ADDENDUM AL CONTRATTO DI SERVIZIO "Whistleblowing Intelligente"
Nomina del Responsabile per il Trattamento dei Dati Personali

Tra

Tecnolink S.r.l., fornitrice del servizio "Whistleblowing Intelligente" (di seguito denominato Servizio), con sede legale Via P. Bagetti, 10 – 10143 – Torino (TO), C.F. e P.IVA 07504810016, in persona del legale rappresentante pro tempore (di seguito denominato "Fornitore"),

e

l'Ente che ha manifestato con proprio atto formale la volontà di acquisire il Servizio ed ivi meglio specificato,Santa Marinella Servizi Srl, con sede legale Via Aurelia, n 455, - 00058 Santa Marinella (Rm) C.F. e P.IVA 0898327100, in persona del legale rappresentante pro tempore (di seguito denominato "Committente").

denominati di seguito singolarmente "Parte" e congiuntamente "Parti".

PREMESSE

i. Il presente Accordo si prefigge di definire gli obblighi delle Parti in relazione alla protezione dei dati personali, in conformità a quanto prescritto dall'art. 28 del Regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito anche "GDPR").

ii. Ai fini del presente Accordo, come "Normativa Rilevante" si intende il GDPR e qualsiasi provvedimento normativo e/o regolamentare adottato da autorità pubbliche nazionali in materia di trattamento di dati personali (ivi compresi i provvedimenti assunti dalle Autorità di controllo), applicabile durante il periodo di validità del presente Accordo, cui si fa riferimento anche per le definizioni di "trattamento di dati" e "dato personale".

iii. Il presente Accordo è espressamente collegato, e si allega integrandolo all'accettazione della proposta tecnico/commerciale presentata dal Fornitore.

iv. Per ogni aspetto non espressamente disciplinato dal presente Accordo, si rinvia alla proposta tecnico/commerciale del Fornitore, alla determinazione di affidamento del servizio o ordine di acquisto del Committente e alla Normativa Rilevante.

v. In caso di contrasto tra le disposizioni contenute nella proposta tecnico/commerciale del Fornitore e/o della determinazione di affidamento/ordine di acquisto del Servizio del Committente e quelle contenute nel presente Accordo, prevarranno queste ultime.

vi. Il Committente ritenuto che il Fornitore presenti garanzie sufficienti, in particolare in merito a conoscenze specialistiche, risorse, affidabilità e abbia adottato misure tecniche ed organizzative che soddisfano i requisiti della Normativa Rilevante per il trattamento dei dati personali, nomina il Fornitore Responsabile del Trattamento relativamente a quelle attività di

trattamento connesse all'affidamento del Servizio.

1. OGGETTO DELL'ACCORDO

1.1. Le premesse e gli allegati sono parte integrante e sostanziale dell'Accordo.

1.2. Il Committente, con il presente Accordo, ai sensi e per gli effetti dell'art. 28 GDPR, nomina il Fornitore Responsabile del trattamento dei dati personali.

1.3. Il Fornitore accetta la nomina e si impegna a rispettare le prescrizioni della Normativa Rilevante e ad adempiere a tutte le clausole del presente Accordo, ivi inclusi i suoi allegati.

1.4. Qualora il Committente sia a sua volta "Responsabile del trattamento", col presente Accordo il Fornitore si intenderà nominato come "altro responsabile del trattamento" ai sensi dell'art. 28 GDPR, cd. "Sub - responsabile".

1.5. In questo caso, Le Parti riconoscono e si danno atto che ai sensi dell'art. 28 GDPR, il presente Accordo sarà valido ed efficace fintanto che il Committente sia legittimato a nominare il Fornitore quale "altro responsabile del trattamento" e salvo eventuali opposizioni alla presente nomina.

1.6. La definizione della natura e della finalità dei trattamenti affidati nonché la tipologia di dati personali e le categorie di interessati cui i dati oggetto dell'Accordo si riferiscono, sono decisi dal Committente e indicati nell'Allegato 1.

2. DIRITTI E OBBLIGHI DEL COMMITTENTE

2.1. Diritti e Obblighi generali

2.1.1. Il Committente determina le finalità e le modalità del trattamento dei dati personali eseguiti dal Fornitore nello svolgimento del Servizio.

2.1.2. Il Committente dovrà far presente eventuali esigenze contrattuali specifiche inerenti il trattamento dei dati personali in sede di trattativa. Il Fornitore, per eseguire il presente Accordo, si atterrà a quanto previsto nella determinazione di affidamento/ordine di acquisto del Servizio e alle istruzioni – specifiche per il trattamento di dati personali - indicate nell'Allegato 1. Non saranno prese in considerazione istruzioni non fornite per iscritto.

2.1.3. Eventuali istruzioni non inserite nell'Allegato 1 potranno essere oggetto di rinegoziazione tra le parti

2.1.4. Il Committente dichiara e garantisce che i dati personali affidati al Fornitore in esecuzione del presente Accordo, sono stati raccolti e trattati dal Committente in conformità alla Normativa Rilevante.

2.1.5. Il Committente garantisce altresì di essere legittimato, in base alla Normativa Rilevante, a sottoscrivere il presente accordo (in qualità di autonomo Titolare, Contitolare o – a sua volta – di Responsabile).

2.1.6. Il Committente ha diritto di verificare che il Fornitore adempia alle istruzioni impartite e rispetti la Normativa Rilevante ad esempio verificando i) le misure di sicurezza adottate, ii) il corretto svolgimento delle operazioni di trattamento, in applicazione delle istruzioni di cui al presente Accordo iii) il rispetto delle finalità individuate e perseguite dal Committente.

2.1.7. Le verifiche di cui al successivo punto 2.2 potranno essere eseguite nella sede del Fornitore ovvero dove quest'ultimo tratta i dati personali, anche per mezzo di professionisti o soggetti terzi, concordando con il Fornitore una data che non interrompa o rechi pregiudizio alla attività lavorativa di quest'ultimo secondo le modalità del punto 2.2.

2.1.8. Il Committente è tenuto ad informare tempestivamente il Fornitore di eventuali utilizzi impropri degli account o delle credenziali di autenticazione nonché ogni eventuale incidente di sicurezza di cui abbia cognizione e che riguardi i dati oggetto del presente Accordo o i sistemi informatici utilizzati per darvi esecuzione.

2.2. Diritti e obblighi del committente – ispezioni e verifiche

2.2.1. Eventuali ispezioni o verifiche svolte dal Committente, anche per mezzo di terzi professionisti da Lui nominati, non dovranno in alcun modo recare pregiudizio all'attività del Fornitore.

2.2.2. Il Committente, eventuali Suoi collaboratori o professionisti terzi da Lui incaricati dovranno trattare ogni informazione o dato conosciuto in ragione delle ispezioni e delle verifiche condotte in esecuzione del presente Accordo, come strettamente confidenziale.

2.2.3. Le Parti concorderanno con congruo anticipo le date, le modalità, l'oggetto dell'ispezione affinché lo svolgimento delle attività avvenga nel pieno rispetto delle norme sulla sicurezza, in conformità alle procedure e alle misure di sicurezza del Fornitore e dei suoi sub-responsabili.

2.2.4. Qualora l'ispezione comporti costi o pregiudizi non previsti dalle Parti che rendano la prestazione troppo onerosa per il Fornitore, le Parti concorderanno un equo compenso.

3. OBBLIGHI DEL FORNITORE

3.1. Obblighi generali

3.1.1. Il Fornitore tratta, per conto del Committente, i dati personali in esecuzione della determinazione di affidamento del Servizio/Ordine di acquisto ed esclusivamente nel quadro del presente Accordo, salvo quanto diversamente previsto dal diritto dell'Unione Europea o di uno Stato membro a cui il Fornitore è soggetto.

3.1.2. I dati forniti non vengono usati per nessun'altra finalità, in particolare non vengono usati dal Fornitore per proprie finalità non previste dall'Allegato 1. Fermo quanto previsto al punto 3.4, il Fornitore può comunicare i dati a terze parti, che svolgono servizi strumentali, qualora sia necessario per dare esecuzione alla determinazione di affidamento/ordine di acquisto del Servizio. Il Fornitore non è autorizzato a fornire i dati a terze parti, diverse da quelle suddette, senza la preventiva approvazione scritta del Committente.

3.1.3. Qualunque trasferimento di dati personali oggetto del presente Accordo verso un Paese o una organizzazione internazionale può avere luogo soltanto se avviene nel pieno rispetto delle garanzie di cui al Capo V del Regolamento Europeo GDPR n. 2016/679 e della Normativa Rilevante. Eventuali trasferimenti non eseguiti nel rispetto delle garanzie suddette dovranno essere autorizzati dal Committente.

3.1.4. Il Fornitore fornisce al Committente tutta l'assistenza necessaria e richiesta da quest'ultimo nell'assicurare il rispetto degli obblighi di cui agli articoli 32 "Sicurezza del Trattamento", 33 "Notifica di una violazione dei dati personali all'autorità di controllo", 34 "Comunicazione di una violazione dei dati personali all'interessato", 35 "Valutazione d'impatto sulla protezione dei dati" e 36 "Consultazione Preventiva" del GDPR.

3.1.5. Il Fornitore mette a disposizione del Committente le informazioni necessarie a dimostrare il rispetto degli obblighi e delle prescrizioni della Normativa Rilevante e collabora con il Committente in caso di ispezioni o controlli di ogni genere da parte delle Autorità o in caso di controversie con l'Interessato.

3.1.6. Il Fornitore coadiuva il Committente nel riscontrare le eventuali richieste degli interessati avanzate al fine di esercitare i diritti dell'interessato definiti al Capo III del GDPR, secondo le modalità previste dal presente Accordo e le eventuali istruzioni aggiuntive impartite dal Committente per specifiche esigenze.

3.1.7. Il Fornitore deve designare le persone autorizzate al trattamento di dati personali, garantendo che queste abbiano la necessaria competenza e formazione in relazione alle attività di trattamento di dati personali da porre in essere, provvedendo altresì a vincolarle a idonei impegni di riservatezza circa i dati personali trattati e le relative informazioni di cui vengano a conoscenza in esecuzione delle attività.

3.1.8. Il Fornitore informa il Committente se nota che un'istruzione impartita dal Committente viola un obbligo legale prescritto dalla Normativa Rilevante o qualsiasi altro obbligo derivante dal presente Accordo. Il Fornitore è autorizzato a sospendere l'esecuzione di tale istruzione od obbligo fino a quando non viene confermata o corretta dal Committente.

3.1.9. Qualora il Committente, nonostante la segnalazione di cui al punto 3.1.8 decida di confermare l'istruzione impartita al Fornitore, si assume la totale responsabilità della decisione intrapresa e si obbliga a tenere indenne il Fornitore di ogni pretesa, danno, pregiudizio o onere trovi causa in tale istruzione.

3.2. Obblighi del fornitore - Misure tecniche e organizzative

3.2.1. Il Fornitore adotta le misure richieste ai sensi dell'art. 32 GDPR ed in particolare, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, si impegna a mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio

3.2.2. Resta in ogni caso fermo quanto previsto ai punti 2.1.2 e 2.1.3 in merito ad eventuali istruzioni aggiuntive del Committente.

3.3. Obblighi del fornitore – Rapporti con i terzi

3.3.1. Qualora gli interessati, le Autorità di controllo o qualsiasi altro terzo (ivi compresi, a titolo esemplificativo e non esaustivo, Autorità giurisdizionali e amministrative diverse dalle Autorità di controllo) avanzassero richieste nei confronti del Fornitore (ivi comprese anche richieste per l'esercizio dei diritti riconosciuti agli interessati, quali il diritto di accesso e gli altri diritti riconosciuti dal GDPR), questo informerà senza ritardo per iscritto il Committente.

3.3.2. Il Fornitore avrà cura, in particolare, di trasmettere al Committente copia delle richieste pervenute, allegando altresì ogni ulteriore eventuale informazione o circostanza ritenuta ut

3.3.3. Il Fornitore non darà riscontro a richieste di terzi senza averne preventivamente informato il Committente fatta eccezione nei casi in cui sia tenuto per legge a fornire immediato riscontro nonché qualora la richiesta dovesse pervenire da Autorità di Pubblica Sicurezza o Autorità di Controllo.

3.3.4. Nei casi di cui al punto 3.3.2 il Fornitore si impegna a porre in essere ogni accorgimento volto a limitare o restringere la divulgazione dei dati.

3.4. Obblighi del Fornitore - Rapporti di Sub-responsabilità

3.4.1. Il Committente autorizza in via generale il Fornitore a ricorrere ad un altro Responsabile del trattamento (d'ora in poi anche solo Sub-responsabile) ai sensi e per gli effetti dell'art. 28 del GDPR esclusivamente per lo svolgimento di specifiche attività di trattamento di dati personali necessarie all'esecuzione della determinazione di affidamento/ordine di acquisto del Servizio. Resta in ogni caso salvo il diritto del Committente di opporsi alle specifiche nomine nei termini di seguito indicati.

3.4.2. Il Fornitore alla sottoscrizione del presente documento informa il Committente dei Sub-Responsabili di cui attualmente si avvale per svolgere attività necessarie o strumentali per eseguire il Servizio, e che il Committente, con la sottoscrizione del presente Accordo, approva. Il Fornitore deve informare il Committente di eventuali modifiche riguardanti l'aggiunta e/o la sostituzione di altri Sub - Responsabili del trattamento almeno 15 (quindici) giorni prima di operare le predette modifiche, dando così al Committente l'opportunità di opporsi.

3.4.3. L'eventuale opposizione dovrà essere adeguatamente motivata e comunicata per iscritto entro 15 (quindici) giorni dalla comunicazione all'indirizzo indicato in calce all'Accordo come persona di contatto.

3.4.4. In caso di opposizione, le Parti si attiveranno per trovare, di comune accordo, una soluzione alternativa. Qualora non si addivenisse ad un accordo sul punto e, nonostante l'opposizione manifestata dal Committente, il Fornitore confermi la variazione di cui al punto 3.4.2, il Committente avrà diritto di recedere dal presente Accordo e richiedere l'interruzione del Servizio, fermo restando l'obbligo di corrispondere al Fornitore gli importi dovuti fino alla data di cessazione del Servizio stesso.

3.4.5. Qualora il Fornitore ricorra, sotto la propria responsabilità, alla nomina di un Sub-responsabile, il Fornitore deve prevedere nel contratto con il nuovo Sub-Responsabile garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR

3.4.6. La comunicazione di cui al punto 3.4.1 potrà essere eseguita dal Fornitore con i mezzi ritenuti più opportuni, incluso l'invio a mezzo posta elettronica.

3.5. Obblighi del fornitore - Notifica delle violazioni da parte del Fornitore (c.d. data breach)

3.5.1. Qualora si verifichi un incidente di sicurezza (a titolo esemplificativo e non esaustivo, qualsiasi evento di distruzione, perdita, alterazione, divulgazione o accesso imprevisto o non autorizzato ai dati personali), riguardante i propri sistemi o quelli dei Sub-Responsabili, il Fornitore dovrà notificare al Committente per iscritto mediante posta elettronica certificata (PEC) tale evento nel minor tempo possibile, dal momento in cui ne sia venuto a conoscenza e comunque senza ingiustificato ritardo.

3.5.2. La comunicazione sarà ritenuta correttamente eseguita qualora contenga:
a) la descrizione nel dettaglio della natura della violazione dei dati personali, ivi compresi, ove possibile, le categorie, il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di dati personali coinvolti;
b) il nominativo e i dati di contatto dell'eventuale responsabile della protezione dei dati o altro punto di contatto ove sia possibile ottenere maggiori informazioni;
c) descrizione delle probabili conseguenze della violazione dei dati personali;
d) descrizione delle misure adottate per far fronte alla violazione e le misure di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

3.5.3. Il Fornitore presterà assistenza e la collaborazione eventualmente richiesta dal Committente al fine di porre rimedio alla violazione di dati personali e al fine di fornire all'Autorità di controllo ogni informazione o chiarimento richiesto.

3.5.4. Resta inteso fra le parti che l'onere di comunicare la violazione all'Autorità garante per i trattamenti di cui al presente Accordo è del Committente.

4. RISERVATEZZA

4.1. Tutti i dati personali ricevuti dal Fornitore da parte del Committente e/o raccolti dal Fornitore nell'ambito dell'esecuzione di questo Accordo, sono soggetti all'obbligo di riservatezza nei confronti di terzi.

4.2. Tale obbligo di riservatezza non sussisterà nel caso in cui il Committente abbia espressamente autorizzato la rivelazione di tali informazioni a terzi, nel caso in cui la rivelazione delle informazioni a terzi sia ragionevolmente necessaria alla luce delle disposizioni e dell'esecuzione del presente Accordo, oppure ove ricorra un obbligo giuridico di rendere disponibili le informazioni a terzi.

5. DURATA

5.1. Il presente Accordo decorre dalla data di sottoscrizione e rimarrà in vigore ed efficace fino al termine o alla cessazione (per qualsivoglia ragione) del Servizio o di eventuali altri accordi vigenti tra le Parti e aventi il medesimo oggetto. Qualora al termine del Servizio vi siano trattamenti o attività ancora in corso, il Fornitore, d'accordo con il Committente, può portarli a termine rimanendo obbligato, per tali attività ad ogni istruzione o obbligo derivante dal presente Accordo.

5.2. Al termine del Contratto di Servizio i dati trattati, in esecuzione del presente Accordo, saranno a disposizione del Committente nei 30 (trenta) giorni successivi alla cessazione del Contratto.

5.3. Trascorso tale termine, compatibilmente con i sistemi di business continuity e disaster recovery del Fornitore, i dati verranno cancellati, salvo che la conservazione non sia richiesta da specifici obblighi di legge.

6. RESPONSABILITÀ E MANLEVE

6.1 Il Committente manleverà e terrà indenne il Fornitore da ogni perdita, costo, spesa, sanzione pecuniaria, danno da risarcire e in generale da ogni responsabilità direttamente o indirettamente derivante dalla esecuzione da parte del Fornitore delle disposizioni del presente Accordo con riferimento alle attività di trattamento di dati personali svolte per conto del Committente sotto sua istruzione. Il Fornitore risponderà nei confronti di Terzi e del Committente di eventuali danni che trovino causa nel mancato rispetto delle istruzioni del Titolare o della Normativa Rilevante.

6.2 Il Fornitore sarà manlevato e tenuto indenne da ogni perdita, costo, spesa, sanzione pecuniaria danno da risarcire, pregiudizio che sia derivato o abbia trovato causa nella violazione da parte del Committente di una delle clausole del presente Accordo. In particolare, qualora il Committente raccolga o tratti dati personali oggetto del presente Accordo in violazione della Normativa Rilevante e dei punti 2.1.4 e 2.1.5 del presente Accordo terrà indenne il Fornitore da qualsivoglia responsabilità, danno, onere, pretesa e pregiudizio che trovi causa in suddetta violazione.

7. DISPOSIZIONI FINALI

7.1 L'Accordo annulla e sostituisce ogni precedente Accordo o intesa tra le Parti in relazione al trattamento di dati personali svolti dal Fornitore per conto del Committente.

7.2 Le Parti dichiarano che tutte le clausole contenute nel presente Accordo sono state oggetto di attenta e singola valutazione e riflettono la comune volontà delle Parti.

7.3 Qualora una qualsiasi clausola del presente Accordo venisse dichiarata invalida, tale dichiarazione non inficerà la validità di tutte le altre clausole ivi contenute. In tale eventualità e per quanto possibile, tale clausola invalida dovrà venire sostituita da un'altra il cui effetto sia il più possibile equivalente a ciò che le Parti intendevano al momento della stipula dell'Accordo.

7.4 Se una parte è obbligata dalla legge a nominare un responsabile della protezione dei dati, deve nominarlo e fornire i relativi dati di contatto alla controparte. Se una parte non è soggetta all'obbligo giuridico di nominare un responsabile della protezione dei dati, nomina la seguente persona come persona di contatto in materia di protezione dei dati (ai fini del presente accordo):

	NOMINATIVO DPO/PERSONA DESIGNATA	INDIRIZZO EMAIL DPO/PERSONA DESIGNATA	TELEFONO DPO/PERSONA DESIGNATA
CLIENTE			
FORNITORE	Antonio Cappiello	acappiello@e-tecnolink.it	3486531590

7.5 Le parti si impegnano a comunicarsi reciprocamente eventuali variazioni intervenute nei suddetti dati di contatto.

8 ALLEGATI
Allegato 1: Dettaglio Servizi
Allegato 2: Elenco Sub-responsabili
Allegato 3: Misure di Sicurezza

Per accettazione

Il Committente	Il Fornitore
Per la Santa Marinella Servizi Srl *Il Presidente del C.d.A.* Fabio Iachini *Firma*	Per Tecnolink S.r.l. *Il legale rappresentante* Antonio Cappiello *Firma*
Luogo e data	Luogo e data

Si approvano specificatamente, ai sensi degli artt. 1341 e 1342 c.c., le seguenti clausole dell'Accordo: art. 2.1 Diritti e Obblighi del Committente - Diritti ed Obblighi generali art. 2.2. Diritti e obblighi del Committente – Ispezioni e Verifiche, art. 3.1.7 Obblighi del Fornitore (nomina autorizzati al trattamento), 3.1.9 Obblighi del Fornitore (esonero di responsabilità in caso di istruzioni che violino la Normativa Rilevante), art. 3.4 Obblighi del Fornitore – Rapporti di sub-responsabilità, art. 5 Durata dell'Accordo, art. art. 6 "Responsabilità e Manleve".

Il Committente	Il Fornitore
Per la Santa Marinella Servizi Srl *Il Presidente del C.d.A.* Fabio Iachini *<Firma>*	Per Tecnolink S.r.l. *Il legale rappresentante* Antonio Cappiello *<Firma>*
Luogo e data	Luogo e data

Allegato 1 - Servizio di gestione del sistema Whistleblowing Intelligente

Lo scopo del trattamento

i dati personali sono acquisiti dal Responsabile del trattamento nell'esclusivo e unico scopo di rendere operativa la piattaforma "Whistleblowing Intelligente" nell'ambito dell'esecuzione dell'affidamento ricevuto

Natura del trattamento

La piattaforma opera come servizio in cloud (Software as a Service) e il trattamento avviene con mezzi informatici.
I dati personali sono trattati con strumenti automatizzati per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti.

Categorie di interessati

I dati personali a cui è riferito il trattamento possono essere riferiti alle seguenti categorie di interessati in relazione al Committente:

- Dipendenti o ex dipendenti
- Lavoratori autonomi Consulenti e collaboratori a qualunque titolo
- Dipendenti e collaboratori di imprese fornitrici di beni, lavori o servizi nel caso in cui la segnalazione riguardi fatti in cui è coinvolto o che riguardino il Committente
- Volontari e tirocinanti, retribuiti o non retribuiti
- Le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto.
- Candidati a ricoprire una posizione lavorativa in qualunque forma e a qualsiasi titolo, anche non retribuita

Tipologia di dati trattati

- dati personali del segnalante (nome, cognome, data e luogo di nascita, codice fiscale, indirizzo di posta elettronica, datore di lavoro e ruolo lavorativo)
- dati personali forniti volontariamente dal segnalante
- non è esclusa la possibilità che il segnalante fornisca informazioni rientranti nelle categorie particolari di dati personali delle persone segnalate, o a condanne penali e ai reati
- dati di navigazione: indirizzo IP e dati di LOG unicamente riferiti alle attività del Responsabile

del trattamento delle segnalazioni e suoi collaboratori designati e dotati di credenziali sulla piattaforma Whistleblowing Intelligente.

ALLEGATO 2 – ELENCO DEI SUB-RESPONSABILI

Tecnolink S.r.l. fornisce la soluzione "Whistleblowing Intelligente" in modalità Cloud tramite il subfornitore

Interzen Consulting s.r.l., con sede in Pescara, Strada Comunale Piana 3, cap. 65129 (P. IVA e C.F. 01446720680)

già nominato da Tecnolink con atto formale Responsabile di tutti i trattamento dei dati inerenti il servizio Whistleblowing Intelligente.

A sua volta, Interzen Consulting s.r.l. si avvale dei servizi del cloud Azure di Microsoft ubicato in un Data Center europeo.

ALLEGATO 3 – MISURE TECNICHE E ORGANIZZATIVE

Il Fornitore, congiuntamente ai sub-responsabili;

- tratta i dati personali nel rispetto dei princìpi e delle disposizioni previsti dal Codice, dal Regolamento, dagli indirizzi e dai provvedimenti a carattere generale emanati dal Garante in materia di protezione dei dati personali e da ogni altra vigente normativa in materia di protezione dei dati personali
- implementa, mantiene ed aggiorna, come previsto dall'art. 32 del Regolamento, le misure tecniche e organizzative (TOM) per garantire il livello di sicurezza adeguato al rischio connesso all'attività. Le TOM sono soggette al progresso e ad ulteriore sviluppo tecnico e tecnologico. Pertanto il fornitore si riserva il diritto di modificare le TOM a condizione che il funzionamento e la sicurezza del servizio non vengano degradati. Le TOM forniscono un adeguato livello di protezione dei Dati Personali prendendo in considerazione i rischi associati al trattamento
- garantisce che le persone autorizzate ad accedere ed utilizzare il Contenuto per le finalità del Servizio Cloud si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

Più specificamente, il programma di sicurezza del Fornitore e dei sub-responsabili comprende:

CONTROLLO ACCESSI ALLE AREE IN CUI SONO SVOLTI I TRATTAMENTI
Misure idonee per impedire a persone non autorizzate di ottenere l'accesso alle apparecchiature di elaborazione dei dati (vale a dire telefoni, database e server delle applicazioni e relativo hardware) in cui i dati personali vengono trattati;

CONTROLLO ACCESSI AI SISTEMI DI TRATTAMENTO DEI DATI PERSONALI
Misure adeguate per impedire che i sistemi di elaborazione dei dati vengano utilizzati da persone non autorizzate;

CONTROLLO ACCESSI PER L'UTILIZZO DI SPECIFICHE FUNZIONALITÀ O AREE DEI SISTEMI DI TRATTAMENTO DATI
Esclusivamente le persone autorizzate possono essere poste nella condizione di accedere ai dati e solo nell'ambito e nella misura coperta dalle rispettive autorizzazioni di accesso (autorizzazione). I dati personali non possano essere letti, copiati, modificati o rimossi senza autorizzazione;

CONTROLLO DISPONIBILITÀ
Misure idonee a garantire che i dati personali siano protetti da distruzione o perdita accidentale;

CONTROLLO DELLA TRASMISSIONE

Misure adeguate per impedire che i dati personali vengano letti, copiati, alterati o cancellati da parti non autorizzate durante la loro trasmissione;

SEPARAZIONE DEI TRATTAMENTI PER FINALITÀ DIVERSE

Il Fornitore implementa misure idonee a garantire che i dati raccolti per finalità diverse possano essere elaborati separatamente;

DOCUMENTAZIONE

E' conservata la documentazione delle misure tecniche e organizzative in caso di audit e per la conservazione delle prove. Sono adottate misure ragionevoli per garantire che le persone nel luogo di lavoro interessati al trattamento, siano a conoscenza e rispettino le misure tecniche e organizzative stabilite nel presente documento;

MONITORAGGIO

Sono implementate misure idonee per monitorare le restrizioni di accesso agli amministratori di sistema e per garantire che agiscano secondo le istruzioni ricevute.

DESCRIZIONE DELLE MISURE TECNICHE DI SICUREZZA

1° LIVELLO – SISTEMI ESTERNI DI PREVENZIONE

Scansione online erabilità	Nessus® Essentials: soluzione per la rilevazione delle vulnerabilità di Tenable®, Inc. Nel 2021 Tenable è stato un Software Vendor di Gartner rappresentativo della Vulnerability Assessment.

2° LIVELLO – INFRASTRUTTURA I.T. DEL CLOUD SERVICE PROVIDER

Service Provider	Microsoft Azure.
Tipologia di servizio cloud	Public Cloud
Certificazioni del cloud service provider	Consulta la documentazione di conformità di Microsoft Azure.
Localizzazione dei data center utilizzati	West Europe (Netherlands)
Livelli di sicurezza adottati dal service provider	Operazioni eseguite da Microsoft per proteggere l'infrastruttura di Azure.

Ridondanza dei dati del service provider	Archiviazione con ridondanza di zona (Zone Redundancy Storage, ZRS): replica i dati archiviati in Azure in modalità sincrona su tre aree disponibili interne all'area primaria (primary region).

3° LIVELLO – INFRASTRUTTURA I.T.

Firewall	PfSense®, firewall riconosciuto come uno dei più potenti, sicuri ed affidabili.
Back-up	Procedura di back-up delle Virtual Machine: • 1. Frequenza: ogni 4 ore. • 2. Modalità di archiviazione: ridondanza geografica GRS (GEO-REDUNDANT-STORAGE). Copia dei dati in modo sincrono tre volte all'interno di un'unica posizione fisica nell'area primaria usando l'archiviazione con ridondanza locale. Copia quindi i dati in modo asincrono in un'unica posizione fisica nell'area secondaria. All'interno dell'area secondaria i dati vengono copiati in modo sincrono tre volte usando l'archiviazione con ridondanza locale. • 3. Area Primaria: West Europe (Netherlands). • 4. Area Secondaria : North Europe (Ireland). • 5. Retention Backup: 15 giorni.
disaster recovery	Procedura di Disaster Recovery delle Virtual Machine: 1. Modalità: Cross Region Restore. 2. Ridondanza: geografica (Geo-Redundancy Storage, GRS). Replica dei dati archiviati in Azure in modalità sincrona su una

	località fisica differente (regione secondaria). 3. Localizzazione del data center utilizzato per il Disaster recovery: North Europe (Ireland).
	RTO (Recovery Time Objective, il tempo necessario per il ripristino del sistema): 2 giorni lavorativi (tempo minimo)
	RPO (Recovery Point Objective, quantità massima di dati - espressa in ore - che l'azienda perde a seguito del verificarsi di un evento disastroso, poiché non rientrati nella normale procedura ciclica di back-up): 4 ore (tempo massimo)

4° LIVELLO – COMPONENTI SOFTWARE	
Sistema operativo	Antivirus Microsoft Forefront
Server virtuale	L'accesso ai server virtuali avviene mediante una VPN ed utilizzando un profilo utente dimensionato strettamente in base alle necessità di monitoraggio e manutenzione.

5° LIVELLO – CODICE APPLICATIVO

Sicurezza informatica del produttore	Nell'ambito del processo di qualificazione del Cloud Marketplace ACN, il produttore ha validato i propri livelli di gestione della riservatezza e della sicurezza dei dati della soluzione Whistleblowing Intelligente presso lo STAR Registry (Security, Trust, Assurance, and Risk) della Cloud Security Alliance. Visualizza la scheda di qualificazione del Marketplace ACN Cloud Visualizza la scheda di Whistleblowing intelligente su Cloud Security Alliance Visualizza la scheda del produttore su Cloud Security Alliance
Sistema di autenticazione	Sistema proprietario. È il sistema che vincola la password di accesso del singolo utente Interfacciamento con sistemi esterni. Possibilità di demandare la gestione dell'accesso utenti mediante procedura di Single Sign On con altri sistemi: SPID (Sistema Pubblico di Identità Digitale)
IP filtering	Utenti collegati. Possibilità di visualizzare tutti gli utenti autenticati (non i Segnalanti) sulla piattaforma Whistleblowing Intelligente con i seguenti dati: cognome, nome, ruolo, indirizzo IP, ultimo accesso effettuato.

6° LIVELLO – DATI E DOCUMENTI DELLA PIATTAFORMA WHISTLEBLOWING INTELLIGENTE

Criptaggio database e documenti	1. Database. Chiave di criptazione dati a sua volta criptata mediante un algoritmo per un ulteriore livello di sicurezza. Il dato resta criptato nel database e la sua decrittazione avviene solo quando viene visualizzato. 2. Documenti. Criptazione e decriptazione mediante chiave privata.
Protocollo HTTPS	L'HyperText Transfer Protocol Secure (over Secure Socket Layer) è un protocollo per la comunicazione su Internet che protegge integrità e riservatezza dei dati scambiati tra la piattaforma e l'hardware (PC, tablet, smartphone) dell'utente che vi accede. Certificato SSL erogato da Network Solutions LLC.