ALLEGATO “A”

INDICAZIONI PER IL RESPONSABILE ESTERNO DEL TRATTAMENTO

1. **Osservare:** il Reg. UE n. 679/2016 (GDPR); i Provvedimenti del Garante per la protezione dei dati personali, il D.Lgs. 30 giugno 200 n. 196, così come modificato ed integrato dal D.Lgs. 101/2018, il vigente Regolamento per il trattamento dei dati sensibili e giudiziari dell’Ente;

2. **Persone autorizzate al trattamento**. Prima di iniziare qualsiasi trattamento di dati, il fornitore deve garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza provvedendo alla loro nomina con atto scritto e avendo cura di fornire tutte le istruzioni necessarie per il corretto, lecito e sicuro trattamento dei dati personali nell’ambito della loro attività;

3. **Clausola di riservatezza**. I dati sono da considerarsi quali informazioni riservate del committente. Su questa base: non deve in alcun modo trasferire dati personali verso un paese terzo o un’organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il fornitore. In tal caso, il fornitore informa il committente circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

4. **Finalità** Il trattamento dei dati deve essere effettuato dal fornitore ai soli fini di dare esecuzione ai servizi commissionatigli. Esso si dovrà configurare, quindi, come strettamente necessario per effettuare il servizio;

5. **Diritto di accesso**. Deve essere garantito agli interessati l'effettivo esercizio dei diritti loro riconosciuti dal GDPR, incluso il diritto di accesso, tenendo conto che il Responsabile del trattamento assiste il Titolare con misure tecniche ed 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 del Regolamento UE 2016/679 (GDPR);

6. **Misure di sicurezza**. 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 fornitore deve adottare idonee ed adeguate misure necessarie ai fini della sicurezza dei dati personali, ai sensi dell’articolo 32 del GDPR;

7. **Assistenza al committente**. Il fornitore deve assistere il committente ai fini del rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a sua disposizione;

8. **Violazione di dati personali (data breach)**. Il fornitore deve implementare soluzioni atte a rilevare per quanto di propria responsabilità eventuali violazioni dei dati personali (ossia le violazioni di sicurezza che comportano accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati) e, al verificarsi di tali violazioni, comunicarle, senza ingiustificato ritardo, al committente. Il fornitore s’impegna, altresì, a collaborare attivamente con il committente ai fini delle conseguenti comunicazioni all’Autorità Garante per la protezione dei dati personali e, eventualmente, agli interessati ai sensi degli artt. 33 e 34 del GDPR;

9. **Verifiche del fornitore**. Il fornitore dovrà mantenere per quanto di propria responsabilità un costante controllo in merito al fatto che i dati siano trattati in modo lecito, secondo correttezza e comunque nel rispetto delle leggi, delle disposizioni in materia di trattamento compreso il profilo relativo alla sicurezza oltre che delle istruzioni impartite;

10. **Verifiche del committente**. Il fornitore deve mettere a disposizione del committente tutte le informazioni necessarie per dimostrare il rispetto degli obblighi derivanti dall'art. 28 del GDPR e contribuire alle attività di revisione, comprese le verifiche realizzate dal committente o da un altro soggetto da questi incaricato.

11. **Restituzione dei dati**. Al termine del servizio oggetto del contratto, il fornitore deve restituire, qualora ne sia in possesso, tutti i dati personali al committente, per poi provvedere alla loro distruzione, provvedendo alle formalità di legge e a comunicarne notizia al Comune committente, salvo che non sia obbligato, da normativa vigente, alla conservazione per un tempo determinato od ai fini dell'esercizio del diritto di agire e/o di difendersi in giudizio.

12. **Dovere di informazione**. Il fornitore deve informare immediatamente il committente qualora, a suo parere, un'istruzione violi il regolamento europeo o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

13. **Vigilanza**. Vigilare e controllare il trattamento svolto dagli Incaricati medesimi.

14. **Valutazione d'impatto sulla protezione dei dati personali (DPIA)**. Il fornitore, su espressa richiesta dell'ente Committente, deve assistere lo stesso con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di agevolare la realizzazione di valutazioni d'impatto sulla protezione dei dati personali, ai sensi dell'art. 35 del GDPR, per il trattamento in questione.

15. **Sub-responsabile**. Il fornitore può ricorrere a un altro responsabile solo previa autorizzazione scritta, specifica o generale, del committente. La presente vale quale autorizzazione scritta generale. Il fornitore è comunque sempre tenuto ad informare il committente in merito alla scelta, aggiunta o sostituzione di qualsiasi responsabile del trattamento, dando così al committente l'opportunità di valutarla e, se del caso, opporvisi. Se il fornitore ricorre a un altro responsabile (sub-responsabile) per l'esecuzione di specifiche attività di trattamento per conto del committente, deve imporgli, 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 presente contratto. In particolare, il sub-responsabile deve presentare garanzie sufficienti per la predisposizione di misure tecniche e organizzative adeguate al fine di soddisfare i requisiti normativi previsti.

16. **Registro delle attività dei trattamenti**. Il fornitore deve tenere un registro delle attività dei trattamenti ai sensi dell'art. 30 c.2 del GDPR.

17. **Responsabile della protezione dei dati (DPO)**. Il fornitore deve procedere, se del caso, alla designazione del responsabile della protezione dei dati (DPO) ai sensi dell'art. 37 del GDPR. Qualora il fornitore ritenga di non doversi dotare di tale figura ne fornisce adeguata e documentata motivazione al committente.

18. Per quanto di competenza del fornitore, tenere indenne il Comune committente da responsabilità derivanti da un erroneo o illegittimo trattamento dei dati.

19. Si rammenta che la violazione delle norme di legge in materia di privacy comporterà la comminazione delle sanzioni e l'eventuale risarcimento del danno previsti dal codice.

Resta inteso che la nomina a Responsabile esterno del trattamento decadrà in qualunque caso di cessazione del servizio appaltato, con effetto dalla data di tale cessazione.

In funzione di quanto sopra deve essere restituito il presente documento, preferibilmente firmato digitalmente, o in subordine con firma autografa e timbro nell'apposito spazio posto in calce e siglato su ogni singola pagina per conferma e accettazione.

Il Titolare del Trattamento dei Dati
Comune di Capannori (Lu)
Dirigente Responsabile del Settore _____
Luogo e data.....

Per accettazione
Il Responsabile Esterno del Trattamento dei dati Dott. Frediano Moretti, Legale Rappresentante della Toscana Arkivi srl
_____
Luogo e data Lucca, il 06.03.2023

Documento firmato digitalmente