e 32 GDPR, in particolare con riferimento all'Articolo 5 (1), (2) GDPR. In generale, le misure da adottare sono volte alla sicurezza dei dati e a garantire un livello di protezione appropriato rispetto al rischio a cui è esposta la riservatezza, integrità, disponibilità e resilienza dei sistemi. Devono essere tenuti in considerazione lo stato dell'arte, i costi di implementazione, la tipologia e lo scopo del trattamento, così come la probabilità dell'evento e la gravità del rischio riguardanti i diritti e le libertà delle persone fisiche secondo quanto statuito dall'Artico 32(1) GDPR. I dettagli sono riportati nell' **Allegato 1**.

(3) Le misure tecnico-organizzative sono soggette a modifiche e integrazioni conseguenti al progresso tecnologico e agli sviluppi futuri. A questo riguardo, il Commissionario ha il permesso di implementare adeguate misure alternative. Il livello di sicurezza delle misure definite deve essere adeguato e i cambiamenti significativi delle stesse devono essere documentati.

4. Correzione, limitazione e cancellazione dei dati

(1) Il Commissionario non può rettificare, cancellare o limitare il trattamento dei dati processati nel contesto dell'Ordine di propria iniziativa, ma solo in base alle istruzioni documentate del Contraente. Se una persona che ha un interesse diretto rispetto ai punti di cui sopra prende contatto con il Commissionario, quest'ultimo deve immediatamente reindirizzare la richiesta al Contraente.

(2) Compatibilmente con la natura del servizio, il concetto di cancellazione, il diritto all'oblio, la correzione, la portabilità dei dati e l'informazione devono essere garantiti direttamente dal Commissionario in accordo con le istruzioni documentate del Contraente.

5. Garanzia di qualità e altri obblighi a carico del Commissionario

(1) Oltre al rispetto delle prescrizioni connesse al presente Ordine, il Commissionario è tenuto anche all'osservanza degli obblighi previsti dagli articoli da 28 a 33 del GDPR; in particolare, deve garantire in l'osservanza delle seguenti prescrizioni:

a) Protezione della riservatezza ai sensi degli articoli 28(3) punto 2 lett. b, 29, 32 (4) GDPR. Nello svolgimento del lavoro, il Commissionario deve impiegare solamente personale vincolato alla riservatezza e che sia stato istruito anticipatamente sulle disposizioni che lo riguardano relativamente alla protezione dei dati. Il Commissionario e qualsiasi persona che per conto del Commissionario abbia accesso a dati personali può trattare tali dati esclusivamente in base alle istruzioni fornite e ai poteri conferiti contrattualmente dal Contraente, a meno che il trattamento non sia obbligatorio per legge.
b) L'implementazione e l'osservanza delle misure tecnico-organizzative richieste per il presente Ordine con quanto disposto dall'articoli 28 (3) punto 2 lett. c, e 32 GDPR [dettagli in **Allegato 1**].
c) Il Contraente e il Commissionario devono, su richiesta, cooperare con l'autorità di controllo nell'espletamento dei loro compiti.
d) Informazioni tempestive al Contraente sulle azioni di controllo e sulle misure intraprese dall'autorità di controllo relativamente al presente Ordine. Questo anche nel caso un'autorità competente stia investigando nel contesto di procedure amministrative, civili o penali, afferenti il trattamento di dati personali durante l'esecuzione dell'ordine da parte del Commissionario.

e) Qualora il Contraente fosse soggetto ad attività ispettiva da parte dell'autorità di controllo, o si trovasse coinvolto in una procedura amministrativa, civile o penale, o in un'azione di responsabilità promossa da persona interessata o da un soggetto terzo, o qualsiasi altra contestazione connessa all'esecuzione dell'Ordine del Commissionario, il Commissionario deve intervenire in ciascun caso in suo sostegno.
f) Il Commissionario deve regolarmente monitorare i processi interni e le misure tecnico-organizzative al fine di garantire che il trattamento, per quanto riguarda la sua area di responsabilità, sia espletato nel rispetto dei requisiti normativi sulla protezione dei dati e che i diritti dei soggetti a cui i dati fanno riferimento siano protetti.
g) Verificabilità delle misure tecnico-organizzative intraprese nei confronti del Contraente nell'ambito dei poteri di controllo di cui al punto 7 del presente Ordine.

(2) In aderenza al disposto dell'art. 30 (2) GDPR il Commissionario predispone e mantiene un registro – anche in forma elettronica – nel quale sono riportate le categorie di attività afferenti il trattamento svolto per conto del Contraente, i nomi e i referenti del Commissionario, il nominativo del *Data Protection Officier*, qualora nominato, e - laddove possibile -, una descrizione delle misure tecnico-organizzative adottate.

L'indirizzo Email responsabileprotezionedati@ista-italia.it è a disposizione quel qualsiasi informazione e chiarimento relativamente all'applicazione delle disposizioni GDPR.

6. Relazioni con i sub-commissionari

(1) Le relazioni di sub-commissione nel contesto della presente regolamentazione devono essere intese come estensione delle disposizioni applicabili al servizio principale. Non sono ricompresi i servizi ausiliari che il Commissionario dovesse utilizzare, quali, ad esempio, i servizi di telecomunicazione, servizi postale e di trasporto, i servizi di manutenzione e assistenza agli utenti o la eliminazione dei supporti dati così come altre misure volte a garantire la riservatezza, la disponibilità, l'integrità, e la resilienza dell'hardware e del software necessari al trattamento dei dati. Tuttavia, al fine di garantire la protezione e la sicurezza dei dati del Contraente, il Commissionario è obbligato a porre in essere accordi contrattuali e misure di controllo appropriati e giuridicamente conformi, anche nel caso di servizi ausiliari esternalizzati.

(2) Il Commissionario può utilizzare terzi sub-commissionari dietro consenso scritto qui genericamente prestato. Il Commissionario deve informare il Contraente dell'intenzione di apportare modifiche afferenti il coinvolgimento o la sostituzione di altri commissionari rendendo disponibile un attuale elenco di sub-commissionari. Il Contraente potrà in ogni tempo conoscere lo stato corrente dei sub-commissionari accedendo all'elenco almeno una volta al mese (es.: tramite adeguate precauzioni tecniche).

(3) Il trasferimento dei dati personali del Contraente al sub-commissionario e la sua prima attività sono consentiti solo nel caso tutti i requisiti per la sub-commissione siano rispettati.

(4) Nel caso in cui il sub-commissionario esegua i servizi contrattualizzati al di fuori dell'Unione Europea o dell'Area Economica Europea, il Commissionario deve adottare adeguate misure per garantire il rispetto della normativa per la protezione dei dati. Lo stesso principio si applica nel caso debbano essere impiegati prestatori di servizi di cui al paragrafo 1, secondo capoverso.

(5) Ulteriori azioni di esternalizzazione effettuate dal sub-commissionario richiedono il consenso espresso del Contraente principale (almeno con e-mail); qualsiasi obbligazione circa la protezione dei dati assunta dal Commissionario in base al presente accordo – ed estesa ai sub-commissionari – deve essere imposta anche agli ulteriori sub-commissionari.

7. Diritto al controllo da parte del Contraente

(1) Il Contraente ha il diritto di constatare, a mezzo di ispezioni a campione da preannunciare con un preavviso minimo di due settimane, l'osservanza del presente accordo da parte del Commissionario. Il personale impiegato a tal fine dal Contraente dovrà

obbligarsi verso il Commissionario alla riservatezza. L'obbligo di riservatezza deve soddisfare alti requisiti di sicurezza. Il personale impiegato non può avere rapporti con i concorrenti del Commissionario.

(2) Il Commissionario assicura che il Contraente può verificare l'osservanza da parte del Commissionario agli obblighi derivanti dall'Articolo 28 GDPR. Il Commissionario si impegna a mettere a disposizione, su richiesta del Contraente, le informazioni necessarie e in particolare fornire prova dell'implementazione delle misure tecnico-organizzative.

(3) La dimostrazione delle predette misure, incluse quelle che non riguardano specificamente l'Ordine, può essere fatta tramite certificazioni, reportistica o estratti della reportistica di enti indipendenti (es.: auditor, audit, Incaricato di tutela dati, dipartimento di sicurezza informatica, auditor preposti alla sicurezza dei dati, auditor preposti alla qualità) o adeguata certificazione da parte della sicurezza informatica o audit protezione dati.

8. Compenso

Il compenso concordato nel contratto di servizio riguarda la fornitura di servizi standard che devono essere forniti a tutti i clienti in egual misura. Sulla base del presente Ordine, potrebbe rendersi necessaria la fornitura di servizi aggiuntivi di protezione dati la cui tipologia o ampiezza dipende strettamente dal rapporto con il singolo Contraente (es.: per audit, supporto nel caso di investigazione da parte dell'autorità di controllo). Tali servizi aggiuntivi dovranno essere remunerati in aggiunta al compenso dovuto per i servizi non connessi alla protezione dei dati così come specificati nel contratto di servizio, in relazione anche al volume di lavoro eseguito. Il compenso per dette prestazioni sarà calcolato applicando i relativi prezzi ordinari.

9. Notifiche in caso di violazioni da parte del Commissionario

Il Commissionario deve sostenere il Contraente nel rispetto degli obblighi previsti dagli artt. da 32 a 36 GDPR riguardo la sicurezza dei dati personali, con obbligo di informativa a seguito di sottrazione di dati, di valutazione dell'impatto e consultazione preliminare. Ciò include, tra le altre cose:

a) La garanzia di un adeguato livello di protezione attraverso misure tecnico – organizzative che tengano conto delle circostanze e degli scopi del trattamento, così come la previsione della probabilità e della gravità di una possibile infrazione dei diritti dovuta a falle nel sistema di sicurezza, e rendere possibile una determinazione immediata dei rilevanti eventi di infrazione.
b) L'obbligo di riportare senza ritardo al Contraente violazioni dei dati personali.
c) L'obbligo di sostenere il Contraente nel contesto del suo obbligo di informare le persone interessate e render loro disponibili senza ritardo tutte le informazioni rilevanti al riguardo.
d) Sostenere il Contraente nella propria valutazione dell'impatto afferente la protezione dei dati
e) Sostenere il Contraente nel quadro delle consultazioni preliminari con l'autorità di controllo.

10. Poteri direttivi del Contraente

(1) Le istruzioni verbali vanno confermate dal Commissionario senza ritardo per iscritto (almeno via e-mail).

(2) Il Commissionario deve informare senza ritardo il Contraente se ritiene che un'istruzione violi le disposizioni sulla protezione dei dati. Il Commissionario è autorizzato a sospendere l'esecuzione delle corrispondenti istruzioni fino a conferma o modifica da parte del Contraente.

(3) A richiesta del Contraente, il Commissionario deve mettere a disposizione dell'autorità di controllo il registro delle attività di trattamento di cui al precedente punto 5 (2) del presente Ordine.

11. Cancellazione e restituzione dei dati personali

(1) Copie o duplicati dei dati non possono essere create senza che il Contraente ne sia informato. La

disposizione non riguarda le copie necessarie all'esecuzione dell'Ordine e per garantire un'ordinata elaborazione dei dati, così come per le copie da effettuare per l'archiviazione dei dati in osservanza di uno specifico obbligo di legge.

(2) Dopo la conclusione dei lavori contrattualmente concordati, o anche prima su richiesta del Contraente - al più tardi alla cessazione del contratto di servizio - il Commissionario deve consegnare tutti i documenti in suo possesso al Contraente, le elaborazioni e i risultati generati, nonché i salvataggi dei dati relativi al rapporto contrattuale, o distruggerli secondo il regolamento di protezione dei dati previo consenso del Contraente. Lo stesso si applica ai test e al materiale di scarto. A richiesta, il protocollo di cancellazione va consegnato.

(3) Sono esclusi dall'obbligo di cancellazione e restituzione i dati per i quali è previsto, per disposizione di legge, un obbligo di archiviazione (per es.: la documentazione a riprova del corretto trattamento dei dati va custodita dal Commissionario nel rispetto dei termini di conservazione anche oltre la scadenza del contratto).

Allegato 1 –
Misure tecnico-organizzative

1. Riservatezza (Articolo 32(1) lett. b GDPR)

- Controllo degli accessi
  - Nessun accesso a persone non autorizzate al sistema di trattamento dei dati del centro dati e dei server periferici
  - Controllo identificativo degli accessi alle aree sensibili dei centri dati
  - Accesso agli uffici controllato da dipendenti durante l'orario di lavoro; i visitatori degli uffici centrali sono identificati e sono accompagnati
  - Elenchi delle persone autorizzate ad accedere alle aree sensibili dei centri dati
  - Elenco delle chiavi per gli uffici centrali
  - Misure di protezione antiscasso (video sorveglianza, bloccaggio porte, sistema di allarme collegato a un servizio di sicurezza)
  - Regolamento per persone esterne (pass visitatori, v. sopra)
  - Registrazione dei visitatori agli uffici centrali e periferici

- Controllo degli ingressi
  - Nessun accesso a persone non autorizzate al sistema di trattamento dei dati del centro dati e dei server periferici
  - Controllo identificativo degli accessi alle aree sensibili dei centri dati
  - Accesso agli uffici controllato da dipendenti durante l'orario di lavoro; i visitatori degli uffici centrali sono identificati e sono accompagnati
  - Elenchi delle persone autorizzate ad accedere alle aree sensibili dei centri dati
  - Elenco delle chiavi per gli uffici
  - Misure di protezione antiscasso (video sorveglianza, bloccaggio porte, sistema di allarme collegato a un servizio di sicurezza)
  - Regolamento per persone esterne (pass visitatori, v. sopra)
  - Registrazione dei visitatori agli uffici centrali e periferici

- Controllo delle acquisizioni
  - Le persone autorizzate possono acquisire solamente i dati la cui acquisizione è stata loro autorizzata
  - I dati personali archiviati possono essere letti, copiati, modificati o rimossi solo nel contesto strutturale del principio delle autorizzazioni
  - Un sistema di autorizzazioni a più livelli sulla base della funzione ricoperta da ciascuna persona preposta all'evasione dell'ordine
  - Utilizzo di un software di protezione contro i virus permanentemente aggiornato
  - Protezione del traffico e-mail da virus e spam (protezione anti-virus centralizzata e sistema di filtraggio spam)
  - Un sistema firewall
  - Password di protezione (combinazione di almeno 8 tra lettere, numeri, caratteri speciali, da cambiare obbligatoriamente

ogni 90 giorni)
- Separazione tra i dati di contabili e anagrafici attraverso differenti diritti di acquisizione
- Registrazione in caso di modifica dei dati

- Controlli di separazione
- Utilizzo di software testati
- Separazione degli ambienti di produzione da quelli di test e sviluppo
- Separazione logica in aderenza al meccanismo di controllo delle acquisizioni
- Procedure di rilascio differenziate (gestione del cambiamento)

2. Integrità (Articolo 32(1) lett. b GDPR)

- Controllo del trasferimento
  - Criptazione/utilizzo di tunnel VPN per le trasmissioni,
  - Criptazione SSL per gli accessi web
  - Regolamentazione del sistema del traffico delle informazioni (sistemi centralizzati di firewall, connessioni WAN dedicate con controlli di accesso), registrazione (autenticazione dell'utente, orario)

- Controllo dell'inserimento
  - Può essere accertato successivamente se e da chi sono stati inseriti, modificati o rimossi dati anagrafici dei clienti nei sistemi di elaborazione (identificazione),
  - Principio delle autorizzazioni.

3. Disponibilità e resilienza (Articolo 32(1) lett. b, c GDPR)

- Controllo della disponibilità
  - I dati personali sono costantemente disponibili e protetti contro l'accidentale distruzione o perdita attraverso un back-up permanente,
  - Principio della messa in sicurezza dei dati (back-up regolari: giornalieri, settimanali, mensili), modalità di conservazione dei back-up (cassaforte, separati compartimenti ignifughi)
  - Sezioni del centro dati protette in modo particolare (separazione strutturale, sistema di controllo degli accessi separati, pareti tagliafuoco per tutte le aree del cento dati, alimentazione elettrica via due connessioni geograficamente separate, UPS ridondante, due distinti sistemi di protezione antiincendio collegati al centro di controllo dei vigili del fuoco),
  - Sistemi di protezione antiincendio nell'ufficio centrale e in quelli periferici,
  - Fornitura di energia elettrica non interrompibile,
  - Fonti di energia elettrica ridondanti,
  - Sistemi di monitoraggio e controllo.

4. Procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. (Articolo 32(1)(d) GDPR, Articolo 25(1) GDPR)

- Principio della protezione e della sicurezza dei dati,
- Gestione delle emergenze,
- Predisposizione predefinita di un sistema di protezione dei dati (Articolo 25(2) GDPR),
- Controllo dell'Ordine
  - Trattamento solo secondo le istruzioni documentate del Contraente,
  - Istruzioni fornite solo da referenti espressamente designati,
  - Dettagli specifici per l'imballaggio e la spedizione dei documenti/oggetti che contengano dati rilevanti,
  - Le persone impiegate sono informate circa i requisiti di protezione dei dati e sono vincolati per iscritto alla riservatezza sui dati ai sensi dell'art. 5 GDPR,
  - I sub-commissionari vengono attentamente esaminati con riferimento alla di loro adeguatezza circa l'osservanza delle precauzioni rilevanti sulla sicurezza e vincolati per iscritto all'osservanza della regolamentazione applicabile alla protezione dei dati.