MANIFESTAZIONE DI INTERESSE PER L'AFFIDAMENTO DEL SERVIZIO DI CONSULENZA E BROKERAGGIO ASSICURATIVO PER LA DURATA DI ANNI 5 DAL 1/1/2023 AL 31/12/2027 - CIG Z9937B654C

Prot. N. _____ del _____

ATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI in applicazione dell'art. 28, REG. (UE) 2016/679

VISTI

- il Regolamento Generale sulla Protezione dei Dati ("RGPD") del Parlamento Europeo e del Consiglio del 27 aprile 2016 n. 679;
- il Codice privacy, D. Lgs. n. 196/2003, integrato con le modifiche introdotte dal Decreto Legislativo 10 agosto 2018, n.101, relativo all'adeguamento della normativa nazionale alle disposizioni del RGPD;
- l'art. 4, par. 1, n. 8, RGPD (il «Responsabile del trattamento» come «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento»);
- l'art. 28, par. 1, RGPD («qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato»);
- l'art. 28, par. 2, RGPD («il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche»);
- l'art. 28, par. 3, RGPD («I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento: a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico; b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza; c) adotti tutte le misure richieste ai sensi dell'articolo 32; d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento; e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III; f) assista il titolare del trattamento nel garantire il

rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento; g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati»);

- l'art. 28, par. 4, RGPD («quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile 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»);
- la Decisione di esecuzione (UE) 2021/915 della Commissione UE del 4 giugno 2021, relativa alle Clausole Contrattuali Tipo ("CCT") tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, del RGPD;
- le vigenti prescrizioni con riguardo all'attribuzione delle funzioni di "Amministratore di Sistema" e il Provvedimento del Garante "Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema" del 27/11/2008, pubblicato in G.U. n.300 del 24 dicembre 2008 e successive modifiche, richiede particolari cautele in relazione all'affidamento di mansioni configurabili come Amministratore di Sistema, con indicazione analitica degli ambiti di operatività consentiti; in particolare il punto 3-bis del suddetto Provvedimento dispone che "l'eventuale attribuzione al Responsabile del compito di dare attuazione alle prescrizioni impartite avvenga nell'ambito della designazione del Responsabile da parte del Titolare o anche tramite opportune clausole contrattuali";

PREMESSO CHE

- il **Comune di Quarrata** è Titolare del trattamento dei dati personali ai sensi dell'art. 4, punto 7, RGPD;
- con D.D. del …….. e contestuali allegati, il cui contenuto si intende integralmente riportato e trascritto nel presente atto, viene affidato il servizio professionale di consulenza e brokeraggio assicurativo, attività che comporta o può comportare il trattamento di dati personali;
- la **……**, nell'ambito delle attività e dei servizi affidati, di cui al contratto richiamato, ha i requisiti di esperienza, capacità ed affidabilità idonei a garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza;

con il presente atto, al fine di affidare il trattamento dei dati personali rientrante nelle attività richiamate,

il Dirigente dell'Area Servizi alla Persona e di Supporto Amministrativo, dott. Luigi Guerrera

DESIGNATO all'assolvimento di compiti e funzioni in materia di protezione dati personali, pur sotto l'autorità del

TITOLARE DEL TRATTAMENTO DEI DATI (anche semplicemente "Titolare")

COMUNE DI Quarrata con sede legale in via Vittorio Veneto 2, cod. fisc. 00146470471, e-mail: attivitanegoziali@comune.quarrata.pistoia.it, PEC comune.quarrata@postacert.toscana.it

NOMINA

RESPONSABILE DEL TRATTAMENTO DEI DATI (anche semplicemente "Responsabile")

La **……,** con sede legale in Via ……., ……. (P.IVA …….), e-mail/PEC ……,
in persona del legale rappresentante pro tempore, dott./dott.ssa ……..,

ART. 1 – SCOPO E AMBITO DI APPLICAZIONE

1.1. Scopo del presente atto di nomina è garantire il rispetto dell'articolo 28, RGPD; le Parti, in virtù dell'accordo contrattuale e dei documenti ad esso allegati, con la sottoscrizione del presente atto di nomina, intendono disciplinare il trattamento dei dati personali da parte del Responsabile per conto del Titolare, specificando l'oggetto, la durata, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti delle Parti.

1.2 Il Titolare ha affidato al Responsabile con D.D. del ……. e contestuali Allegati, il servizio professionale di consulenza e brokeraggio assicurativo dell'Ente.

1.3 Il Titolare, i cui obblighi restano impregiudicati da questo atto di nomina, intende affidare al Responsabile, in conformità alle istruzioni da egli prescritte ed alle clausole del presente atto di nomina sul trattamento dei dati personali, le attività di trattamento di dati personali relative ai servizi pocanzi descritti.

1.4 Il Titolare, pertanto, impegna il Responsabile, che con la sottoscrizione accetta, come "Responsabile del trattamento" dei dati effettuato con strumenti elettronici o comunque automatizzati o con strumenti diversi, per l'ambito di attribuzioni, funzioni e competenze come specificato dall'incarico in essere.

1.5 Il Responsabile ha il compito e la responsabilità di adempiere a tutto quanto necessario per il rispetto delle disposizioni vigenti in materia e di osservare scrupolosamente quanto in essa previsto, nonché le seguenti istruzioni impartite dal Titolare.

1.6 Il Responsabile non ha diritto ad alcun compenso specifico ulteriore per l'esecuzione delle attività descritte nel presente atto di nomina, in quanto svolte nell'ambito dell'incarico in essere, per il quale è stata già definita l'intera valutazione economica del rapporto contrattuale.

ART. 2 – DEFINIZIONI E INTERPRETAZIONE

2.1 Il presente atto di nomina va letto e interpretato alla luce delle disposizioni del RGPD. Esse non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal RGPD. Per qualsiasi dubbio sulle definizioni, si rinvia all'art. 4 del RGPD.

ART. 3 - DESCRIZIONE DEL TRATTAMENTO

3.1 I dettagli del trattamento sono i seguenti:

1. **Finalità del trattamento.** I dati relativi alle attività di trattamento di cui al precedente art. 1.2 sono trattati per le sole finalità relative al servizio professionale di consulenza e brokeraggio assicurativo dell'Ente. Tra le diverse attività offerte dal Responsabile, alcune comportano un trattamento di dati personali, quali, ad esempio:
   - analisi delle polizze assicurative esistenti;
   - valutazione delle offerte di gara e partecipazione alla commissione di gara;
   - assistenza nella gestione tecnica ed amministrativa dei contratti e aggiornamento dei contratti stessi in relazione alle esigenze assicurative degli enti;
   - collaborazione nella gestione e nell'esecuzione delle polizze assicurative in essere;
   - assistenza nella gestione sinistri attivi e passivi;
   - collaborazione nella gestione dei sinistri pregressi all'assunzione dell'incarico;
   - ricerca di polizze assicurative, se richieste dal Comune;
   - supporto formativo del personale dell'Ente.

1. **Natura del trattamento.** Le attività di trattamento di cui al precedente art. 1.2 consistono nelle operazioni di raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, limitazione, cancellazione o distruzione, elaborazione ed uso per fini statistici con esclusivo trattamento dei dati in forma anonima, comunicazione mediante trasmissione (a soggetti pubblici che ne facciano richiesta per il proseguimento dei propri fini istituzionali e se prescritto dalla normativa vigente comunitaria e nazionale), raffronto o interconnessione.
2. **Categorie di dati personali trattati.** I dati personali trattati sono sia dati comuni, che di tipo particolare, quelli previsti, cioè, dagli art. 9 e 10, RGPD, il cui trattamento deve avvenire nel rispetto degli artt. 5 e 32, RGPD (si veda l'Allegato 1 al presente atto di nomina), garantendo il rispetto dei principi di liceità, correttezza, trasparenza, limitazione delle finalità e della conservazione, minimizzazione dei dati, esattezza, integrità e riservatezza; se del caso, per tali dati vengono adottate misure di sicurezza supplementari;
3. **Categorie di interessati.** Le attività di trattamento di cui al precedente art. 1.2 e i relativi dati trattati interessano dipendenti e collaboratori dell'Ente, cittadini residenti e non residenti, fornitori dell'Ente o comunque soggetti che partecipano a procedure di gara, concessioni, affidamenti, ecc.
4. **Durata del trattamento.** I dati verranno conservati per il tempo strettamente necessario al raggiungimento della finalità del trattamento e, successivamente, soltanto ove richiesto dalla normativa di settore.

ART. 4 - OBBLIGHI DEL TITOLARE

Il Titolare del trattamento persegue le seguenti finalità:

Conformità: il Titolare è responsabile per la valutazione della legittimità del trattamento dei dati e nel garantire i diritti degli interessati coinvolti;

Sicurezza: le misure tecniche e organizzative adottate devono garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento e dalla natura dei dati da proteggere, tenendo conto dello stato dell'arte e del costo della loro attuazione;

Istruzioni: il Titolare potrà rilasciare istruzioni scritte riguardanti lo scopo e la procedura del trattamento dei dati, se del caso, amplificando, specificando e modificando le clausole di questo atto di nomina; le istruzioni orali saranno immediatamente confermate per iscritto e saranno parte integrante e sostanziale del presente atto di nomina.

ART. 5 - OBBLIGHI DEL RESPONSABILE

5.1 Al Responsabile sono demandati i seguenti obblighi.

a) **Competenza.** Il Responsabile deve possedere sufficienti conoscenze specialistiche nonché affidabilità e risorse per attuare misure tecniche e organizzative che soddisfino i requisiti del RGPD.
b) **Rispetto delle istruzioni del Titolare.** Il responsabile del trattamento tratta i dati personali limitatamente alle attività strettamente necessarie per l'espletamento delle funzioni affidate, in conformità con il Contratto e con il presente atto di nomina. Qualora il responsabile non fosse in grado di fornire tale conformità per qualsiasi motivo, informerà tempestivamente il Titolare che ha il diritto di sospendere il trattamento dei dati e/o valutare l'adozione dei provvedimenti inerenti al Contratto espressamente previsti dalle norme civilistiche nazionali.
c) **Conformità alla legge.** Il Responsabile, qualora ritenga che una modifica legislativa possa avere un sostanziale effetto negativo sulle garanzie e gli obblighi del Contratto e/ o del presente atto di nomina, ne darà prontamente notizia al Titolare che avrà il diritto di sospendere l'elaborazione dei dati e/o di risolvere il Contratto nell'ambito delle attività/prestazioni professionali o dei servizi affidati e quindi il presente atto di nomina.
d) **Limitazione delle finalità.** Il Responsabile tratta i dati personali soltanto per le finalità specifiche del trattamento di cui alla lettera a) del precedente art. 3.1, salvo ulteriori istruzioni del Titolare.
e) **Durata del trattamento dei dati personali.** Il Responsabile tratta i dati personali soltanto per la durata specificata nella lettera e) del precedente art. 3.1, salvo ulteriori istruzioni del Titolare.

f) **Trasferimenti internazionali.** Qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del responsabile del trattamento è effettuato soltanto su istruzione documentata del titolare del trattamento o per adempiere a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il Responsabile, e nel rispetto del capo V del RGPD. Il Titolare conviene che, qualora il Responsabile ricorra a un Sub-responsabile del trattamento conformemente all'art. 8 del presente atto di nomina, per l'esecuzione di specifiche attività di trattamento (per conto del Titolare) e tali attività di trattamento comportino il trasferimento di dati personali ai sensi del capo V del RGPD, il Responsabile e il Sub-responsabile possono garantire il rispetto del capo V del RGPD utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, RGPD, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte (Decisione di esecuzione (UE) 2021/914 della Commissione, 4 giugno 2021, relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi a norma del RGPD).

g) **Sicurezza del trattamento.** Tenuto conto del rischio per i diritti e le libertà degli interessati, il Responsabile, in applicazione del concetto di *accountability*, adotterà misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio. Le misure richiamate comprendono, tra l'altro, le misure e le valutazioni di cui all'art. 32[1] del RGPD; tali misure, che devono necessariamente garantire i requisiti di disponibilità, riservatezza e integrità dei dati personali, devono essere periodicamente aggiornate sulla base del progresso tecnologico. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati. Si veda, in tal senso, l'Allegato 1 al presente atto di nomina. Nei casi in cui si evidenziasse una non piena corrispondenza tra la tipologia di trattamento prevista dal Contratto e le misure di sicurezza, il Responsabile si impegna a comunicarlo per iscritto al Titolare, fornendo al medesimo l'effettuata analisi del rischio e indicando le misure di sicurezza ritenute adeguate. Il Responsabile concede l'accesso ai dati personali oggetto di trattamento ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Il Responsabile garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza. Se il trattamento riguarda dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati («categorie particolari di dati personali»), il Responsabile applica limitazioni specifiche e/o garanzie supplementari.

h) **Pronta notifica.**

---

1 **Art. 32 RGPD "Sicurezza del trattamento"**

1. 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, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

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

1. 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.

2. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'art. 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

3. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

i. il Responsabile informerà tempestivamente il Titolare del trattamento di qualsiasi richiesta legalmente vincolante da parte di un'autorità giudiziaria;
ii. il Responsabile, in caso di sospetta o effettiva violazione dati personali (*data breach),* dovrà darne comunicazione al Titolare del trattamento senza ritardo e comunque non oltre 24 ore dal momento in cui il Responsabile ne è venuto a conoscenza, anche se durante le festività, mediante la compilazione del modulo ad hoc (Allegato 2), nonché rimanere a piena disposizione del Titolare, in particolare collaborando attivamente con il medesimo nella raccolta documentale e in tutte le attività, anche di indagine, connesse alla valutazione e all'effettuazione dell'eventuale notifica al Garante *privacy* e ai soggetti interessati, ai sensi degli artt. 33 e 34 RGPD;
iii. qualsiasi richiesta ricevuta direttamente dagli interessati per poterne dare riscontro nei tempi previsti dal RGPD, considerato che il legislatore europeo impone al Titolare di fornire risposta agli interessati entro 30 giorni o, in casi particolari, tale arco temporale si estende di 60 giorni;
iv. qualsiasi istruzione scritta ricevuta dal Titolare che, secondo il parere del Responsabile, sia in violazione del RGPD e/o dei doveri di cui al presente atto di nomina.

i) Dimostrazione di conformità, ispezioni, audit. Il Responsabile rende disponibili al Titolare, volontariamente o su richiesta dello stesso, tutte le informazioni necessarie (comprese eventuali certificazioni), a dimostrare la conformità agli obblighi stabiliti nel presente atto di nomina e, su richiesta del Titolare, a presentare le proprie procedure di trattamento dei dati per la revisione delle stesse. Il Responsabile consentirà e contribuirà a tali verifiche, comprese le ispezioni, svolte dal Titolare o da un organismo di controllo da questi nominato, con un preavviso ragionevole. Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente atto di nomina e consentire/contribuire alle attività di revisione, comprese ispezioni o audit, svolti dal Titolare o da un altro soggetto da questi incaricato, informando immediatamente il Titolare qualora, a suo parere, un'istruzione violi il RGPD o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati. Le risultanze dell'audit saranno discusse in buona fede tra le Parti e il Responsabile si impegna sin d'ora ad attuare gli eventuali cambiamenti ritenuti necessari dal Titolare in seguito all'audit, al fine di garantire la conformità alla normativa vigente e al Contratto.

j) Cooperazione con il Titolare per le indicazioni diramate dall'Autorità di Controllo. Il Responsabile collabora con il Titolare per il rispetto di eventuali ordini emessi dall'Autorità di Controllo o dalle Autorità Giudiziarie in relazione al trattamento dei dati, nonché evadere tempestivamente e adeguatamente le richieste del Titolare in ordine alle indicazioni e alle linee guida dell'Autorità di Controllo in materia di protezione dei dati personali.

k) Cooperazione con il Titolare per la valutazione di impatto (DPIA). Il Responsabile, ove ne ricorrano i presupposti previsti dalla normativa in materia di protezione dei dati personali e dai Provvedimenti del Garante *ratione materiae*, deve collaborare con il Titolare per il rispetto dell'art. 35, RGPD, fornendo, qualora si renda necessario, ogni elemento utile all'effettuazione, da parte del Titolare, della valutazione di impatto sulla protezione dei dati nonché ogni collaborazione nell'effettuazione della eventuale consultazione preventiva al Garante per la protezione dei dati personali ai sensi dell'art. 36, RGPD.

l) Cooperazione nel corso delle ispezioni del Garante o dell'Autorità Giudiziaria. Il Responsabile si impegna a collaborare col Titolare, in buona fede e nei limiti delle rispettive competenze, in caso di ispezioni del Garante o dell'Autorità Giudiziaria. Il Responsabile è altresì tenuto ad informare tempestivamente il Titolare in merito ad ispezioni eseguite da parte del Garante *privacy* o dell'Autorità Giudiziaria con riferimento ai Trattamenti dei dati personali. Il Responsabile è tenuto, altresì, a fornire, secondo le modalità indicate dal Titolare, i dati e le informazioni necessarie per consentire allo stesso di svolgere una tempestiva difesa e relative al trattamento dei dati personali in eventuali procedure instaurate davanti al Garante o all'Autorità Giudiziaria.

m) Cooperazione con il Responsabile della Protezione dei Dati Personali. Il Responsabile si impegna a collaborare, su richiesta, con il Responsabile della Protezione dei Dati Personali nominato dal Titolare, nell'esecuzione dei suoi compiti.

n) Informativa. Ogni qualvolta si raccolgano direttamente dati personali, il Responsabile provvede a che venga fornita l'informativa[2] ai soggetti interessati.

o) Soggetti autorizzati dal Responsabile. Il Responsabile è tenuto, nella propria organizzazione, a individuare, nominare e formare gli autorizzati del trattamento per i dati che gli sono state affidati e fornirgli le istruzioni adeguate, vigilando sul rispetto delle stesse. È tenuto, altresì, ad assegnare agli autorizzati del trattamento, a seconda dei compiti attribuiti ad ognuno e laddove sia tecnicamente possibile, le credenziali di autenticazione che permettano di svolgere solo le operazioni di propria competenza, nonché le dovute responsabilità per le aree ad accesso controllato, ove presenti, garantendo che le persone autorizzate al trattamento dei dati si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

ART. 6 - PRINCIPI GENERALI DA OSSERVARE

6.1 Ogni trattamento di dati personali deve avvenire nel rispetto dei seguenti principi di ordine generale.

6.2 Ai sensi dell'art. 5, RGPD, rubricato "Principi applicabili al trattamento dei dati personali", per ciascun trattamento di propria competenza, il Responsabile deve fare in modo che siano sempre rispettati i seguenti presupposti:

- i dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- i dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che il trattamento non sia incompatibile con tali finalità;
- i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- i dati devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare e rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

---

2 **ART. 13 "Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato"**

1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:
   - ♋① l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
   - ♌① i dati di contatto del responsabile della protezione dei dati, ove applicabile;
   - ♍① le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
   - ♎① qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
   - ♏① gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
   - ♐① ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:
   - α) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
   - β) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
   - χ) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
   - δ) il diritto di proporre reclamo a un'autorità di controllo;
   - ε) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
   - φ) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

3. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.

4. I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.

- i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- i dati devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

6.3 Ai sensi dell'art. 6, RGPD, rubricato "Liceità del trattamento", il Responsabile deve tenere conto che il trattamento è lecito solo se e nella misura in cui venga rispettata la base giuridica individuata.

ART. 7 – NOMINA DEL RESPONSABILE PROTEZIONE DATI (RPD-DPO)

7.1 Il Responsabile è tenuto a provvedere, ove ne ricorrano i presupposti previsti dalla normativa in materia di protezione dei dati personali e dai Provvedimenti del Garante *ratione materiae*, alla nomina di un proprio Responsabile della Protezione dei Dati personali (RPD-DPO)[3], quale figura di raccordo per le questioni attinenti alla protezione dei dati personali con il Titolare e comunicare il nominativo e i dati di contatto del Responsabile della Protezione dei Dati personali al Titolare.

ART. 8 - ESECUZIONE DI SPECIFICHE ATTIVITÀ DI TRATTAMENTO (SUB-RESPONSABILE)

8.1 Il Responsabile del trattamento può affidare o ricorrere a un altro responsabile (c.d. "Sub-Responsabile del trattamento") le operazioni di trattamento dei dati di cui al presente atto di nomina, soltanto previa autorizzazione scritta del Titolare del trattamento.

8.2 In questo caso, il Responsabile dovrà informare il Titolare, mediante una comunicazione scritta, di eventuali modifiche comportanti la nomina, l'aggiunta o la sostituzione di eventuali Sub-Responsabili del trattamento e, in particolare, dovrà indicare chiaramente le attività di trattamento delegate, l'identità e i dati di contatto del Sub-Responsabile del trattamento ed i contenuti del contratto sottoscritto con quest'ultimo, dandone comunicazione, entro 15 giorni dalla data di sottoscrizione, al Titolare che ha facoltà di opporsi a tali modifiche entro 15 giorni dal ricevimento di tale comunicazione. Il Titolare dovrà quindi sommariamente indicare al Responsabile le ragioni della sua opposizione.

8.3 Nel caso in cui il Responsabile del trattamento ricorra a un Sub-responsabile, su tale Sub-responsabile sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti in questo atto di nomina, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del RGPD. Su richiesta del Titolare, il Responsabile fornisce copia del contratto stipulato con il Sub-responsabile e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il Responsabile può espungere informazioni dal contratto prima di trasmetterne una copia.

8.4 In caso di autorizzazione scritta generale, il Responsabile del trattamento informerà il Titolare del trattamento di eventuali modifiche relative all'aggiunta o alla sostituzione di altri Responsabili del trattamento, dando così al Titolare la possibilità di opporsi a tali modifiche.

8.5 In ogni caso, le Parti convengono che, nel caso di nomina di un Sub-Responsabile, prima che il Sub-Responsabile cominci a svolgere le attività di trattamento dei dati personali delegategli, il Responsabile dovrà svolgere un'accurata *due diligence* volta ad assicurarsi che il Sub-Responsabile del trattamento sia in grado di garantire il livello di protezione dei dati personali richiesto dal Contratto e dal presente atto di nomina.

8.6 Qualora il Sub-Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile nominato con il presente atto di nomina conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del Sub-Responsabile. Il Responsabile notifica al Titolare qualunque inadempimento, da parte del Sub-responsabile, degli obblighi contrattuali.

8.7 Il Responsabile concorda con il Sub-responsabile una clausola del terzo beneficiario secondo la quale, qualora il Responsabile sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, il Titolare ha diritto di risolvere il contratto con il Sub-responsabile e di imporre a quest'ultimo di cancellare o restituire i dati personali.

3 Si vedano gli artt. 37-39, RGPD

ART. 9 - DIRITTI E RICHIESTE DEGLI INTERESSATI

9.1 Il Responsabile del trattamento comunica ogni informazione utile al fine di aiutare il Titolare a rispettare i diritti degli Interessati, ai sensi degli artt. 15-22 RGPD[4] e nei tempi stabiliti dal RGPD. Il Responsabile assiste il Titolare con adeguate misure tecniche e organizzative per l'adempimento dell'obbligo del Titolare di rispondere alle richieste di esercizio dei diritti degli Interessati. In caso di esercizio dei predetti diritti, il Responsabile darà immediata comunicazione scritta, in adesione a quanto espressamente previsto dall'art. 12, par. 3, RGPD, al Titolare, allegando una copia della richiesta dell'Interessato. Il Responsabile non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dal Titolare.

9.2 Oltre all'obbligo di assistere il Titolare in conformità dell'art. 9.1, il Responsabile assiste il Titolare anche nel garantire il rispetto dei seguenti obblighi, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del Responsabile:

- qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'obbligo di effettuare una valutazione del rischio dei trattamenti previsti sulla protezione dei dati personali e prevedere misure in grado di mitigare tali rischi;
- l'obbligo di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il Titolare qualora il Responsabile venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;
- gli obblighi di cui all'articolo 32, RGPD (si veda l'Allegato 1 al presente atto di nomina).

ART. 10 – AMMINISTRATORE DI SISTEMA

10.1 Il Titolare, ove ne ricorrano i presupposti previsti dalla normativa in materia di protezione dei dati personali e dai Provvedimenti del Garante *ratione materiae*, attribuisce al Responsabile il compito di dare attuazione alle prescrizioni di cui al Provvedimento generale del Garante *privacy* del 27 novembre 2008 e s.m.i., relativo alle "Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema", in particolare con riferimento alle lettere d), e) ed f) dell'art. 10.2.

10.2 Il Responsabile del trattamento, all'esito della nomina dell'Amministratore di sistema, deve dare comunicazione dei dati di contatto dello/degli stesso/i al Titolare del trattamento.

ART. 11 - COMUNICAZIONE DEI DATI PERSONALI A TERZI

11.1 Il Responsabile si asterrà dal comunicare dati personali oggetto del trattamento a terzi senza il preventivo consenso, rilasciato per iscritto, dal Titolare.

ART. 12 - RESPONSABILITÀ IN CASO DI VIOLAZIONE DEI DATI

12.1 Come espressamente previsto dall'art. 5, lettera h) del presente atto di nomina, in caso di violazione dei dati personali, il Responsabile del trattamento informa il Titolare del trattamento senza ingiustificato ritardo, e comunque entro 24 ore dall'avvenuta conoscenza della violazione, in modo che quest'ultimo possa provvedere, a notificare la violazione al Garante per la Protezione dei Dati Personali, senza ingiustificato ritardo[5] e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora il Responsabile non comunichi al Titolare entro 24 ore l'avvenuta violazione dei dati, è tenuto a motivare tale ritardo.

---

4 *Art. 15 RGPD "Diritto di accesso dell'interessato", art. 16 "Diritto di rettifica", art. 17 "Diritto alla cancellazione («diritto all'oblio»), art. 18 "Diritto di limitazione di trattamento", art. 19 "Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento", art. 20 "Diritto alla portabilità dei dati", art. 21 "Diritto di opposizione", art. 22 "Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione"*

5 **Art. 33 "Notifica di una violazione dei dati personali all'autorità di controllo"**

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

12.2 Ciascun Responsabile deve, inoltre, essere a conoscenza del fatto che per la violazione delle disposizioni in materia di trattamento dei dati personali sono previste sanzioni, secondo il disposto dell'art. 83, RGPD, cui si rinvia.

ART. 13 - CESSAZIONE E SUCCESSIVE OBBLIGAZIONI, RISOLUZIONE

13.1 Questo atto di nomina diventerà effettivo dal momento della firma delle Parti fino allo spirare dei termini del Contratto di "attività/prestazioni professionali e servizi" o al termine del trattamento dei dati personali per cause estintive del Contratto.

13.2 Alla cessazione del Contratto principale o del trattamento dei dati, il Responsabile dovrà restituire entro 30 giorni le relative copie oggetto del trattamento e ogni altra informazione, di proprietà del Titolare e rilevanti sotto il profilo della protezione dei dati personali, in un formato comune, leggibile, tale da poter tener conto del progresso tecnologico, favorendo la consultazione e il riutilizzo dei dati in capo al Titolare. Inoltre, dovrà, su espressa e precisa indicazione del Titolare, cancellare i dati personali. Il Responsabile garantirà la riservatezza dei dati e si impegnerà a non procedere più al loro trattamento, garantendo, a conclusione dell'atto di nomina, la cancellazione sicura e certificata dei dati personali, dandone espressa comunicazione al Titolare. Finché i dati non sono cancellati o restituiti, il responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.

13.3 Fatte salve le disposizioni del RGPD, qualora il Responsabile violi gli obblighi che gli incombono a norma del presente atto di nomina, il Titolare può dare istruzione al Responsabile di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le disposizioni del presente atto di nomina o non sia risolto il contratto. Il Responsabile informa prontamente il titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole.

13.4 Il Titolare ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali conformemente al presente atto di nomina qualora:

a) il trattamento dei dati personali da parte del Responsabile sia stato sospeso dal Titolare per violazione delle disposizioni del presente atto di nomina e il rispetto delle stesse non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;
b) il Responsabile violi in modo sostanziale o persistente le stesse disposizioni o gli obblighi che gli incombono a norma del RGPD;
c) il Responsabile non rispetti una decisione vincolante di un organo giurisdizionale competente o della o delle autorità di controllo competenti per quanto riguarda i suoi obblighi in conformità delle disposizioni del presente atto di nomina o del RGPD.

13.5 Il Responsabile ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle disposizioni del presente atto di nomina qualora, dopo aver informato il titolare del trattamento che le sue istruzioni violano i requisiti giuridici applicabili, il Titolare insista sul rispetto delle istruzioni.

ART. 14 - LEGGE APPLICABILE E FORO COMPETENTE

14.1 Il presente atto di nomina, salvo quanto diversamente ivi previsto, in linea con il RGPD, è regolato dalle leggi della giurisdizione del Titolare.

14.2 La sede esclusiva per tutte le controversie derivanti da o in connessione con questo atto di nomina è il luogo di stabilimento del Titolare, fatto salvo il diritto di quest'ultimo di presentare un'azione giudiziaria contro il Responsabile, di fronte a qualsiasi altro tribunale ritenuto competente.

ART. 15 - NORME FINALI

15.1 Salvo quanto previsto per il conferimento o la modifica delle istruzioni da parte del Titolare al Responsabile, il presente atto di nomina disciplina l'intero accordo tra le Parti in relazione al suo oggetto. Per tutto quanto non espressamente previsto nel presente atto di nomina, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

15.2 Se una disposizione del presente atto di nomina diviene, successivamente, invalida o inapplicabile, la validità e l'applicabilità delle altre disposizioni dello stesso rimangono inalterate. In questo caso, le Parti concordano di adottare una disposizione che corrisponda al meglio allo scopo previsto nella disposizione non valida o agli interessi delle Parti, come riportato nell'intera struttura del presente atto di nomina.

Luogo….. e data……..

Il Titolare del Trattamento dei Dati
Comune di ……..
Il Dirigente dell'Area……..,
Dott. ……..

_____

per accettazione

Il Responsabile Esterno del Trattamento dei Dati
Società ……
Il legale rappresentante
Dott./Dott.ssa ……..

_____

Allegati:
All. 1 Disciplinare tecnico
All. 2 Modulo per la segnalazione del data breach al Titolare
All. 3 Contratto tra Comune di ….. e Società ……

Si prega di restituire una copia del presente atto controfirmata per accettazione.

Allegato 1

DISCIPLINARE TECNICO

RELATIVO ALLA NOMINA DEL RESPONSABILE DEL TRATTAMENTO PER IL SERVIZIO DI consulenza brokeraggio assicurativo.

N.B.: Questo allegato, poiché non esistono misure standard per qualsiasi trattamento di dati personali, deve essere adeguato al tipo di trattamento affidato al Responsabile, sulla base del contesto e della natura del trattamento, delle categorie di dati trattati, delle categorie di interessati, del livello di rischio del trattamento per i diritti e le libertà degli interessati.

Premessa

Questo Allegato contiene una descrizione delle misure di sicurezza tecniche e organizzative che è tenuto a mettere in atto dal Responsabile del trattamento per garantire un adeguato livello di sicurezza, tenuto conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche.

Il Responsabile è tenuto a comunicare tempestivamente al Titolare se non è in grado di assicurare l'implementazione delle misure seguenti, nonché a comunicare l'eventuale possesso di certificazioni pertinenti.

Si riporta, di seguito, l'elenco di possibili misure presente nella Decisione di esecuzione (UE) 2021/915 della Commissione UE del 4 giugno 2021, relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, del RGPD.

- *misure di pseudonimizzazione e cifratura dei dati personali*
- *misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento*
- *misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico*
- *procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento*
- *misure di identificazione e autorizzazione dell'utente*
- *misure di protezione dei dati durante la trasmissione*
- *misure di protezione dei dati durante la conservazione*
- *misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati*
- *misure per garantire la registrazione degli eventi*
- *misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita*
- *misure di informatica interna e di gestione e governance della sicurezza informatica*
- *misure di certificazione/garanzia di processi e prodotti*
- *misure per garantire la minimizzazione dei dati*
- *misure per garantire la qualità dei dati*
- *misure per garantire la conservazione limitata dei dati*
- *misure per garantire la responsabilità*
- *misure per consentire la portabilità dei dati e garantire la cancellazione.*

1. MISURE DI SICUREZZA IN GENERALE

1.1. MISURE ORGANIZZATIVE.

Il Responsabile del trattamento deve adottare le misure organizzative di seguito indicate, elencate e descritte, con riferimento alle strutture, agli strumenti e al personale dallo stesso impiegati per effettuare il trattamento di dati, indicando dette misure, ove opportuno, nel Registro delle attività di trattamento.

1. Politiche in materia di protezione dati, anche con l'ausilio di schemi di certificazioni quali ISDP 10003, ISO 27001, ISO 31000;
2. Nomina del proprio Responsabile Protezione Dati, se necessario.
3. Nomina Sub-Responsabili del trattamento (per iscritto), previa autorizzazione del Titolare.

4. Nomina del personale autorizzato ai trattamenti (per iscritto).
5. Adozione di Istruzioni per il trattamento/Disciplinari tecnici e policies interne che definiscano le modalità e le condizioni di utilizzo da parte del personale autorizzato dei dispositivi e dei sistemi informatici aziendali.
6. Formazione dei dipendenti in merito ai metodi di riconoscimento e prevenzione degli attacchi IT e in merito agli obblighi del Reg. UE 2016/679 e delle Linee guida del Garante per la posta elettronica e internet (Del. n. 13 del 1° marzo 2007).
7. Adozione di una Procedura per il data breach, con l'istituzione di un team di risposta e gestione degli incidenti informatici (CSIRT – Computer Emergency Response, CERT – Computer Emergency Response Team) e l'adozione di piani di risposta agli incidenti informatici (Response Plan, Disaster Recovery Plan e Business Continuity Plan) testati e aggiornati, comprensivi di revisione delle misure di sicurezza a seguito di un attacco informatico.
8. Procedura per testare, verificare e valutare periodicamente l'efficacia delle misure tecniche e organizzative, con cadenza almeno annuale, al fine di procedere ad una loro rivalutazione e, se del caso, aggiornamento.
9. Adozione di politiche di data retention, ossia atte a monitorare la scadenza dei tempi di conservazione delle varie categorie di dati personali. La finalità del trattamento è il criterio principale per stabilire la durata del trattamento.

1.2. MISURE TECNICHE.

Il Responsabile del trattamento deve adottare le misure tecniche di seguito indicate, elencate e descritte, con riferimento alle strutture, agli strumenti e al personale dallo stesso impiegati per effettuare il trattamento di dati, indicando dette misure, ove opportuno, nel Registro delle attività di trattamento:

a) Misure idonee ad assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.

b) Misure idonee a ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.

c) Pseudonimizzazione e cifratura dei dati, laddove applicabile, qualora non sia necessaria l'identificazione diretta del soggetto i cui dati si riferiscono.

d) Adozione di una procedura di autenticazione per accedere ai dispositivi informatici, attraverso "credenziali personalizzare di autenticazione", che consistono in un user - ID associato a una parola chiave segreta (password di almeno 8 caratteri contenente obbligatoriamente almeno una lettera maiuscola, un numero e un carattere speciale; previsione di un meccanismo di rinnovo periodico della password).

e) Adozione di forme forti di criptazione o di autenticazione per gli accessi amministrativi ai sistemi IT, come l'autenticazione a due fattori, oltre a un sistema di gestione delle password.

f) Custodia delle credenziali di autenticazione, che devono essere utilizzate in modo pertinente e strettamente personale e non essere comunicate ad altri soggetti, neppure se parimenti autorizzati al trattamento, al fine di minimizzare i rischi di accesso illeciti e utilizzi impropri delle stesse.

g) Firewall e Antivirus.

h) Business continuity e Disaster recovery.

i) Procedura di backup aggiornata, sicura e testata, con separazione tra i dispositivi utilizzati per i backup a lungo termine e quelli a medio termine, oltre che rispetto a terze parti.

l) Procedure di aggiornamento periodico e automatico dei software di sicurezza.

1.3. TRATTAMENTI EFFETTUATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI.

In ordine ai trattamenti effettuati senza l'ausilio di strumenti elettronici, il Responsabile del Trattamento è tenuto al rispetto delle seguenti misure.

a) conservare gli atti e documenti cartacei contenenti dati personali in archivi o locali ad accesso autorizzato e riservato e custodire con diligenza gli atti e i documenti contenenti dati personali in maniera tale che le persone non autorizzate al trattamento non possano venirne a conoscenza, neppure accidentalmente (es. non lasciare documenti incustoditi sulla scrivania);

b) evitare la duplicazione, laddove non strettamente necessaria, sia essa in forma elettronica o cartacea, di atti e documenti contenenti dati personali; in caso di

duplicazione, conservare la copia cartacea o il supporto fisico su cui è memorizzata la copia in forma elettronica con le medesime modalità degli originali cartacei, al fine di assicurarne la riservatezza e integrità;

10. c) qualora sia necessario distruggere atti e documenti contenenti dati personali e utilizzare appositi strumenti o modalità che ne impediscano il ricomponimento e il successivo utilizzo.

2. ADOZIONE DI SPECIFICI ACCORGIMENTI TECNICI.

2.1 DISPOSITIVI, DATABASE, RETI, ACCESSI

In osservanza del Reg. UE 2016/679, del novellato D.Lgs. n. 196/2003 e delle Linee guida del Garante del 24 luglio 2008, il Responsabile del trattamento deve adottare idonei accorgimenti tecnici volti ad incrementare il livello di sicurezza dei dati, con particolare riferimento alle operazioni di registrazione e gestione con strumenti elettronici dei dati personali.
In relazione a tali operazioni di trattamento, il Responsabile deve adottare:
a) laddove siano utilizzati sistemi di memorizzazione o archiviazione dei dati, idonei accorgimenti per garantire la protezione dei dati registrati dai rischi di accesso abusivo, furto o smarrimento parziali o integrali dei supporti di memorizzazione o dei sistemi di elaborazione portatili o fissi (ad esempio, attraverso l'applicazione parziale o integrale di tecnologie crittografiche a file system o database, oppure tramite l'adozione di altre misure informatiche di protezione che rendano inintelligibili i dati ai soggetti non legittimati);
b) protocolli di comunicazione sicuri basati sull'utilizzo di standard crittografici per la trasmissione elettronica dei dati;
c) con specifico riferimento ai database:

i. idonei sistemi di autenticazione e di autorizzazione per i soggetti autorizzati al trattamento, in funzione dei ruoli e delle esigenze di accesso e trattamento;
ii. procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati ai soggetti autorizzati al trattamento;
iii. sistemi di audit log per il controllo degli accessi ai database e per il rilevamento di eventuali anomalie, con inoltro a un server di log centrale;

d) con specifico riferimento alle reti:
- aggiornamento di firmware, sistemi operativi e software presenti sui server, dispositivi client, componenti attivi della rete, etc.;
- progettare e organizzazione dei sistemi informatici in modo tale da segmentare e isolare i sistemi e le reti contenenti i dati, al fine di evitare che il malware si propaghi all'interno delle strutture o verso sistemi esterni all'organizzazione;
- installazione di software anti-malware, firewall e sistema di detenzione e prevenzione delle intrusioni;
e) con specifico riferimento agli accessi logici:
- è necessario definire un processo di gestione delle credenziali di autorizzazione e dei relativi profili di accesso;
- l'accesso alle informazioni in formato digitale da parte di utenti e sistemi autorizzati deve essere subordinato al superamento di una procedura di identificazione ed autenticazione degli stessi;
- le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui e devono essere periodicamente sottoposte a revisione;
- l'accesso alle informazioni da parte di ogni singolo utente deve essere limitato alle sole informazioni di cui necessita per lo svolgimento dei propri compiti (c.d. principio del "need to-know");
- la comunicazione e trasmissione di informazioni all'interno, così come verso l'esterno, deve fondarsi sullo stesso principio;
- i sistemi che costituiscono l'infrastruttura ICT devono essere opportunamente protetti e segregati, in modo da minimizzare la possibilità degli accessi non autorizzati.

2.2 BUSINESS CONTINUITY

Al fine di garantire la continuità delle attività e l'eventuale ripristino tempestivo dei servizi erogati colpiti da eventi anomali di una certa gravità, il Responsabile deve:

a) attentamente identificare e valutare, in termini di probabilità di accadimento e possibili conseguenze, tutti gli eventi da cui può dipendere un'interruzione della continuità;
b) predisporre un piano di continuità che permetta all'organizzazione di affrontare, in modo organizzato ed efficiente, le conseguenze di un evento imprevisto garantendo il ripristino dei servizi critici in tempi e con modalità che consentano la riduzione delle conseguenze negative;
c) preparare, validate e opportunamente divulgate tutte le procedure operative ed organizzative necessarie per assicurare l'implementazione del piano di continuità;
d) periodicamente effettuare i test per tutti i componenti del piano di continuità;
e) assicurare il mantenimento e l'aggiornamento dei piani e delle procedure di cui ai punti precedenti al fine di garantire l'efficacia del sistema nel tempo a fronte di eventuali cambiamenti organizzativi/tecnologici.

2.3 PIATTAFORME DIGITALI, SITI WEB, CASELLE DI POSTA ELETTRONICA

Anche con riferimento alle attività di sviluppo e gestione di piattaforme digitali, APP e siti web il Responsabile del trattamento deve adottare soluzioni in grado di garantire la riservatezza, la disponibilità e l'integrità dei dati, nonché in grado di garantire il rispetto della normativa in materia di protezione dati personali, e più in particolare:

a) utilizzare soluzioni provenienti da fornitori affidabili;
b) effettuare controlli periodici della sicurezza (site-check);
c) crittografare il sito con un certificato "Secure Socket Layer" (SSL) e utilizzare il linguaggio di markup HTTPS, che permettono trasferimenti di dati in sicurezza;
d) dare la possibilità agli utenti, di attivare l'autenticazione a due fattori (anche per le caselle di posta elettronica), laddove ciò sia possibile;
e) proteggere l'accesso al sito con credenziali mediante un sistema di blocco IP (ad es. se viene inserito per 5 volte un nickname non esistente o per 10 volte una password non corretta), imponendo agli utenti l'utilizzo di password sicure ed univoche;
f) utilizzare le ultime versioni dei browser e dei software (CMS, Wordpress, PHP, ecc.);
g) integrare i "captcha", laddove ciò sia possibile;
h) fornire i dati aziendali sul sito web, per come richiesto dalla normativa in materia;
i) prestare attenzione nella gestione delle caselle e-mail, ove attivate;
j) effettuare backup completo, dei file e del Database, in maniera regolare (possibilmente quotidianamente);
k) installare un firewall che blocca eventuali iniezioni di codice esecutivo;
l) bloccare tutte le funzioni che permettono l'ottenimento di informazioni di versioni e utenti.

Con riferimento, invece, ai cookie è necessario conformarsi alle Linee Guida del Garante del 10 giugno 2021[6] e, nello specifico, prevedere gli accorgimenti necessari a:

- anonimizzare i dati personali ove necessario (es. verificare che i file di registro nei server web non contengano dati personali come ad esempio l'indirizzo IP; si veda, in tal senso, per Google Analytics, https://support.google.com/analytics/answer/2763052?hl=it&visit_id=637782692001573690-2500739750&rd=1)
- ridurre all'indispensabile l'utilizzo di identificatori utente univoci;
- informare gli utenti ai sensi dell'art. 13, Reg. UE 2016/679, prima di trattare i dati;
- laddove sia necessario il consenso dell'utente come base giuridica del trattamento (ad es. per l'installazione di cookie di profilazione, per trattamenti di dati a fini di marketing, ecc.):
  - ✓ configurare un sistema di raccolta (e conservazione) del consenso esplicito dell'utente, in maniera corretta e trasparente;
  - ✓ implementare un banner per la raccolta del consenso, conforme alle Linee Guida del garante, e che dia la possibilità, ai visitatori, di modificare o revocare il consenso;
  - ✓ non prevedere cookie wall, scrolling e consensi flaggati di default.

Resta inteso che, qualora il Titolare decidesse di elaborare una propria policy per il sito web o l'APP, per poter adempiere all'obbligo informativo è necessario che il Responsabile del

6 GARANTE PRIVACY, Provvedimento 10 giugno 2021, n. 231, "Linee guida cookie e altri strumenti di tracciamento" (doc. web n. 9677876, pubblicato sulla Gazzetta Ufficiale n. 163 del 9 luglio 2021), che aggiorna il precedente Provvedimento dell'8 maggio 2014, n. 229, avente ad oggetto "Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie"

trattamento comunichi allo stesso Titolare: le modalità del trattamento, le misure di sicurezza, se vi è un trasferimento di dati al di fuori dell'UE, nonché l'elenco dei cookie installati sul pc dell'utente, indicando, in particolare, il nome del cookie, la finalità, la durata, lo scopo, e se si tratta di cookie anonimo o univoco.

3. NORME FINALI

- Il Responsabile del trattamento è tenuto a comunicare al Titolare qualsiasi aspetto e/o modifica riguardante la comunicazione ai terzi e la diffusione dei dati degli interessati, la profilazione degli interessati, il trasferimento dei dati degli interessati al di fuori dello SEE, i tempi di conservazione dei dati trattati, la cancellazione sicura dei dati alla cessazione del Contratto.
- Il Responsabile del trattamento è tenuto a comunicare al Titolare del trattamento, entro 30 giorni dall'avvio delle attività contrattuali il nome e dati di contatto del DPO, qualora nominato;
- In caso di trasferimento dei dati personali a Sub-responsabili del trattamento, il Responsabile è tenuto a descrivere anche le misure tecniche e organizzative specifiche che il Sub-responsabile del trattamento deve implementare per essere in grado di fornire assistenza al Titolare del trattamento.
- Il Responsabile del trattamento, in caso di dubbi sul presente Allegato, può contattare in ogni momento il DPO del Titolare.

Allegato 2 MODULO PER LA SEGNALAZIONE DEL DATA BREACH AL TITOLARE

Data	
Nome e cognome del segnalante	
Struttura di afferenza, funzione e dati di contatto del segnalante (tel., e-mail ecc.)	
Ulteriori soggetti coinvolti nel trattamento	
Informazioni sulla violazione	
1. Momento in cui è avvenuta la violazione	☐ Il _____ ☐ Dal _____ (la violazione è ancora in corso) ☐ Dal _____ al _____ ☐ In un tempo non ancora determinato
2. Modalità con la quale il Responsabile del trattamento è venuto a conoscenza della violazione	
3. Momento nel quale il Responsabile del trattamento è venuto a conoscenza della violazione (e motivi del ritardo, se la segnalazione è inviata dopo il termine previsto nella "Nomina a Responsabile del trattamento")	
4. Tipo di violazione	☐ Ransomware
	☐ Lettura (presumibilmente i dati non sono stati copiati)
	☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
	☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
	☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
	☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)

	☐ Altro:_____ _____ (*DESCRIVERE*)
5. Natura della violazione dal punto di vista del RID	☐ Perdita di riservatezza del dato personale (R) ☐ Perdita di integrità del dato personale (I) ☐ Perdita di disponibilità del dato personale (D)
6. Causa della violazione	☐ Azione intenzionale interna ☐ Azione accidentale interna ☐ Azione intenzionale esterna ☐ Azione accidentale esterna ☐ Sconosciuta
7. Descrizione dei sistemi, software, servizi e delle infrastrutture IT coinvolti nella violazione, con indicazione della loro ubicazione	
8. Misure tecniche e organizzative, in essere al momento della violazione, adottate per garantire la sicurezza dei dati personali coinvolti	
9. Categorie di interessati coinvolti nella violazione	☐ Dipendenti/Consulenti ☐ Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali) ☐ Associati, soci, aderenti, simpatizzanti, sostenitori ☐ Soggetti che ricoprono cariche sociali ☐ Beneficiari o assistiti ☐ Pazienti ☐ Minori ☐ Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo) ☐ Altro _____
10. Numero (anche approssimativo) di interessati coinvolti nella violazione.	☐ N. ___ interessati ☐ Circa n. _____ interessati ☐ Non determinabile ☐ Non ancora determinato
11. Categorie di dati personali oggetto di violazione	☐ Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale) ☐ Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile) ☐ Dati di accesso e di identificazione (username, password, customer ID, altro…) ☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…) ☐ Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…) ☐ Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza ☐ Dati di profilazione ☐ Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente,

	CNS, altro…) ☐ Dati di localizzazione ☐ Dati che rivelino l'origine razziale o etnici ☐ Dati relativi a opinioni politiche ☐ Dati relativi a convinzioni religiose o filosofiche ☐ Dati che rivelino l'appartenenza sindacale ☐ Dati relativi alla vita sessuale o all'orientamento sessuale ☐ Dati relativi alla salute ☐ Dati genetici ☐ Dati biometrici ☐ Altro _____ ☐ Categorie ancora non determinate
12. Numero (anche approssimativo) di registrazioni dei dati personali oggetto di violazione	☐ N.0 ☐ Circa N. ☐ Non determinabile ☐ Non ancora determinato
13. Descrizione di dettaglio delle categorie di dati personali oggetto della violazione per ciascuna categoria di interessati	
Probabili conseguenze della violazione	
1. Probabili conseguenze della violazione per gli interessati	**In caso di perdita di riservatezza:** ☐ I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento ☐ I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati ☐ I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito ☐ Altro _____ ☐ In corso di valutazione **In caso di perdita di integrità:** ☐ I dati sono stati modificati e resi inconsistenti ☐ I dati sono stati modificati mantenendo la consistenza ☐ Altro _____ ☐ In corso di valutazione **In caso di perdita di disponibilità:** ☐ Mancato accesso a servizi ☐ Malfunzionamento e difficoltà nell'utilizzo di servizi ☐ Altro _____ ☐ In corso di valutazione Eventuali ulteriori considerazioni sulle conseguenze della violazione: _____
2. Potenziale impatto per gli interessati	☐ Perdita del controllo dei dati personali ☐ Limitazione dei diritti

	☐ Discriminazione ☐ Furto o usurpazione d'identità ☐ Frodi ☐ Perdite finanziarie ☐ Decifratura non autorizzata della pseudonimizzazione ☐ Pregiudizio alla reputazione ☐ Perdita di riservatezza dei dati personali protetti da segreto professionale ☐ Conoscenza da parte di terzi non autorizzati ☐ Qualsiasi altro danno economico o sociale significativo _____ ☐ Non ancora definito
3. Gravità del potenziale impatto per gli interessati	☐ Trascurabile ☐ Bassa ☐ Media ☐ Alta ☐ Non ancora definita _____
Misure adottate a seguito della violazione	
1. Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati	
2. Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per prevenire simili violazioni future	