

Allegato B

da inserire nella "Documentazione Amministrativa"

Oggetto:

INDAGINE DI MERCATO FINALIZZATA ALL’AFFIDAMENTO DEL SERVIZIO DI BROKERAGGIO ASSICURATIVO E GESTIONE DEI SINISTRI AI SENSI DELL’ART. 50 COMMA 1 LETT. B) DEL D. LGS. 36/2023, PER UN PERIODO DI 6 ANNI, CON POSSIBILITÀ DI PROROGA DI ULTERIORI 6 MESI

Accordo per la designazione del Responsabile (esterno) del trattamento dei dati, ai sensi dell’art. 28 Reg. UE 2016/679, con eventuale ruolo di Amministratore di Sistema.

tra

il **COMUNE DI ATRI** (di seguito, “Titolare”), in persona del Sindaco pro-tempore, con sede legale in Atri (TE) alla Piazza Duchi D'Acquaviva, Cod. fisc. 00076610674,

e

la ditta _____, in persona del legale rappresentante pro-tempore, con sede legale in _____ (____), via _____ n. _____, Cod. Fisc. _____ e P.Iva n. _____ (di seguito denominato “Responsabile”),

PREMESSO CHE

- per “Responsabile” si intende la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che tratta i dati personali per conto del Titolare;
- il Responsabile è fornitore del Titolare in virtù dell’incarico professionale conferito o del contratto di prestazione di servizi in essere, che regola le attività affidate;
- l’espletamento dei servizi comporta un trattamento di dati personali, come definiti all’art. 4 comma 1 GDPR, che il Responsabile deve svolgere per conto del Titolare;
- il G.D.P.R. e il Codice della Privacy impongono una serie di obblighi e vincoli al trattamento di dati personali da parte del Titolare, che anche il Responsabile è tenuto a rispettare;
- per trattamento si intende: qualsiasi operazione o insieme di operazioni, compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto l’interconnessione, la limitazione, la cancellazione o la distruzione;
- si è valutato che il Responsabile possiede l’esperienza, la capacità, l’affidabilità e fornisce idonee garanzie del pieno rispetto delle disposizioni vigenti in materia di trattamento dati, ivi compreso il profilo della sicurezza in relazione alle finalità e modalità delle operazioni di trattamento;

- il Responsabile presenta garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente contratto e garantisca la tutela dei diritti dell'interessato;
- le parti, in relazione a tale nomina, intendono regolare con il presente contratto i loro reciproci rapporti in tema di disciplina del trattamento dei dati personali effettuato dal Responsabile per conto del Titolare;
- nel caso di servizi di amministrazione di sistema affidati in outsourcing il provvedimento del Garante per la Privacy del 27.11.2008 "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" e s.m.i. prevede, tra le altre cose, che il titolare o il responsabile esterno devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema;
- in relazione ai servizi erogati dal Responsabile in virtù dei contratti in essere, la designazione degli amministratori di sistema è effettuata direttamente dal Responsabile che eroga i servizi stessi al Titolare in qualità di Responsabile del trattamento;
- il Responsabile si impegnerà a conservare e a tenere l'elenco dei propri dipendenti preposti all'attività di Amministratore di Sistema costantemente aggiornato e a disposizione del Titolare del trattamento, a semplice richiesta dello stesso.

Tanto premesso si conviene e stipula quanto di seguito riportato.

I. OGGETTO

Oggetto del presente contratto è definire le modalità con le quali il Responsabile si impegna ad effettuare per conto del Titolare le operazioni di trattamento dei dati personali affidate. Nel quadro delle loro relazioni contrattuali, le parti si impegnano al rispetto della normativa vigente relativamente alla protezione dei dati personali e, in particolare, il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (di seguito, "il Regolamento Europeo sulla protezione dei dati personali").

II. DESCRIZIONE DELLE PRESTAZIONI DEL RESPONSABILE

Il Responsabile è autorizzato a eseguire, per conto del Titolare, i trattamenti dei dati personali necessari per fornire il servizio o i servizi seguenti per i quali ha ricevuto incarico professionale:

Materia disciplinata	Trattamento di dati personali trattati per conto del Titolare nell'erogazione delle attività/servizi di cui al (Contratto d'appalto relativo al servizio di tesoreria comunale)		
Tipo di dati personali	<i>(Indicare le tipologie di dati personali alle quali potreste, anche potenzialmente, accedere nell'espletamento delle attività previste da Contratto/Bando/Delibera)</i>		
	Dati comuni: ☒ dati anagrafici ☒ dati di contratto ☒ dati finanziari / bancari ☒ dati reddituali ☒ targhe mezzi ☐ curriculum ☒ dati bancari (c/c, iban,...) ☐ immagini/suoni di videosorveglianza	Dati particolari: ☒ dati generici ☐ dati biometrici ☐ origine etnica, opinioni politiche e religiose ☒ dati relativi alla salute ☐ dati relativi orientamento sessuale ☐ TUTTI	☐ Dati giudiziari

	☐ altri: ☐ TUTTI
Categorie di interessati	<i>(Indicare i soggetti persone fisiche i cui dati personali potrebbero essere oggetto di trattamento nell'espletamento delle attività e servizi previsti dal Contratto/Bando/Delibera)</i> ☒ dipendenti del Comune ☒ utenti dei servizi erogati dal comune ☒ cittadini ☒ dipendenti dei clienti ☒ dipendenti di fornitori ☐ altri:.....
Natura e finalità del trattamento	Adempimento degli obblighi derivanti dal rapporto contrattuale in essere tra le parti in virtù del Contratto d'appalto relativo al servizio di tesoreria comunale.
Durata del trattamento	Fino al termine del contratto, salvo quanto previsto al par. IV, punto 13

III. DURATA DELL'ATTO DI NOMINA

Il presente atto di nomina avrà la stessa durata del contratto principale stipulato tra le parti e ne costituisce parte integrante.

IV. OBBLIGHI DEL RESPONSABILE DI FRONTE AL TITOLARE

Il Responsabile si impegna a:

- 1) **Finalità specifiche:** trattare i dati solo per le finalità sopra specificate e per l'esecuzione delle prestazioni contrattuali.
- 2) **Istruzioni:** trattare i dati conformemente alle istruzioni documentate del Titolare annesse al presente contratto o fornite nel corso del contratto stesso. Se il Responsabile considera che una istruzione costituisca una violazione del Regolamento Europeo sulla protezione dei dati o di tutte le altre disposizioni delle leggi dell'Unione o delle leggi degli stati membri relative alla protezione dei dati, deve informare immediatamente il Titolare. Inoltre, se il Responsabile è tenuto a procedere ad un trasferimento dei dati verso un paese terzo o un'organizzazione internazionale, in virtù delle leggi dell'Unione o delle leggi dello stato membro al quale è sottoposto, deve informare il Titolare di quest'obbligo giuridico prima del trattamento, a meno che le leggi interessate proibiscano una tale informazione per motivi importanti di interesse pubblico.
- 3) **Trasferimento dati all'estero:** garantire che i dati personali saranno conservati in Data Center allocati in Italia o comunque in paesi appartenenti all'Unione Europea o in paesi la cui normativa in ambito privacy sia stata dichiarata equiparabile a quella Europea. In ogni caso il Responsabile dovrà fornire indicazione specifica al Titolare in merito al luogo di conservazione dei dati ed alle garanzie per tale trasferimento. Qualora i dati debbano essere trasferiti in paesi extra UE la cui normativa non è stata dichiarata, da parte delle autorità europee, equiparabile a quella Europea, il Responsabile dovrà dare riscontro preventivo della volontà di effettuare il trasferimento e dovranno essere concordate garanzie adeguate a tale azione in modo preventivo.

- 4) **Garanzia di riservatezza:** garantire la riservatezza dei dati personali trattati nell'ambito del presente contratto.
- 5) **Controllo autorizzazioni:** controllare che le persone autorizzate a trattare i dati personali in virtù del presente contratto:
- si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza;
 - ricevano la formazione necessaria in materia di protezione dei dati personali.
- 6) **Amministratore di Sistema:** conformarsi, nell'eventualità in cui il Responsabile ricopra il ruolo di A.d.S., al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e s.m.i., e ad ogni altro pertinente provvedimento dell'Autorità e, in particolare, designare le persone fisiche preposte all'attività di Amministratore di Sistema con specificazione delle funzioni loro attribuite e conservare e tenere un elenco, costantemente aggiornato e a disposizione del Titolare del trattamento a semplice richiesta dello stesso, favorendo altresì il Titolare del trattamento affinché quest'ultimo adotti sistemi idonei a favorire la registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema;
- 7) **Privacy by Design e by Default:** tenere conto di ogni aspetto del GDPR fin dalla fase di prima progettazione in ogni progetto di trattamento dati che gli venga richiesto dal Titolare e fornire la necessaria consulenza qualora il progetto venga disegnato e realizzato dal Titolare stesso o da terzi incaricati.
- 8) **Sub-Responsabile:** con la sottoscrizione del presente atto, il Titolare autorizza il Responsabile, ad avvalersi di propri sub-responsabili, quali anche terzi fornitori e Società controllate e/o controllanti, per l'erogazione di servizi connessi alla prestazione richiesta riconoscendo ed accettando che ciò possa comportare il trattamento di dati da parte dei medesimi.
- Ai fini della nomina di un sub-responsabile, il Responsabile assicura, tramite un contratto scritto, che:
- a) il sub-responsabile si impegna a trattare i dati del Titolare, in modo lecito, corretto e trasparente, nel rispetto di quanto disposto dal Regolamento UE 2016/679 e delle altre norme in materia di trattamento dei dati personali e nella misura richiesta per adempiere alle obbligazioni al medesimo delegate in conformità con il Contratto;
 - b) il sub-responsabile assuma gli obblighi di cui all'art. 28 del Regolamento UE 2016/679;
 - c) Il Responsabile rimane responsabile nei confronti del Titolare per tutti gli obblighi assunti, anche in relazione alle attività affidate al sub-responsabile.

Al fine di consentire al Titolare un preciso controllo sui suddetti terzi, nonché di provvedere agli adempimenti sussistenti rispetto a tutta la categoria di detti terzi, il Responsabile si impegna a conservare aggiornata la lista di tali soggetti terzi, nonché apposita documentazione da cui risultino gli obblighi assunti da detti soggetti terzi in relazione agli oneri in materia di trattamento dei dati personali precisati nel presente documento, qualora gli stessi trattino dati nell'ambito del Servizio prescelto; il Responsabile si impegna a tenere a disposizione del Titolare e a fornirgli, a semplice richiesta dello stesso, detta documentazione. Il Responsabile si impegna ad informare il Titolare, qualora richiesto, in caso di modifiche di tali soggetti terzi.

- 9) **Esercizio dei diritti degli interessati:** per quanto possibile, il Responsabile deve assistere il Titolare nell'espletamento dei propri obblighi di far seguito alle richieste di esercizio dei diritti delle persone interessate (diritto di accesso, di rettifica, di cancellazione e di opposizione, diritto alla limitazione del trattamento, diritto a trasportare i dati, diritto di non essere oggetto di una decisione individuale automatizzata, compresa la profilazione). Inoltre, il Responsabile deve rispondere, in nome e per conto del Titolare e nei tempi previsti dal Regolamento Europeo sulla protezione dei dati alle domande delle persone interessate qualora queste esercitino i loro diritti, dato che si tratta di dati che sono oggetto delle prestazioni previste dal presente contratto.
- 10) **Notifica della violazione di dati personali:** il Responsabile notifica al Titolare ogni violazione di dati personali nel tempo massimo di 48 ore dopo esserne venuto a conoscenza e per via telefonica e PEC. Tale notifica è accompagnata da ogni documentazione utile per permettere al Titolare, se necessario, di notificare questa violazione all'autorità di controllo competente.
- La notifica deve almeno:
 - descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
 - comunicare il nome e i dati di contatto dell'eventuale Responsabile della protezione dei dati (di seguito "DPO") o di altro punto di contatto presso cui ottenere più informazioni;
 - descrivere le probabili conseguenze della violazione dei dati personali;
 - descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
 - Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
 - Previo accordo con il Titolare, il Responsabile comunica, in nome e per conto del Titolare, la violazione di dati personali alla persona interessata al più presto, qualora essa sia suscettibile di generare un rischio elevato per i diritti e le libertà di una persona fisica.
 - La comunicazione alla persona interessata descrive, in termini chiari e semplici, la natura della violazione di dati personali e deve perlomeno:
 - descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
 - comunicare il nome e i dati di contatto dell'eventuale DPO o di altro punto di contatto presso cui ottenere più informazioni;
 - descrivere le probabili conseguenze della violazione dei dati personali;
 - descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
- 11) **Collaborazione:** assistenza del Responsabile nell'attuazione degli obblighi del Titolare. Pertanto:

- il Responsabile assiste il Titolare nella realizzazione di analisi d'impatto relative alla protezione dei dati, conformemente all'Art. 35;
- il Responsabile assiste il Titolare nella consultazione preventiva dell'autorità di controllo, prevista dall'Art. 36;
- il Responsabile dovrà rispondere tempestivamente ad ogni e qualsiasi richiesta del Titolare, di eventuali soggetti interessati e dell'Autorità Garante per la protezione dei dati personali o altre autorità di controllo e, in ogni caso, consentire prontamente al Titolare anche tramite propri incaricati, e all'autorità di controllo ed ai suoi rappresentanti tutti i controlli e gli accessi che dovessero ritenersi opportuni e/o necessari.

12) **Misure di sicurezza:** il Responsabile dovrà garantire l'adozione, di misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, che possono comprendere:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

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

Il Responsabile, in relazione alle possibili variazioni nelle operazioni o nei dati trattati, adotta quelle misure urgenti idonee a salvaguardare la riservatezza, l'integrità, l'aggiornamento e la disponibilità dei dati oggetto delle operazioni di trattamento.

A tal fine, il Responsabile deve dotarsi di misure di sicurezza rapportata a:

- le conoscenze acquisite in base al progresso tecnico;
- la natura dei dati;
- le specifiche caratteristiche delle operazioni di trattamento.

Il Responsabile deve assicurarsi che tali misure di sicurezza siano adeguate in modo da ridurre al minimo i rischi di:

- distruzione o perdita intenzionale o accidentale dei dati;
- accesso non autorizzato;
- trattamento non consentito;
- trattamento non conforme alla finalità delle Operazioni dei Trattamenti;
- integrità dei dati.

Il Responsabile, qualora necessario, deve realizzare tempestivamente, dandone immediata comunicazione al Titolare, quegli interventi di urgenza atti a conseguire gli obiettivi di salvaguardia della riservatezza, dell'integrità e della completezza dei dati oggetto delle operazioni di trattamento, quando l'imprevedibilità degli eventi non abbia consentito la ordinaria

pianificazione degli stessi. Per dimostrare la conformità ai requisiti di cui all'art. 32 "GDPR" può essere utilizzato come elemento valido l'adesione ad un codice di condotta approvato o a un meccanismo di certificazione approvato (art.li 40 e 42 "GDPR")

- 13) **Disposizione dei dati al termine delle prestazioni contrattuali:** al termine della prestazione dei servizi relativi al trattamento di questi dati, il Responsabile s'impegna a restituire tutti i dati personali al Titolare oppure se richiesto a distruggere tutte le copie dei dati esistenti nei propri sistemi e a documentarlo per iscritto. Fatti salvi i diritti al trattamento che si renderanno necessari per adempimenti di obblighi legge o contrattuali, ovvero per la pendenza di eventuali contenziosi.
- 14) **DPO/RPD - Responsabile della protezione dei dati:** il Responsabile comunica al Titolare il nome ed i dati del proprio DPO, qualora ne abbia designato uno conformemente all'Art. 37 del Regolamento Europeo sulla protezione dei dati.
- 15) **Registro delle categorie di attività di trattamento:** il Responsabile dichiara di tenere per iscritto, se dovuto, un registro di tutte le categorie di attività di trattamento effettuate per conto del Titolare e che comprendono:
 - il nome ed i dati del Titolare per conto del quale lui tratta, degli eventuali responsabili e, se applicabili, del DPO;
 - le categorie di trattamenti effettuati per conto del Titolare;
 - se applicabili, i trasferimenti di dati personali verso un paese terzo o ad una organizzazione internazionale e, nel caso di trasferimenti previsti dall'Art. 49, paragrafo 1, secondo comma del Regolamento Europeo sulla protezione dei dati, i documenti che attestano l'esistenza di opportune garanzie;
 - per quanto possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative, ivi compresi, fra gli altri, secondo le necessità:
 - la pseudonimizzazione e la numerazione dei dati personali;
 - i mezzi che permettono di garantire la segretezza, l'integrità, la disponibilità e la resilienza costanti dei sistemi e dei servizi di trattamento;
 - i mezzi che permettono di ristabilire la disponibilità dei dati personali e l'accesso a questi nei tempi appropriati in caso di incidente fisico o tecnico;
 - una procedura che mira a testare, ad analizzare ed a valutare regolarmente l'efficacia delle misure tecniche ed organizzative per assicurare la sicurezza del trattamento.
- 16) **Evidenza della documentazione:** il Responsabile mette a disposizione del Titolare la documentazione necessaria per dimostrare il rispetto di tutti gli obblighi e per permettere la realizzazione di revisioni, comprese le ispezioni, da parte del Titolare o di un altro revisore che lui ha incaricato, le cui spese saranno ad esclusivo carico del Titolare.

V. OBBLIGHI DEL TITOLARE DI FRONTE AL RESPONSABILE

Il Titolare s'impegna a:

- 1) fornire al Responsabile i dati previsti al punto II delle presenti clausole;
- 2) documentare per iscritto tutte le istruzioni riguardanti il trattamento dei dati da parte del Responsabile;
- 3) vigilare, in anticipo e durante la durata di tutto il trattamento, sul rispetto degli obblighi previsti dal Regolamento Europeo sulla protezione dei dati da parte del Responsabile;
- 4) supervisionare il trattamento, comprese le revisioni e le ispezioni da parte del Responsabile.

VI. DISPOSIZIONI FINALI

Con l'occasione, si ricorda l'importanza delle prescrizioni di legge in materia di trattamento dei dati personali, nonché il fatto che la violazione di dette normative può comportare responsabilità sia civili che penali per il Titolare e per il Responsabile, nonché l'applicazione di sanzioni amministrative, ai sensi degli Artt. 83 e 84 del Regolamento UE 679/2016. Resta inteso che la nomina quale Responsabile, come prevista e disciplinata nel presente contratto, potrà essere liberamente revocata in qualsiasi momento dal Titolare in caso di mancata adozione delle misure condivise. Inoltre, il mancato rispetto delle presenti condizioni, che sono legate all'adempimento di prescrizioni normative, potrà essere causa di risoluzione del contratto per inadempimento. Resta altresì inteso che nessun ulteriore compenso o rimborso spetterà per l'assunzione della funzione di Responsabile dei dati personali di cui alla presente nomina.

Il Responsabile

*** *firma digitale* ***