Comune di Positano
Via Marconi 111, 84017 Positano (SA)
P.E.C. protocollo@pec.comunedipositano.it

CONTRATTO PER IL TRATTAMENTO DEI DATI PERSONALI

ai sensi dell'art. 28 GDPR — Clausole Contrattuali Tipo (Decisione di Esecuzione UE 2021/915)

Oggetto: Servizi di supporto gestionale ed operativo presso l'Area Vigilanza

(periodo 01.01.2025 - 31.12.2026)

TITOLARE del trattamento

Comune di Positano — Sede legale: Via G. Marconi 111, 84017 Positano (SA) — P.IVA: 00232340653 – C.F.: 80025630650 — legale rappresentante Sindaca dott.ssa GUIDA Gabriella domiciliata per la carica ed ai fini del presente contratto presso la sede legale del Comune

RESPONSABILE del trattamento

Consulenti Associati Sas di TORTORA Vincenzo & C. — Sede: Via G. Amendola 66, 84016 Pagani (SA) — P.IVA/C.F.: 02701650653 — legale rappresentante rag. TORTORA Vincenzo (c.f. TRTVCN64E22G230E) domiciliato ai fini del presente contratto presso la sede legale della Società

Anagrafica completa delle parti in Allegato I.

SEZIONE I — Clausole generali

Clausola 1 — Finalità e ambito di applicazione

Le presenti clausole garantiscono il rispetto dell'art. 28, parr. 3 e 4, GDPR; le parti indicate nell'Allegato I le accettano per disciplinare il trattamento descritto nell'Allegato II.

Clausola 2 — Invariabilità delle clausole

Le parti non modificano le clausole, salvo aggiornare le informazioni negli allegati; ciò non impedisce di inserirle in un contratto più ampio o di aggiungere clausole che non contraddicano, direttamente o indirettamente, le presenti.

Clausola 3 — Interpretazione e gerarchia

Le clausole si interpretano alla luce del GDPR; in caso di contrasto prevalgono sulle pattuizioni connesse esistenti tra le parti.

SEZIONE II — Obblighi delle parti

Clausola 4 — Descrizione del trattamento

Materia, durata, natura e finalità, tipi di dati e categorie di interessati sono specificati nell'Allegato II.

Clausola 5 — Istruzioni e limitazione delle finalità

Il responsabile tratta i dati solo su istruzione documentata del titolare e per le sole finalità dell'affidamento, salvo obblighi di legge; informa il titolare se un'istruzione viola la normativa.

Clausola 6 — Durata

Il trattamento ha la durata indicata nell'Allegato II (Log degli amministratori di sistema: almeno 6 mesi (Provv. Garante 27/11/2008) — verificare sul Piano di conservazione/massimario dell'ente).

Clausola 7 — Sicurezza del trattamento (art. 32)

Il responsabile adotta le misure tecniche e organizzative prescritte dal titolare nell'Allegato III, garantisce la riservatezza degli autorizzati (art. 29) e tratta i dati particolari (artt. 9-10) con le garanzie rafforzate ivi indicate.

Clausola 8 — Documentazione e conformità

Il responsabile mette a disposizione del titolare le informazioni necessarie a dimostrare la conformità all'art. 28.

Clausola 9 — Ricorso a sub-responsabili

Il responsabile ricorre a sub-responsabili solo previa autorizzazione (specifica o generale) del titolare, imponendo loro per contratto gli stessi obblighi ed elencandoli in Allegato IV; informa il titolare di ogni modifica con almeno 30 giorni di preavviso, dando tempo utile per opporsi prima del ricorso al nuovo sub-responsabile.

Clausola 10 — Trasferimenti internazionali

Trasferimenti verso Paesi terzi solo su istruzione del titolare e con garanzie adeguate (artt. 44 ss.).

Clausola 11 — Assistenza al titolare

Il responsabile assiste il titolare per le richieste degli interessati (artt. 15-22) e per gli obblighi di sicurezza, notifica delle violazioni, DPIA e consultazione preventiva (artt. 32-36).

Clausola 12 — Notifica delle violazioni dei dati

In caso di violazione dei dati personali, il responsabile notifica il titolare senza ingiustificato ritardo e comunque entro 24 ore dal momento in cui ne è venuto a conoscenza, utilizzando il modulo dell'Allegato V, e lo assiste per gli adempimenti conseguenti (notifica al Garante entro 72 ore, comunicazione agli interessati se necessaria).

Clausola 13 — Cancellazione e restituzione dei dati

Al termine del trattamento il responsabile, a scelta del titolare, cancella o restituisce i dati e le copie, salvo obblighi di legge.

Clausola 14 — Audit e ispezioni

Il responsabile mette a disposizione del titolare le informazioni necessarie a dimostrare la conformità e consente le attività di revisione, incluse le ispezioni, con un preavviso ragionevole (almeno 15 giorni lavorativi) e senza indebita interruzione della propria attività.

SEZIONE III — Disposizioni finali

Clausola 15 — Violazione delle clausole e risoluzione

In caso di inosservanza il titolare può sospendere il trattamento o risolvere il contratto.

Clausola 16 — Responsabilità

Resta ferma la disciplina della responsabilità e del risarcimento di cui all'art. 82 GDPR.

Clausola 17 — Legge applicabile e foro competente

Il contratto è regolato dalla legge italiana; foro competente: Salerno.

FIRME

IL TITOLARE DEL TRATTAMENTO	IL RESPONSABILE DEL TRATTAMENTO
Comune di Positano **La Sindaca dott.ssa Gabriella Guida** _____ (Firma)	**Consulenti Associati Sas di Tortora Vincenzo & C.** **Il legale Rappresentante rag. Vincenzo Tortora** _____ (Firma)

Luogo e data: Positano, 09.07.2026

ALLEGATO I — ELENCO DELLE PARTI

A. Titolare del trattamento

Ragione Sociale	**Comune di Positano**
Sede Legale	Via Marconi 111, 84017 Positano (SA)
P.IVA / C.F.	P.IVA: 00232340653 – C.F. 80025630650
Legale Rappresentante	dott.ssa Gabriella Guida
PEC	protocollo@pec.comunedipositano.it
Referente	dott.ssa Cecilia Iorio
Email Referente	protocollo@pec.comunedipositano.it
DPO (se nominato)	Davide Pasquale

B. Responsabile del trattamento

Ragione Sociale	**Consulenti Associati Sas di Tortora Vincenzo & C.**
Sede Legale	Via Amendola 66, 84016 Pagani (SA)
P.IVA / C.F.	02701650653
Legale Rappresentante	rag. Tortora Vincenzo
PEC	consulentiassociatisnc@pec.it
Referente	rag. Tortora Vincenzo
Email Referente	consulentiassociati@libero.it
Telefono	08119001554

ALLEGATO II — DESCRIZIONE DEL TRATTAMENTO

1. Descrizione generale
Servizi di supporto gestionale ed operativo presso l'Area Vigilanza (periodo 01.01.2025 – 31.12.2026)

2. Categorie di interessati
Cittadini e soggetti giuridici diversi

3. Categorie di dati personali
Fascicoli, dati e pratiche amministrative, banche dati dell'Area Vigilanza

4. Categorie particolari di dati (art. 9-10 GDPR)
Nessuna

5. Finalità del trattamento
Supporto gestionale ed operativo alle attività dell’Area Vigilanza

6. Natura del trattamento
Supporto gestionale e operativo continuativo per l'Area Vigilanza.

7. Durata del trattamento e conservazione
Log degli amministratori di sistema: almeno 6 mesi (Provv. Garante 27/11/2008) — verificare sul Piano di conservazione/massimario dell'ente.

8. Frequenza del trattamento
☑ Continuativo ☐ Periodico ☐ Occasionale

ALLEGATO III — MISURE TECNICHE E ORGANIZZATIVE

Il Titolare prescrive, quali condizioni minime del presente affidamento e ai sensi dell'art. 32 GDPR, le misure tecniche e organizzative di cui alla Sezione A. Il Responsabile, sottoscrivendo il presente contratto, dichiara di adottarle e si impegna a mantenerle per l'intera durata del trattamento; può inoltre indicare misure ulteriori adottate a integrazione.

A. Misure generali di sicurezza (prescritte dal Titolare)

Sicurezza fisica

☑ Controllo degli accessi fisici ai locali e alle aree di trattamento

☑ Sistemi di videosorveglianza e/o allarme antintrusione

☑ Custodia protetta di supporti e documenti cartacei

Sicurezza logica e controllo accessi

☑ Autenticazione informatica con credenziali individuali

☑ Autenticazione a più fattori (MFA) per gli accessi critici

☑ Gestione dei profili di autorizzazione secondo il principio del “need-to-know”

☑ Revisione periodica delle utenze e dei profili di accesso

☑ Policy di gestione delle password (complessità, scadenza, non riutilizzo)

Protezione dei dati

☐ Cifratura dei dati personali «a riposo» (storage)

☑ Cifratura dei dati personali «in transito» (comunicazioni)

☑ Pseudonimizzazione dei dati, ove applicabile

☑ Segmentazione della rete e isolamento degli ambienti critici

Continuità e resilienza

☑ Backup periodici e verificati (test di ripristino)

☑ Piano di disaster recovery / business continuity

☑ Ridondanza dei sistemi critici

Monitoraggio e risposta agli incidenti

☑ Log e monitoraggio degli accessi e delle attività di trattamento

☑ Protezione antimalware/antivirus aggiornata

☑ Aggiornamento e patching periodico di sistemi e applicazioni

☑ Procedura di gestione e risposta agli incidenti di sicurezza

☑ Test periodici di vulnerabilità (vulnerability assessment / penetration test)

Organizzazione e personale

☑ Formazione periodica del personale autorizzato al trattamento

☑ Impegni di riservatezza sottoscritti dal personale autorizzato

☑ Politiche di conservazione e cancellazione sicura dei dati

Ulteriori misure adottate dal Responsabile, a integrazione di quanto sopra (indicazione a cura del Responsabile):

Misure minime richieste (baseline PA, art. 32 GDPR e Misure minime di sicurezza ICT per le PA — AgID Circolare 2/2017): Controllo degli accessi e autenticazione, profili autorizzativi, cifratura ove appropriata, backup e continuità, aggiornamenti e protezione da malware, gestione dei fornitori e formazione del personale. Per le pubbliche amministrazioni le misure sono attuate in coerenza con le Misure minime di sicurezza ICT per le PA (AgID, Circolare 2/2017 del 18/04/2017) e con il Codice dell'Amministrazione Digitale (D.Lgs. 82/2005), secondo il livello di attuazione (minimo, standard, alto) adeguato all'ente.

B. Misure specifiche per la tipologia di trattamento

Ogni trattamento di dati personali e dati sensibili deve avvenire, nel rispetto di quanto previsto dal GDPR e nel rispetto dei principi di ordine generale. In particolare, per ciascun trattamento di competenza il Responsabile esterno del trattamento dovrà fare in modo che: a) i dati siano trattati secondo il principio di liceità, secondo

correttezza. b) i dati dovranno essere trattati soltanto per la finalità prevista in ogni contratto; conservati per un periodo non superiore a quello strettamente necessario per gli scopi del trattamento. Ciascun trattamento dovrà avvenire nei limiti imposti dal principio fondamentale di riservatezza ed il Responsabile esterno è a conoscenza che per la violazione delle disposizioni in materia di trattamento dei dati personali sono previste sanzioni penali (articolo 84 del GDPR) e sanzioni amministrative pecuniarie (articolo 83 del GDPR). Il Responsabile esterno del trattamento si impegna a non divulgare, diffondere, trasmettere e comunicare i dati di proprietà del Titolare del trattamento, nella piena consapevolezza che i dati rimarranno sempre e comunque di proprietà esclusiva del Titolare del trattamento, e pertanto non potranno essere venduti o ceduti, in tutto o in parte, ad altri soggetti. Ai sensi e per gli effetti dell'articolo 28 c. 3 del GDPR, il Titolare del trattamento, ha facoltà di vigilare, anche tramite verifiche periodiche, sulla puntuale osservanza dei compiti e delle istruzioni qui impartite al Responsabile esterno del trattamento che si impegna a cancellare fisicamente dai propri sistemi e dai propri archivi elettronici e cartacei tutti i dati di proprietà del Titolare del trattamento decorsi 60 giorni dalla data di cessazione del contratto di cui sopra.

C. Certificazioni del Responsabile (se presenti)

☐ ISO/IEC 27001 — Gestione Sicurezza Informazioni

☐ ISO/IEC 27017 — Sicurezza servizi cloud

☐ ISO/IEC 27018 — Protezione dati personali nel cloud

☐ ISO 22301 — Business Continuity

☐ SOC 2 Type II

☐ Altre: _____

D. Misure supplementari per dati particolari (art. 9-10 GDPR)

Il Titolare prescrive, in caso di trattamento di categorie particolari di dati, le seguenti misure supplementari:

☐ Cifratura rafforzata dei dati particolari

☐ Accesso riservato a personale specificamente autorizzato e formato

☐ Log dedicato e tracciabilità rafforzata degli accessi

☐ Formazione specifica sul trattamento di categorie particolari

ALLEGATO IV — ELENCO SUB-RESPONSABILI

Il Titolare autorizza sin d'ora il ricorso ai seguenti sub-responsabili del trattamento:

Ragione Sociale	Sede	Attività delegata	Trasf. Extra-UE
_____	_____	_____	☐ Sì ☐ No
_____	_____	_____	☐ Sì ☐ No
_____	_____	_____	☐ Sì ☐ No

Procedura per nuovi sub-responsabili

Per il ricorso a nuovi sub-responsabili non presenti nell'elenco di cui sopra, il Responsabile dovrà:

• comunicare per iscritto al Titolare l'intenzione di ricorrere a un nuovo sub-responsabile con almeno 30 giorni di anticipo;

• fornire le informazioni relative a: identità, sede, attività delegata, misure di sicurezza, eventuali trasferimenti extra-UE;

• attendere l'eventuale opposizione motivata del Titolare entro il termine di 15 giorni;

• in caso di mancata opposizione, procedere alla nomina garantendo l'imposizione degli stessi obblighi contrattuali.

In caso di opposizione motivata, le parti si impegneranno a trovare una soluzione alternativa; qualora non fosse possibile, il Responsabile non potrà ricorrere al sub-responsabile proposto per le attività oggetto del presente contratto.

ALLEGATO V — MODULO DI SEGNALAZIONE DATA BREACH

Modulo da utilizzare dal Responsabile del trattamento per segnalare al Titolare un sospetto data breach. Il modulo, una volta compilato, va trasmesso senza ingiustificato ritardo e comunque entro 24 ore dal momento in cui il Responsabile è venuto a conoscenza della violazione (Clausola «Notifica delle violazioni dei dati»), all'indirizzo PEC/email del Titolare indicato in Allegato I.

Data	_____
Nome e cognome del segnalante	_____
Struttura di afferenza, funzione e dati di contatto del segnalante	_____
Ulteriori soggetti coinvolti nel trattamento	_____

Informazioni sul data breach

1. Momento in cui è avvenuta la violazione	**☐ Il** _____ **☐ Dal** _____ **(ancora in corso) ☐ Dal** ____ **al** ____ **☐ In un tempo non ancora determinato**
2. Modalità di scoperta della violazione	_____
3. Momento di conoscenza della violazione	_____
4. Tipo di violazione	☐ Ransomware ☐ Lettura ☐ Copia ☐ Alterazione ☐ Cancellazione ☐ Furto ☐ Altro: _____
5. Natura della violazione (RID)	☐ Perdita di riservatezza (R) ☐ Perdita di integrità (I) ☐ Perdita di disponibilità (D)
6. Causa della violazione	☐ Azione intenzionale interna ☐ Azione accidentale interna ☐ Azione intenzionale esterna ☐ Azione accidentale esterna ☐ Sconosciuta
7. Sistemi coinvolti	_____
8. Misure di sicurezza in essere	_____
9. Categorie di interessati coinvolti	☐ Dipendenti/Consulenti ☐ Clienti/Contraenti ☐ Fornitori ☐ Minori ☐ Persone vulnerabili ☐ Altro: _____
10. Numero interessati	☐ N. ___ ☐ Circa n. ____ ☐ Non determinabile ☐ Non ancora determinato
11. Categorie di dati oggetto di violazione	☐ Dati anagrafici ☐ Dati di contatto ☐ Dati di accesso/identificazione ☐ Dati di pagamento ☐ Dati relativi alla salute ☐ Dati giudiziari ☐ Altro: _____ ☐ Non ancora determinate
12. Numero registrazioni coinvolte	☐ N. ___ ☐ Circa N. ___ ☐ Non determinabile ☐ Non ancora determinato
13. Descrizione di dettaglio	_____

Probabili conseguenze della violazione

1. Probabili conseguenze per gli interessati	**In corso di valutazione**
2. Potenziale impatto	☐ Perdita del controllo dei dati ☐ Furto o usurpazione d'identità ☐ Frodi ☐ Perdite finanziarie ☐ Pregiudizio alla reputazione ☐ Non ancora definito
3. Gravità del potenziale impatto	☐ Trascurabile ☐ Bassa ☐ Media ☐ Alta ☐ Non ancora definita

Misure adottate a seguito della violazione

1. Misure per porre rimedio alla violazione	_____
2. Misure per prevenire simili violazioni future	_____