COMUNE DI
COMO

Settore Patrimonio e Smart City
Servizio SMART CITY

ATTO DI DESIGNAZIONE A RESPONSABILE DEL TRATTAMENTO

Tra

Il Comune di COMO con sede legale in sede in Via Vittorio Emanuele II, n. 97, P. IVA 00417480134, in persona del Suo delegato Ing. GIOVANNI FAZIO (di seguito, "**Ente"** e/o **"Titolare"**)

E

TECNOLINK S.R.L, con sede legale in sede in **VIA P. BAGETTI, 10 - 10143 TORINO**, P. IVA 07504810016 in persona del suo legale rappresentante Dott. Antonio Cappiello (di seguito, il **"Fornitore"** e/o **"Responsabile"**)
(di seguito, collettivamente, definite le **"Parti"**)

Premesso che:

i) l'Ente ha affidato al Fornitore con contratto sottoscritto in data 24/10/2025 l'esecuzione delle attività descritte nell' allegato 1 *("Allegato 1 – descrizione del trattamento")*, da intendersi parte integrante del presente atto (di seguito, "**Servizi**");
ii) lo svolgimento della suddetta attività da parte del Fornitore comporta il trattamento, da parte di quest'ultimo, per conto dell'Ente, dei dati personali di interessati di cui il primo è Titolare del trattamento (anche "Dati"), ai sensi del Regolamento europeo in materia di protezione dei Dati personali n. 679/2016, (di seguito anche solo "RGPD" o "Regolamento") e del Codice privacy come ss. modificato (di seguito "Codice");
iii) con il presente atto, le Parti, ai sensi dell'art. 28 del RGPD, intendono regolare i trattamenti dei Dati personali, meglio descritti nell'allegato 1, da parte del Fornitore: l'Ente e il Fornitore sono qualificati anche, nel prosieguo, rispettivamente, quali Titolare e Responsabile.
Tutto ciò premesso (e costituendo le premesse parte integrante e sostanziale del presente atto di designazione, unitamente agli allegati), considerata l'idoneità del Fornitore rispetto alle caratteristiche di esperienza, capacità ed affidabilità per la tutela del trattamento dei Dati in relazione alle attività e Servizi affidati al Fornitore in forza del contratto stipulato, l'Ente, quale Titolare del trattamento dei Dati personali

DESIGNA

il Fornitore come Responsabile del trattamento dei Dati personali connesso all'erogazione dei Servizi ai sensi e per gli effetti dell'art. 28 del RGPD. (di seguito anche "Responsabile"), assumendosi ogni obbligo in capo al Responsabile del Trattamento. Il Responsabile del trattamento, che accetta la nomina, dichiara espressamente di conoscere la normativa ed essere conforme.
Per l'effetto, fra le Parti si conviene e si stipula quanto segue:

1. OGGETTO E MANTENIMENTO DEI REQUISITI

1.1 Con il presente atto di nomina (di seguito anche "Atto") le Parti intendono disciplinare, dopo ampia trattativa contrattuale, i relativi rapporti, poteri e facoltà in relazione al trattamento dei Dati personali connesso all'erogazione dei Servizi.
1.2 I servizi oggetto di fornitura e le relative informazioni accessorie sono specificati nell'allegato 1 del presente documento. In caso di modifica o integrazione degli stessi, le parti potranno modificare o integrare le informazioni del medesimo allegato sottoscrivendolo per accettazione. Analogamente, qualora si rendesse necessaria la modifica o l'integrazione delle misure di sicurezza relative alla fornitura del servizio, le parti provvederanno all'aggiornamento dell'allegato 2, sottoscrivendo per accettazione le nuove condizioni stabilite.
1.3 Il Fornitore prende atto che l'incarico è stato assegnato esclusivamente perché il profilo professionale del Fornitore è stato ritenuto idoneo a soddisfare i requisiti di esperienza, capacità, affidabilità previsti dal RGPD. Tali requisiti sono una condizione normativa e contrattuale inderogabile per la fornitura del servizio. Qualsiasi variazione delle condizioni di erogazione del servizio che possa sollevare incertezze sul loro mantenimento, dovrà essere preventivamente segnalata al Titolare, che potrà esercitare il diritto di revoca in piena libertà, senza penali e/o eccezioni di sorta, qualora le modifiche riscontrate non consentano di garantire i requisiti di sicurezza previsti dalle norme e dall'accordo tra le parti.
1.4 Con tale nomina si intende disciplinare altresì gli obblighi del Responsabile anche in tema di amministratore di sistema.

2. OBBLIGHI DEL RESPONSABILE

2.1 Il Responsabile è tenuto a trattare i Dati personali solo ed esclusivamente ai fini dell'esecuzione dei Servizi, nel rispetto di quanto disposto dalla normativa applicabile in materia di protezione dei Dati personali, nonché delle istruzioni del Titolare riportate nei successivi articoli e negli allegati e di ogni altra indicazione orale o scritta che potrà essergli dallo stesso fornita.
2.2. Il Responsabile svolge funzioni di amministrazione di sistema per l'infrastruttura gestita per conto del Titolare. A tal proposito, il Responsabile è tenuto alla designazione dei soggetti che svolgeranno le funzioni di amministratore di sistema per conto del Titolare, individuando le persone fisiche che effettueranno attività di gestione e manutenzione dei sistemi informatici tramite cui si svolgeranno i trattamenti di dati oggetto del presente documento.
La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.
Il Responsabile deve inoltre fornire, su richiesta dello stesso Titolare, la lista nominativa degli Amministratori di Sistema.
Il Responsabile è inoltre tenuto all'osservanza delle prescrizioni del Garante della Privacy in tema di amministratori di sistema per i contesti di propria competenza, in particolar modo in tema di registrazione degli accessi logici da parte degli amministratori di sistema.

3. MISURE DI SICUREZZA

3.1 Il Responsabile, previa effettuazione dell'analisi dei rischi e tenendo conto, in particolare, dei rischi che derivano dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, ai Dati personali trasmessi, conservati o comunque trattati, dovrà adottare misure tecniche, fisiche ed organizzative adeguate per proteggere la sicurezza, la riservatezza e l'integrità dei Dati personali, tenendo conto, fra l'altro, della tipologia di trattamento, delle finalità perseguite, del contesto e delle specifiche circostanze in cui avviene il trattamento, nonché della tecnologia applicabile e dei costi di attuazione.
3.2 Fermo restando quanto sopra, il Responsabile si obbliga ad adottare, in particolare, le istruzioni e le misure di sicurezza fisiche, logiche e organizzative di cui *all'Allegato 2*, parte integrante del presente Atto ("*Allegato 2 – istruzioni e misure di sicurezza da adottare"*) ed in ogni caso tutte le misure indicate ai sensi dall'art. 32 del RGPD. Il Responsabile è tenuto ad informare immediatamente il Titolare laddove ritenga di non adottare anche una delle misure indicate da quest'ultimo. Si impegna altresì a fornire la dovuta motivazione, assistenza ed informazione, anche documentale, al Titolare.
3.2 *bis* Per quanto attiene alla misure fisiche, logiche e organizzative di cui al punto 3.2 nel caso di infrastrutture utilizzate dal Responsabile in modalità IaaS, si intendono quelle adottate dal gestore della infrastruttura cloud acquisita dal Responsabile stesso.
3.3 Eventuali evoluzioni e/o modifiche delle misure di sicurezza resesi necessarie a causa di modifiche e aggiornamenti della normativa in materia di protezione dei Dati personali saranno adottate ed implementate dal Fornitore e/o suoi eventuali subappaltatori a onere e spese del Fornitore stesso.
3.4 In ogni caso, oltre a quanto precedentemente indicato, il Responsabile deve garantire sempre l'osservanza, almeno per il livello M ("Minimo"), delle misure minime di sicurezza ICT per le Pubbliche Amministrazioni e degli aggiornamenti normativi sul tema.
In particolare, il Responsabile deve garantire il rispetto delle misure relative a:

- backup e copie di sicurezza;
- protezione dei dati;
- valutazione e correzione continua delle vulnerabilità;
- difese contro i malware;
- uso appropriato dei privilegi di amministratore.

Il Responsabile deve ottemperare a tutti gli adempimenti di propria competenza.
3.4 Il Responsabile si impegna altresì ad adottare tutte le misure tecniche e organizzative appropriate per garantire un livello di sicurezza adeguato per il trattamento di dati effettuato tramite eventuali software forniti o utilizzati dal Titolare. Tali misure devono essere commisurate rispetto al rischio per le persone che possa derivare dall'utilizzo del software e dalla correlata attività di assistenza e manutenzione. In particolare, il Responsabile deve garantire la valutazione e correzione continua delle vulnerabilità, oltre che l'adozione dei principi di protezione dei dati.

4. VIOLAZIONI DI DATI PERSONALI (CD. "DATA BREACH")

4.1 Il Responsabile si impegna ad informare il Titolare di ogni violazione della sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la

divulgazione non autorizzata o l'accesso ai Dati personali trasmessi, conservati o comunque trattati, informando altresì delle conseguenze della violazione e dei provvedimenti adottati per porvi rimedio. La violazione ed ogni utile informazione va comunicata per iscritto senza ingiustificato ritardo, e comunque entro e non oltre 48 ore dal momento in cui ne è venuto a conoscenza, ai contatti del Titolare indicati nell'art. 17 che segue. Il Responsabile, entro lo stesso termine, deve altresì fornire al Titolare i documenti e ogni informazione relativi alla violazione dei Dati personali del Titolare e deve prestare ogni necessaria collaborazione al Titolare in relazione all'adempimento degli obblighi sullo stesso gravanti di notifica delle suddette violazioni all'Autorità ai sensi dell'art. 33 del RGPD o di comunicazione della stessa agli interessati ai sensi dell'art. 34 del RGPD.

5. VALUTAZIONE D'IMPATTO (CD. "DATA PROTECTION IMPACT ASSESSMENT")

5.1 Il Responsabile s'impegna fin da ora a fornire al Titolare ogni elemento utile all'effettuazione, da parte di quest'ultimo, della valutazione di impatto sulla protezione dei Dati personali, qualora il Titolare sia tenuto ad effettuarla ai sensi dell'art. 35 del Regolamento, nonché ogni collaborazione nell'effettuazione della eventuale consultazione preventiva al Garante da parte di quest'ultimo ai sensi dell'art. 36 del Regolamento stesso.

6. SOGGETTI AUTORIZZATI AL TRATTAMENTO

6.1 Fatto salvo quanto previsto all'articolo 10 che segue, il Fornitore garantisce che l'accesso ai Dati personali sarà limitato esclusivamente a soggetti autorizzati per iscritto, identificando l'ambito autorizzativo, adeguato e non eccedente rispetto alla mansione.

6.2 Il Fornitore si obbliga a garantire che le persone autorizzate dal Responsabile medesimo a trattare i Dati personali:

- si impegnino a tutelarne la riservatezza, la disponibilità e l'integrità, o siano sottoposti ad un obbligo legale appropriato di segretezza;
- ricevano adeguate istruzioni, oltre che la formazione necessaria in materia di protezione dei Dati personali.

7. RAPPORTI CON LE AUTORITÀ

7.1 Il Responsabile, su richiesta del Titolare, si impegna a coadiuvare quest'ultimo nella difesa in caso di procedimenti dinanzi all'autorità di controllo o all'autorità giudiziaria che riguardino il trattamento dei Dati personali connessi ai Servizi.

8. ISTANZE DEGLI INTERESSATI

8.1 Il Responsabile si obbliga ad assistere il Titolare con misure tecniche ed organizzative adeguate, nell'adempimento degli obblighi gravanti su quest'ultimo in relazione all'esercizio dei diritti degli interessati, consentendo al Titolare di dar seguito efficacemente alle istanze degli interessati di cui al capo III del RGPD fornendogli ogni informazione e/o documento utile entro **5** giorni lavorativi dalla ricezione della richiesta, anche nel caso sia pervenuta direttamente al Responsabile, e circoscritto ai soli metadati di sistema in possesso della Società.

9. ULTERIORI OBBLIGHI

9.1 Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla normativa in materia di protezione dei Dati personali e/o delle istruzioni del Titolare di cui al presente atto di designazione e consente al Titolare del trattamento, previo ragionevole preavviso, l'esercizio del potere di controllo e ispezione, prestando ogni ragionevole collaborazione alle attività di audit effettuate dal Titolare stesso o da un altro soggetto da questi incaricato o autorizzato, con lo scopo di controllare l'adempimento degli obblighi e delle istruzioni di cui al presente Atto.

10. ULTERIORI RESPONSABILI

10.1 È fatto divieto al Responsabile di ricorrere, per l'esecuzione delle attività di trattamento di Dati personali oggetto del presente atto, ad ulteriori responsabili (di seguito, "Sub-responsabili") senza la preventiva autorizzazione scritta del Titolare.
A tal fine, il Responsabile sarà tenuto a comunicare per iscritto al Titolare:

i. la denominazione e la sede legale dei Sub-responsabili di cui intende avvalersi;
ii. il luogo in cui essi svolgono la loro attività se diverso dalla sede legale;
iii. informazioni dettagliate circa le attività di trattamento che, con riferimento ai Servizi, verranno ad essi affidate.

10.2 Il Responsabile si obbliga ad imporre per iscritto ai propri Sub-responsabili, attraverso appositi accordi vincolanti, i medesimi obblighi in materia di protezione dei Dati personali cui è soggetto il Responsabile in virtù del presente atto. Nell'adempimento delle proprie obbligazioni ogni sub-fornitore, nell'ambito del trattamento dei Dati oggetto dell'incarico del Responsabile, è obbligato a rispettare il RGPD e ogni altra istruzione impartita dal Titolare, nonché a tenere conto dei provvedimenti del Garante e/o Autorità europea per la protezione dei Dati. Qualora uno degli altri sub-responsabili del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei Dati, il Responsabile iniziale conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.
10.3 Il Titolare avrà diritto di richiedere al Responsabile di fornire copia degli accordi intercorrenti con i propri Sub-responsabili ed in generale di tutte le informazioni e i documenti comprovanti il rispetto degli obblighi assunti con il presente Atto. Al sub-fornitore sarà concesso di trattare solo i Dati strettamente necessari per l'espletamento dell'incarico.
10.4 II Responsabile si impegna espressamente ad informare il Titolare di eventuali modifiche riguardanti l'aggiunta o la sostituzione degli ulteriori Sub-responsabili. Il Titolare avrà il diritto di opporsi a tali modifiche, comunicando la sua opposizione per iscritto entro 30 giorni dalla notifica da parte del Responsabile.
10.5 Il Responsabile non ricorrerà ai Sub-responsabili nei cui confronti il Titolare abbia manifestato la sua opposizione.
10.6 Nel caso delle sole piattaforme tecnologiche SaaS è concesso, per motivi di sicurezza o di variazione del mercato, la possibilità di modificare il sub-responsabile senza preventiva autorizzazione a condizione che tale modifica sia comunicata entro 7 giorni dalla stipula del contratto con il relativo nuovo sub-responsabile.

11. RESPONSABILITÀ E MANLEVA

11.1 Il Responsabile si impegna a manlevare e tenere indenne il Titolare da danni, costi o sanzioni amministrative pecuniarie che siano **conseguenza diretta e immediata** di violazioni delle disposizioni normative applicabili, nonché di una violazione del Regolamento (UE) 2016/679 o degli obblighi derivanti dal presente Atto, qualora tale violazione sia **esclusivamente imputabile a dolo o colpa del Responsabile** (o dei suoi dipendenti/sub-responsabili); in tali casi, il Responsabile sarà considerato alla stregua di un Titolare del trattamento e ne risponderà direttamente anche dal punto di vista sanzionatorio.

11.2 Il Responsabile risponde del danno cagionato dal trattamento solo qualora non abbia adempiuto agli obblighi del Regolamento specificamente diretti ai responsabili del trattamento o abbia agito in modo difforme o contrario rispetto alle istruzioni impartite dal Titolare, ai sensi dell'Art. 82, par. 2 del RGPD.

11.3 Qualora il Titolare e il Responsabile siano coinvolti nel medesimo trattamento e siano entrambi responsabili del danno cagionato, ciascun soggetto è tenuto a risarcire il danno in misura proporzionale alla propria quota di responsabilità per l'inadempimento, in conformità al principio di solidarietà attenuata di cui all'Art. 82, par. 4 e 5 del RGPD.

11.4 Il Responsabile non potrà essere ritenuto responsabile per danni derivanti da:

- Istruzioni del Titolare rivelatesi errate o in contrasto con la normativa, segnalate dal Responsabile ai sensi dell'Art. 28.3, ultimo comma;
- Uso improprio delle credenziali di accesso da parte del personale autorizzato del Titolare;
- Eventi di forza maggiore o malfunzionamenti della rete internet non imputabili alla piattaforma.

11.5 In caso di contestazione o azione intrapresa da un terzo o dall'Autorità Garante nei confronti del Titolare, quest'ultimo si impegna a darne immediata comunicazione al Responsabile, consentendogli di partecipare attivamente alla difesa e di fornire ogni elemento utile alla contestazione del preteso illecito, prima di procedere a eventuali transazioni o pagamenti.

12. DURATA E REVOCA DEL TITOLARE

12.1 La presente designazione decorre dalla data di sottoscrizione e rimarrà in vigore ed efficace fino al termine o alla cessazione (per qualsivoglia ragione) dell'affidamento del Servizio ovvero fino alla eventuale revoca anticipata per qualsiasi motivo da parte del Titolare, fermo restando che, anche successivamente alla cessazione del contratto predetto o dei Servizi o alla revoca, il Responsabile dovrà mantenere la massima riservatezza sui Dati personali e le informazioni relative al Titolare delle quali sia venuto a conoscenza nell'adempimento delle sue obbligazioni.

13. RESTITUZIONE E CANCELLAZIONE DEI DATI PERSONALI

13.1 Il Responsabile, all'atto della scadenza del contratto in forza del quale sono forniti i

Servizi o, comunque, in caso di cessazione per qualunque causa dell'efficacia del presente atto di designazione, salvo la sussistenza di un obbligo di legge (es. fiscale) o di regolamento nazionale e/o comunitario che preveda la conservazione dei Dati personali, dovrà interrompere ogni operazione di trattamento degli stessi e dovrà provvedere a rendere disponibili i dati in formato aperto al Titolare del trattamento dei Dati personali e, su richiesta di quest'ultimo, alla loro integrale cancellazione e distruzione, rilasciando contestualmente una dichiarazione scritta che da tale momento non conserva più alcuna copia dei Dati personali, indicando altresì le modalità tecniche e le procedure scelte per la cancellazione/distruzione.

14. TRASFERIMENTO DI DATI PERSONALI VERSO STATI STRANIERI

14.1 Il Responsabile del trattamento si obbliga a non inviare i Dati personali e a non consentire a qualsivoglia Sub-responsabile del trattamento di inviare i Dati personali in Paesi extra-UE, salvo previa autorizzazione da parte del Titolare. In questo caso il trasferimento deve avvenire rigorosamente nel rispetto del RGPD.

14.2 Richiamato quanto sopra, Si accorda alla Società Tecnolink s.r.l. l'autorizzazione alla nomina dei "sub-responsabili" indicati nel documento "Dichiarazione Nomina trattamento dati personali Whistleblowing" reso disponibile dalla Società TECNOLINK S.R.L, di cui in atti.

14.3 Si prende atto che i dati personali raccolti dalla piattaforma https://wb.anticorruzioneintelligente.it/ sono trattati dalla Società: Interzen Consulting s.r.l., con sede in Pescara, Strada Comunale Piana 3, cap. 65129 (P. IVA e C.F. 01446720680), in persona dell'amministratore delegato pro tempore regolarmente nominata da Tecnolink S.r.l con atto formale come sub responsabile del trattamento dei dati personali.

14.4 Si prende atto che il sub-fornitore Interzen Consulting s.r.l., con sede in Pescara, Strada Comunale Piana 3, cap. 65129 (P. IVA e C.F. 01446720680) a sua volta, si avvale di Microsoft Azure la piattaforma cloud pubblica di Microsoft con ubicazione dell'infrastruttura fisica in Europa occidentale all'interno di paesi UE. I dati relativi al subfornitore Microsoft sono i seguenti:

Microsoft Ireland Operations Limited
One Microsoft Place
South County Business Park
Leopardstown
Dublino 18
D18 P521
Irlanda
Numero partita IVA IE 8256796 U

14.5 Si prende, altresì, atto della regolarizzazione dei rapporti contrattuali di Interzen con Microsoft Ireland secondo le modalità stabilite da Microsoft stessa. Dette modalità comprendono uno specifico Addendum relativo alle responsabilità del trattamento dei dati, anche di quelli personali, coerente con quanto previsto dal Regolamento Europeo n. 2016/679 (GDPR).

14.6 L'Addendum sopra richiamato, equivale a nomina da parte di Interzen nei

confronti di Microsoft quale Responsabile del Trattamento dei dati personali**.**
14.7 Si prende atto dell'avvenuta Certificazione ISO/IEC 27001 del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) della Società TECNOLINK
14.8 Si prende, infine, atto del documento "Addendum Nomina Responsabile Trattamento Dati", contenente informazioni aggiuntive di dettaglio sulle misure adottate e da intendersi quale esplicitazione di quanto si chiede come misure minime di sicurezza.

15. LEGGE APPLICABILE E FORO COMPETENTE

15.1 Il presente contratto avente ad oggetto la designazione del Responsabile e la disciplina dei Dati personali trattati dal Responsabile per conto del Titolare sarà regolato dalla legge italiana. Qualsiasi controversia che non possa essere risolta amichevolmente tra le Parti sarà devoluta alla competenza esclusiva del Tribunale competente ove ha sede il Titolare.

16. DISPOSIZIONI FINALI

16.1 Resta inteso che la presente designazione non comporta alcun diritto per il Responsabile ad uno specifico compenso o indennità o rimborso per l'attività svolta, né ad un incremento del compenso spettante allo stesso in virtù del contratto di affidamento dei Servizi stipulato con il Titolare.
Solo nel caso di richiesta di audit straordinari dovrà essere presentato dalla Società un preventivo per sostenere i costi.
16.2 Per tutto quanto non previsto dal presente atto di designazione si rinvia alle disposizioni generali vigenti ed applicabili in materia protezione dei Dati personali.
16.3 Le Parti si danno atto che tutte le condizioni del presente Contratto sono state ampiamente negoziate e che, quindi, sono stati ben compresi i reciproci vantaggi, le obbligazioni e gli oneri assunti. Per tale ragione non si applicano gli articoli 1341 e 1342 del Codice civile.

17. COMUNICAZIONI

17.1 Tutte le comunicazioni tra le Parti dovranno avvenire tramite posta elettronica certificata agli indirizzi di contatto specificati all'allegato 1.

Il documento viene sottoscritto digitalmente dalle parti per accettazione.

Per il Titolare
Il Direttore del Settore
(nome e cognome)

Per il Responsabile
(nominativo responsabile)

Firmato digitalmente da

GIOVANNI FAZIO
Data e ora della firma:
04/05/2026 15:51:26

COMUNE DI COMO

Settore Patrimonio e Smart City
Servizio SMART CITY

ALLEGATO 1
DESCRIZIONE DEL TRATTAMENTO

1. DESCRIZIONE DEL SERVIZIO OFFERTO E DEL TRATTAMENTO CORRELATO

Il servizio offerto dal responsabile è il seguente:
servizio di gestione – assistenza, supporto, inerente il SERVIZIO IN MODALITA SAAS (SOFTWARE AS A SERVICE) PIATTAFORMA WEB DI WHISTLEBLOWING INTELLIGENTE PER IL PERIODO 01/11/2025-31/10/2026 (ordine MEPA n° 8746012 accettato il 24/10/2025).

In particolare dovranno essere garantite le seguenti macro linee di attività (attività minime non esaustive):

- ✓ esecuzione dei compiti propri dell'"Amministratore di Sistema" e " Responsabile della sicurezza dei dati";
- ✓ supporto agli utenti per la soluzione di malfunzionamenti e/o criticità;
- ✓ creazione di report periodici a supporto dell'attività di monitoraggio dei progetti;

Il trattamento di dati correlato consiste nel potenziale **accesso** a tutti i dati detenuti sui sistemi informatici per ottemperare agli obblighi contrattuali di servizio.

2. FINALITA' DEL TRATTAMENTO

Il servizio ha le seguenti finalità:

i) Esecuzione del contratto.

3. DURATA DEL TRATTAMENTO

La durata del trattamento si riferisce al periodo NOV 2025/OTT 2026.

4. TIPOLOGIA DI DATI TRATTATI[1]

[1] Per il Responsabile della Prevenzione della corruzione ed eventuali collaboratori autorizzati, in aggiunta vengono trattati i seguenti dati: indirizzo ip, dati di log**.** Sono altresì trattati, in quanto acquisiti implicitamente nell'uso dei protocolli di comunicazione di Internet, tra gli altri, i seguenti dati: indirizzi IP o i nomi a dominio dei computer utilizzati dagli utenti che si connettono al sito, gli indirizzi in notazione URI (Uniform Resource Identifier) delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente. Questi dati vengono utilizzati al solo fine di ricavare informazioni statistiche anonime sull'uso del sito e per controllare il corretto funzionamento e vengono cancellati immediatamente dopo l'elaborazione. I dati potrebbero essere utilizzati per l'accertamento di responsabilità in caso di ipotetici reati informatici ai danni della piattaforma o su richiesta delle autorità competenti.

DATI PERSONALI TRATTATI			
[X]	Nome e cognome	[X]	Luogo e data di nascita
[X]	Codice fiscale	[X]	Dati di contatto (indirizzo, email, telefono)
[]	Credenziali accesso a sistemi informatici	[X]	Indirizzo IP, geolocalizzazione, dati di sessione
[X]	Datore di lavoro e ruolo lavorativo	[X]	Altri dati forniti volontariamente
[]	Situazione patrimoniale / di reddito	[]	Situazione finanziaria
[]	Situazione economica	[]	Situazione tributaria/fiscale
DATI PARTICOLARI E RELATIVI ALLA SALUTE			
[X]	Dati inerenti origine razziale ed etnica	[X]	Convinzioni religiose o filosofiche
[X]	Opinioni politiche	[X]	Appartenenza a sindacati
[X]	Orientamento sessuale	[X]	Dati biometrici
[X]	Dati relativi alla salute	[X]	Dati relativi a condanne penali
[X]	Altri dati personali forniti volontariamente	[ ]	

5. CATEGORIE DI INTERESSATI

[X]	Dipendenti o ex dipendenti, nonché dipendenti delle Società in house	[X]	Volontari e tirocinanti, retribuiti o non retribuiti
[X]	Lavoratori autonomi, Consulenti e collaboratori a qualunque titolo	[X]	Candidati a ricoprire una posizione lavorativa in qualsiasi forma ed a qualsiasi titolo, anche non retribuita e/o assunti in periodo di prova
[X]	Personale che opera a vario titolo presso l'ente		
[X]	Soggetti che fruiscono del servizio erogato dal Titolare		
[X]	Soggetti i cui dati sono trattati per obbligo di legge correlato al procedimento		
[X]	Dipendenti e collaboratori di imprese fornitrici di beni, lavori o servizi nel caso in cui la segnalazione riguardino fatti in cui è coinvolto o il Committente		
[X]	Le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto		
[X]	Aziende, consulenti e studi professionali partecipanti a procedure di scelta del contraente		

6. ELENCO DEI SUB-RESPONSABILI AUTORIZZATI

DENOMINAZIONE	FUNZIONE SVOLTA
Società: Interzen Consulting s.r.l con sede in Pescara, Strada Comunale Piana 3, cap. 65129 (P. IVA e C.F. 01446720680)	Si rinvia ai punti da 14.3 a 14.6 sopra riportati

7. RIFERIMENTI E DATI DI CONTATTO

SOGGETTO	RIFERIMENTI
REFERENTE DEL TITOLARE	RESPONSABILE DELLA PREVENZIONE E DELLA CORRUZIONE
RESPONSABILE PROTEZIONE DATI PERSONALI DEL TITOLARE	A partire dal 1 marzo 2023 il Responsabile della Protezione dei Dati ai sensi dell'Art. 37 del Regolamento UE 2016/679 è la Società SI.net Servizi Informatici s.r.l., come da Decreto Sindacale RG. n. 6 del 20/02/2023. Il punto di contatto dell'RPD è rpd@comune.como.it
REFERENTE DEL RESPONSABILE	TECNOLINK S.R.L, nella persona del suo legale rappresentante Dott. Antonio Cappiello
RESPONSABILE PROTEZIONE DATI PERSONALI DEL RESPONSABILE	TECNOLINK S.R.L, nella persona del suo legale rappresentante Dott. Antonio Cappiello

COMUNE DI COMO

Settore Patrimonio e Smart City
Servizio SMART CITY

ALLEGATO 2
ISTRUZIONI E MISURE DI SICUREZZA DA ADOTTARE

Le prescrizioni riportate nella seguente tabella costituiscono specifiche istruzioni sul trattamento dei dati effettuato per conto del titolare del trattamento. Le disposizioni sono tassative e la loro mancata osservazione comporta una violazione delle disposizioni normative e contrattuali relative al contratto di servizio in essere tra il titolare e il responsabile.

1.	**MISURE ORGANIZZATIVE**
a.	Tenuta di un registro delle attività del trattamento come previsto dall'art. 30 RGPD, in cui siano riportati i trattamenti effettuati per conto del titolare
b.	Presenza di una procedura di gestione degli incidenti che preveda, nei casi si renda necessario, la sollecita segnalazione al titolare secondo le disposizioni definite nell'accordo fra le parti
c.	Nomina di un Data Protection Officer
d.	Conferimento di istruzioni scritte ai soggetti autorizzati dal responsabile in tema di protezione e sicurezza dei dati personali
e.	Formazione dipendenti in tema di protezione e messa in sicurezza dei dati trattati nello svolgimento di attività correlate al servizio svolto per conto del titolare
f.	Formalizzazione per tutti i dipendenti e collaboratori del responsabile di un impegno alla riservatezza sui dati trattati nello svolgimento di attività correlate al servizio svolto per conto del titolare
g.	Ricorso a sub-responsabili solo a seguito di preventiva comunicazione al titolare e a sua mancata opposizione entro 30 giorni dalla sua comunicazione
h.	Limitazione ai sub-responsabili di accesso ai dati del titolare espressamente per l'espletamento dei servizi oggetto dell'accordo tra titolare e responsabile
i.	Verifiche periodiche sui fornitori (ad es. tramite verifica documentale, verifica presenza e/o sussistenza certificazioni del fornitore o audit presso il fornitore)
j.	Espresso divieto di trasferimento dati verso un paese terzo o un'organizzazione internazionale che non garantiscano (o in assenza di) un livello adeguato di tutela, ovvero, in assenza di strumenti di tutela previsti dal Regolamento UE 2016/679 (Paese terzo giudicato adeguato dalla Commissione Europea, BCR di gruppo, clausole contrattuali modello, consenso degli interessati, etc.)
k.	Trasferimento o effettuazione di trattamento dei dati personali del titolare verso un paese terzo e/o al di fuori dell'Unione Europea esclusivamente a seguito di autorizzazione scritta del Titolare
2.	**MISURE FISICHE**
a.	Presenza di sistemi di protezione degli ambienti in cui viene effettuato il trattamento dei dati per conto del titolare (es. allarmi perimetrali o volumetrici, presenza di inferriate o blindatura alle finestre e porte antisfondamento, sistemi

	antincendio)
b.	Presenza di sistemi di limitazione degli accessi ai soli soggetti autorizzati agli ambienti in cui viene effettuato il trattamento dei dati per conto del titolare (es. tramite accessi con chiavi/badge, monitoraggio/tracciamento degli accessi, guardiania, ecc)
c.	Adozione di policy e procedure per la gestione degli accessi fisici ai locali in cui viene effettuato il trattamento dei dati per conto del titolare
d.	Protezione fisica e conservazione in sicurezza dei supporti portatili di archiviazione in uso presso l'organizzazione
3.	**MISURE SUGLI ARCHIVI CARTACEI**
a.	Messa in sicurezza degli archivi cartacei attraverso i quali viene effettuato il trattamento dei dati per conto del titolare
b.	Limitazione degli accessi agli archivi cartacei (es. mediante chiusura a chiave degli armadi e/o degli uffici in assenza del personale, etc…)
c.	Condivisione e della comunicazione cartacea esclusivamente con soggetti autorizzati
d.	Comunicazione a terzi di documentazione cartacea solamente quando previsto all'interno delle attività di trattamento di dati effettuato per conto del titolare
e.	Conferimento dell'informativa agli interessati se previsto tra le condizioni di fornitura del servizio
4.	**MISURE SULLE RISORSE ICT**
a.	Adozione di procedure e sistemi di gestione degli accessi logici (sistemi e processi di autorizzazione, profilazione degli accessi, gestione delle utenze, verifica periodica di sussistenza dei diritti di accesso dei soggetti autorizzati con disabilitazione delle utenze non più operanti)
b.	Implementazione di sistemi e processi di salvataggio (backup) e ripristino dei dati trattati per conto del titolare (schedulazione periodica dei backup in ambiente separato dalla rete di produzione, test di ripristino, custodia dei supporti e dispositivi di backup in luoghi sicuri)
c.	Limitazione di utilizzo esclusivo di software autorizzati dall'organizzazione per il trattamento di dati personali, con divieto di utilizzo di risorse non autorizzate
d.	Adozione di procedure di dismissione e/o eliminazione di dispositivi e supporti hardware contenenti dati del titolare
e.	Ove necessario, adozione di tecniche di cifratura e/o pseudonimizzazione degli archivi informatici
f.	Adozione di sistemi antimalware per postazioni di lavoro, server e altri dispostivi elettronici di trattamento dati
g.	Implementazione di processi e sistemi di verifica di vulnerabilità sui sistemi e di distribuzione delle patch di sicurezza rilevanti sui dispositivi in uso presso l'organizzazione
h.	Aggiornamento continuo dei livelli di sicurezza dei sistemi informatici in uso

	presso l'organizzazione con cui si trattano dati per conto del titolare
i.	Impiego di dispositivi di sicurezza perimetrale con funzioni di sicurezza (ad esempio Firewall e sistemi di Network Detection ed Event & Log Monitoring, SIEM, ecc.) necessari a rilevare e contenere eventuali incidenti di sicurezza ICT e in grado di gestire gli IoC (Indicator of Compromise)
j.	Effettuazione di audit periodici tramite organizzazioni esterne specializzate sui propri sistemi di sicurezza (es. vulnerability assessment, penetration test, security assessment, ecc.)
k.	Attivazione di sistemi di cifratura sui canali di connessione esterna autorizzata alla rete dell'organizzazione (es. Virtual Private Network o strumenti equivalenti)
l.	Implementazione di sistemi di protezione, autorizzazione, autenticazione e crittografia sulle reti wireless utilizzate presso l'organizzazione
m.	Attivazione di sistemi di cifratura sui dispositivi portatili che trattano dati personali
n.	Adozione ed osservanza delle Misure Minime di Sicurezza ICT per le PA, almeno per il livello M ("Minimo"), sui sistemi informativi attraverso cui sono trattati i dati per conto del titolare del trattamento
o.	Distruzione e smaltimento dei supporti informatici di memorizzazione logica o cancellazione dei dati (o attuazione di misure atte a garantire la loro non intelliggibilità) presenti sui supporti per il loro reimpiego, alla luce del Provvedimento del Garante per la Protezione dei Dati personali del 13 ottobre 2008 in materia di smaltimento strumenti elettronici
5.	**MISURE SULLE CREDENZIALI DI ACCESSO**
a.	Definizione di politica di gestione delle password (password complesse con caratteri alfanumerici, lunghezza di almeno 8 caratteri, scadenza con obbligo di modifica della password ogni 3 mesi, reimpostazione password obbligatoria al momento della comunicazione)
b.	Comunicazione agli utenti di userid e password utilizzando differenti canali di comunicazione
c.	Assegnazione di credenziali personali ad ogni utente
d.	Divieto di condivisione di credenziali fra gli utenti autorizzati e di comunicazione ad altri soggetti delle credenziali personali
e.	Conservazione in sicurezza delle credenziali assegnate
f.	Istruzione agli autorizzati circa la messa in sicurezza delle proprie credenziali
g.	Blocco delle utenze in caso di tentativi ripetuti di inserimento di credenziali scorrette
6.	**MISURE SUGLI AMMINISTRATORI DI SISTEMA**
a.	Individuazione e designazione individuale degli amministratori di sistema dei soggetti che svolgono le attività di gestione e manutenzione dei sistemi informatici, definite dal provvedimento del Garante Privacy del 2008 in tema di

	amministratori di sistema
b.	Individuazione degli specifici ambiti di operatività degli amministratori di sistema autorizzati in base al profilo di operatività assegnato
c.	Attribuzione di credenziali specifiche, con obbligo di utilizzo di password con lunghezza di almeno 14 caratteri per tutti i profili di amministrazione dei sistemi informatici attraverso i quali vengono trattati i dati del titolare del trattamento
d.	Aggiornamento continuo dell'elenco degli amministratori di sistema che operano sulle risorse attraverso cui sono trattati i dati del titolare del trattamento
e.	Tracciamento e registrazione diretta o indiretta degli accessi degli amministratori di sistema sui sistemi gestiti dal responsabile, con mantenimento per almeno 6 mesi dei log di accesso ai sistemi
f.	Adozione ed osservanza delle Misure Minime di Sicurezza ICT per le PA, almeno per il livello M ("Minimo"), per gli ambiti di propria competenza in materia di amministratori di sistema
7.	**MISURE DI SICUREZZA SUI CENTRI ELABORAZIONE DATI**
a.	Limitazione, monitoraggio e tracciamento degli ingressi/uscite tramite controllo degli accessi fisici ai locali da parte dei soggetti autorizzati (attraverso l'utilizzo di credenziali, dispositivi di autenticazione o identificazione personale)
b.	Presenza di adeguati sistemi di protezione fisica dei locali (es. porte antisfondamento, finestre blindate o protette da inferriate)
c.	Installazione di sistemi di controllo antintrusione (telecamere interne o sistemi volumetrici)
d.	Presenza di adeguati sistemi di protezione ambientale dei locali (sistema di rilevamento fumi e/o sistema antincendio allarmato, sistema di rilevamento allagamento allarmato, sistema di rilevamento temperatura allarmato, sistema di condizionamento)
e.	Presenza di sistemi di continuità elettrica costituiti da UPS di zona e, in caso di necessità, gruppi elettrogeni
f.	Adozione di sistemi di ridondanza delle risorse ICT (elaboratori di dati, sistemi di comunicazione e trasmissione, dispositivi di archiviazione)
g.	Adozione di procedure e sistemi di disaster recovery e business continuity
8.	**MISURE DI SICUREZZA SUL SOFTWARE**
a.	Progettazione e sviluppo del software con tecniche di *security by design* e *security by default*
b.	Implementazione di specifiche di sicurezza nel codice, nella struttura della base dati e nei sistemi di autenticazione degli utenti
c.	Adozione di tecniche di cifratura e/o pseudonimizzazione sulle basi di dati in caso di trattamento di categorie particolari di dati o dati personali relativi a condanne penali e reati

d. Effettuazione di test periodici di sicurezza sul software sviluppato (es. penetration test, security assessment, ecc.)
e. Valutazione e correzione continua delle vulnerabilità sul software fornito

Il Titolare del trattamento - Delegato	Il Responsabile del Trattamento
Comune di Como	*Legale rappresentante Società Tecnolink S.rl.*
Ing. Fazio Giovanni	*Dott. Antonio Cappiello*