

## **Allegato B: Disciplina di dettaglio per la nomina a Responsabile del trattamento dei dati**

### **PREMESSO CHE**

- 1) l'articolo 4, paragrafo 1, n. 8) del Regolamento (UE) 2016/679 (di seguito, per brevità, "GDPR") definisce quale responsabile del trattamento *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento"*;
- 2) a norma dell'articolo 28, paragrafo 1 del GDPR *"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"*;
- 3) a norma dell'articolo 28, paragrafo 3 del GDPR *"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"*;
- 4) a norma dell'articolo 28, paragrafo 9 del GDPR *"Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico"*
- 5) in conseguenza dell'affidamento del servizio di che trattasi, il fornitore si troverà ad effettuare il trattamento di dati personali per conto dell'Ente (Titolare del trattamento), assumendo la qualifica di Responsabile del trattamento ai sensi e per gli effetti di cui all'articolo 28 del GDPR;
- 6) è intenzione dell'Ente subordinare l'autorizzazione al trattamento dei dati personali, per proprio conto, al rispetto delle seguenti prescrizioni minime ed a quelle eventualmente contenute in altri atti e documenti, da questo atto richiamati;

### **SI STABILISCE QUANTO SEGUE**

#### **Articolo 1 – Disposizioni generali**

1. Le previsioni contenute nel presente documento riguardano espressamente il servizio rispetto al quale è stata avviata la presente procedura di selezione del contraente e si intendono accettate - senza riserva alcuna da parte del fornitore - a seguito dell'invio della propria offerta.
2. Le prescrizioni contenute nel presente documento possono subire modifiche ed integrazioni in conseguenza della valutazione delle informazioni rese dal Responsabile in ottemperanza a quanto previsto negli atti che hanno dato avvio alla procedura di selezione del contraente. Il Responsabile del trattamento informa immediatamente il Titolare qualora, a suo parere, una specifica prescrizione, in qualunque tempo impartita, violi il GDPR o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati. L'esecuzione delle operazioni di trattamento per conto del Titolare costituisce manifestazione espressa della volontà di accettare tutte le prescrizioni da esso impartite.
2. I presente documento non costituisce autorizzazione generale, bensì, autorizzazione limitata esclusivamente ai trattamenti relativi al servizio oggetto della presente procedura selettiva.
3. Il Responsabile è tenuto a trattare i dati personali di cui entra in possesso o rispetto ai quali abbia comunque accesso, in adempimento degli obblighi derivanti dall'affidamento e di eventuali servizi accessori allo stesso, nel rispetto dei principi e delle norme contenute

nel GDPR ed attenendosi alle istruzioni del Titolare del trattamento, tenendo altresì conto dei provvedimenti, tempo per tempo, emanati dall'Autorità di controllo inerenti al trattamento svolto.

## **Articolo 2 – Durata del trattamento**

1. Il trattamento per conto del Titolare deve avere una durata non superiore a quella necessaria ad eseguire la prestazione contrattuale per la quali i dati personali sono stati raccolti e tali dati devono essere conservati nei sistemi e nelle banche dati del Responsabile, in una forma che consenta l'identificazione degli Interessati, per un periodo di tempo non superiore a quello in precedenza indicato, fatta salva l'osservanza di specifiche disposizioni di legge che ne impongano la conservazione.

2. A seguito della cessazione del trattamento affidato al Responsabile, nonché a seguito della cessazione del rapporto contrattuale sottostante, qualunque ne sia la causa, il Responsabile sarà tenuto, a discrezione del Titolare, a:

- restituire al Titolare i dati personali trattati, oppure a
- provvedere alla loro integrale distruzione, salvi solo i casi in cui la conservazione dei dati sia richiesta da norme di legge e/o altre finalità (contabili, fiscali, ecc.) od il caso in cui si verificano circostanze autonome e ulteriori che giustifichino la continuazione del trattamento dei dati da parte del Responsabile, con modalità limitate e per il periodo di tempo a ciò strettamente necessario.

3. Il Responsabile, su richiesta del Titolare, provvede a rilasciare apposita dichiarazione scritta contenente l'attestazione che, presso di sé, non esiste alcuna copia dei dati personali e delle informazioni trattate per conto del Titolare. Sul contenuto di tale dichiarazione il Titolare si riserva il diritto di effettuare controlli e verifiche volte ad accertarne la veridicità.

4. In caso di fallimento o sottoposizione ad altra procedura concorsuale del Responsabile, ovvero in caso di mancato assolvimento da parte di quest'ultimo degli obblighi previsti ai commi che precedono, ovvero ancora in caso di omissione ovvero di sospensione anche parziale, da parte del Responsabile, dell'esecuzione delle obbligazioni qui previste, il Titolare, ove possibile e dandone opportuna comunicazione, potrà sostituirsi al Responsabile nell'esecuzione delle obbligazioni ovvero potrà avvalersi di soggetto terzo in danno ed a spese del Responsabile, fatto salvo il risarcimento del maggior danno.

## **Articolo 3 - Obblighi in capo al Responsabile**

1. Il Responsabile dichiara e conferma la propria diretta ed approfondita conoscenza degli obblighi ed oneri derivanti dall'osservanza delle disposizioni contenute nel GDPR, in conseguenza della relazione contrattuale instaurata con il Titolare. Dichiara inoltre di possedere esperienza, capacità e affidabilità idonee a garantire il rispetto delle disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza, ed in ogni caso di essere in grado di fornire garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti della normativa e garantisca la tutela dei diritti dell'Interessato.

2. Il Responsabile è tenuto a:

a) trattare i dati nel rispetto dei principi del trattamento previsti nel GDPR e solo per la sola finalità di dare esecuzione al contratto. In particolare, il Responsabile garantisce che i dati da trattarsi per conto del Titolare, saranno:

a1) trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato;

a2) raccolti per le finalità determinate, esplicite e legittime sopra indicate, e successivamente trattati in modo che non sia incompatibile con tali finalità;

a3) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

a4) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

a5) 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;

b) trattare i dati secondo le istruzioni documentate del Titolare del trattamento dei dati;

c) garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate formalmente alla riservatezza od abbiano un adeguato obbligo legale di riservatezza ed abbiano ricevuto la formazione necessaria in materia di protezione dei dati personali;

d) prendere in considerazione, in termini di strumenti, prodotti, applicazioni o servizi, i principi della protezione dei dati in base alla progettazione e per impostazione predefinita (cc.dd. data protection by design e by default);

e) assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento ed in particolare a collaborare nelle comunicazioni di violazioni di dati personali, negli adempimenti della valutazione di impatto e consultazione preventive;

3. Il Responsabile si impegna ad informare il Titolare di ogni richiesta, ordine o controllo da parte di una o più

Autorità e da soggetti da queste autorizzati e/o delegati, in relazione ai trattamenti oggetto di affidamento;

#### **Articolo 4 - Obblighi in capo al Titolare del trattamento**

1. Il Titolare del trattamento si impegna a:

a) fornire al Responsabile i dati oggetto del trattamento curandone l'esattezza, la veridicità, l'aggiornamento, la pertinenza e la non eccedenza rispetto alle finalità per le quali sono stati raccolti e saranno successivamente trattati;

b) individuare la base legale del trattamento dei dati personali degli Interessati.

c) documentare, per iscritto, ogni istruzione relativa al trattamento dei dati da parte del Responsabile. Il Responsabile del trattamento informa immediatamente il Titolare qualora, a suo parere, un'istruzione violi il GDPR od altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati;

d) assicurare, prima e durante l'intero processo, il rispetto degli obblighi su di sé incombenti ai sensi del GDPR e della normativa nazionale di riferimento;

e) supervisionare il trattamento, in tutte le sue fasi, anche effettuando audit ed ispezioni presso il Responsabile;

f) adottare tutte le misure di sicurezza di sua competenza idonee a garantire il rispetto della normativa in materia di privacy e di trattamento dei dati in regime di sicurezza.

2. Il Titolare si dichiara edotto che in caso di violazione di dati personali (c.d. data breach) rimane a suo carico, ai sensi dell'art. 33 del GDPR, l'obbligo di notifica all'Autorità di controllo senza ingiustificato ritardo e, comunque, entro 72 ore dal momento in cui il Titolare è venuto a conoscenza della violazione di dati personali.

3. Il Titolare si impegna, altresì, a comunicare al Responsabile del trattamento qualsiasi variazione si dovesse rendere necessaria nelle operazioni di trattamento dei dati.

4. Il Titolare rimane Responsabile del trattamento dei dati personali attuato tramite procedure applicative sviluppate secondo sue specifiche e/o attraverso propri strumenti informatici o di telecomunicazioni.

5. Il Titolare si impegna ad informare il Responsabile di ogni richiesta, ordine o controllo da parte di una o più

Autorità e da soggetti da queste autorizzati e/o delegati, in relazione ai trattamenti oggetto di affidamento;

## **Articolo 5 - Incaricati e persone autorizzate**

1. Il Responsabile dovrà identificare e designare le persone autorizzate ad effettuare operazioni di Trattamento sui dati per conto del Titolare identificando l'ambito autorizzativo consentito ai sensi dell'art. 29 del GDPR e provvedendo alla relativa formazione. Allo stesso tempo, il Responsabile dovrà fornire ai soggetti da sé autorizzati le dovute istruzioni relativamente alle operazioni ed alle modalità di trattamento dei dati personali.
2. Il Responsabile garantisce che i propri dipendenti e collaboratori sono affidabili ed hanno piena conoscenza della normativa primaria e secondaria in materia di protezione dei dati personali.

## **Articolo 6 - Sub-responsabile del trattamento e Terze parti**

1. Il Responsabile del trattamento non ricorre ad un altro Responsabile se non previa autorizzazione scritta, del Titolare del trattamento. Qualora, anche successivamente all'affidamento, il Responsabile ravvisasse la necessità di avvalersi di un altro responsabile del trattamento (Sub-responsabile) per l'esecuzione di specifiche attività di trattamento per conto del Titolare, è tenuto a richiederne l'autorizzazione al Titolare con congruo preavviso. La mancata autorizzazione non consentirà il ricorso al Sub-responsabile.
2. Nel caso in cui il Responsabile del trattamento (Responsabile primario) ricorra ad un altro Responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del Titolare del trattamento, su tale altro Responsabile sono imposti, mediante un contratto od 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 documento per il Responsabile del trattamento, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti della legge vigente.
3. Nel caso in cui 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, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è imputabile.
4. Il Responsabile si impegna a non comunicare, trasferire o condividere, i dati personali trattati per conto del Titolare a Terze parti, salvo qualora legislativamente richiesto e, in ogni caso, informandone preventivamente il Titolare.

## **Articolo 7 - Misure di sicurezza**

1. Il Responsabile, in considerazione della conoscenza maturata in relazione ai progressi tecnici e tecnologici, della natura dei dati personali e delle caratteristiche delle operazioni di trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche ed organizzative adeguate e dovrà assicurare che le misure di sicurezza progettate ed implementate siano in grado di ridurre il rischio di danni volontari o accidentali, perdita di dati, accessi non autorizzati ai dati, trattamenti non autorizzati o trattamenti non conformi agli scopi di cui alla presente Appendice.
2. Ai fini della sicurezza dei dati e dei sistemi IT, il Responsabile si obbliga:
  - ad adottare adeguate misure IT per la sicurezza dei dati personali, ai sensi dell'art. 32 del GDPR, in modo da garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
  - ad adottare adeguate misure che consentano di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

- a non trasferire i dati personali oggetto di trattamento per conto del Titolare, senza il preventivo consenso di questi, al di fuori dell'usuale luogo di lavoro, a meno che tale trasferimento non sia autorizzato dalle competenti pubbliche autorità, anche regolamentari e di vigilanza;
- a fornire, in caso di richiesta, al Titolare una descrizione dettagliata delle misure fisiche, tecniche ed organizzative applicate al trattamento dei dati personali;
- ad impiegare sistemi di cifratura per i dati personali memorizzati su dispositivi di archiviazione digitali od elettronici, come computer portatili, CD, dischetti, driver portatili, nastri magnetici o dispositivi simili. I dati personali dovranno essere cifrati nel rispetto della normativa vigente ed il Responsabile dovrà compiere ogni ragionevole sforzo per assicurare l'aggiornamento degli standard di cifratura in modo da tenere il passo dello sviluppo tecnologico e dei rischi ad esso connaturati, includendo ogni richiesta o indicazione emanata da qualsiasi pubblica autorità competente, anche regolamentare e di vigilanza;
- ad adottare una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento

### **Articolo 8 - Registro delle categorie di trattamento**

1. Il Responsabile del trattamento adotta, aggiorna e conserva una registrazione scritta di tutte le categorie di attività relative al trattamento svolte per conto del Titolare, avente il contenuto minimo previsto dall'articolo 30, paragrafo 2 del GDPR e, su richiesta, lo rende disponibile all'Autorità di controllo ed al Titolare.

### **Articolo 9 - Violazioni di dati personali**

1. In eventuali casi di violazione della sicurezza dei dati personali che comporti, accidentalmente od 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 tali da mettere a rischio i diritti e le libertà degli individui i cui dati personali sono trattati dal Responsabile per conto del Titolare (c.d. data breach), il Responsabile deve osservare le disposizioni organizzative contenute nella data breach policy adottata dal Titolare e, in ogni caso:

a) informare il Titolare tempestivamente ed in ogni caso entro e non oltre 24 ore dalla scoperta dell'evento, tramite PEC, di essere venuto a conoscenza di una violazione e fornire al Titolare tutti i dettagli della violazione subita, in particolare una descrizione della natura della violazione dei dati personali, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati in questione, l'impatto della violazione dei dati personali sul Titolare e sugli Interessati coinvolti e le misure adottate per mitigare i rischi. Spetta unicamente al Titolare del trattamento di effettuare la valutazione circa la probabilità di rischio derivante dalla violazione stessa;

b) fornire assistenza al Titolare per far fronte alla violazione ed alle sue conseguenze soprattutto in capo agli Interessati coinvolti. Il Responsabile si attiverà per mitigare gli effetti delle violazioni, proponendo tempestive azioni correttive al Titolare ed attuando tutte le azioni correttive approvate e/o richieste dal Titolare. Tali misure sono richieste al fine di garantire un livello di sicurezza adeguato al rischio correlato al Trattamento eseguito;

2. Il Responsabile del trattamento si impegna a predisporre e tenere aggiornato un registro interno delle violazioni di dati personali nonché a raccogliere e conservare tutti i documenti relativi ad ogni violazione, compresi quelli inerenti alle circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

### **Articolo 10 - Accordo relativo al trasferimento dei dati all'estero**

1. Il Responsabile si impegna a circoscrivere gli ambiti di circolazione e di trattamento dei Dati personali (es.

memorizzazione, archiviazione e conservazione dei dati sui propri server od in cloud) ai Paesi facenti parte dell'Unione Europea, con espresso divieto di trasferirli in paesi extra UE che non garantiscano (o in assenza di) un livello adeguato di tutela, ovvero, in assenza di strumenti di tutela previsti dal Regolamento UE 2016/679 (Paese terzo giudicato adeguato dalla Commissione Europea, BCR di gruppo, clausole contrattuali modello, consenso degli interessati, etc.).

2. Il Responsabile, pertanto, non dovrà trasferire od effettuare il Trattamento dei Dati personali per conto del Titolare al di fuori dell'Unione Europea, per nessuna ragione, in assenza di autorizzazione scritta del Titolare. Qualora il Titolare rilasci l'autorizzazione di cui al presente articolo e venga pertanto effettuato un trasferimento dei dati personali del Titolare al di fuori dell'Unione Europea, tale trasferimento dovrà rispettare le previsioni di cui al GDPR sopra indicate. Resta inteso tra le Parti che il Responsabile dovrà garantire che i metodi di trasferimento impiegati, ivi inclusa la conformità alle clausole contrattuali standard approvate dalla Commissione Europea e sulla base dei presupposti indicati nella medesima decisione consentano il mantenimento di costanti e documentabili standard di validità per tutta la durata della presente Appendice.

Il Responsabile è obbligato a comunicare immediatamente al Titolare il verificarsi di una delle seguenti fattispecie:

(a) mancato rispetto delle clausole contrattuali standard di cui sopra, oppure

(b) qualsiasi modifica della metodologia e delle finalità trasferimento dei dati personali all'estero.

### **Articolo 11 - Diritti delle persone interessate**

1. È compito del Responsabile del trattamento fornire adeguata informativa agli Interessati dalle operazioni di trattamento, nel momento in cui i dati vengono raccolti presso di loro. L'informativa dovrà evidenziare il fatto che la raccolta avviene per conto del Titolare.

2. Il Responsabile, per quanto di propria competenza, si obbliga ad assistere ed a supportare il Titolare con misure tecniche e organizzative adeguate al fine di soddisfare l'obbligo del Titolare di dare riscontro alle richieste per l'esercizio dei diritti dell'Interessato (negli ambiti e nel contesto del ruolo ricoperto e in cui opera il Responsabile) nel rispetto dei termini previsti dall'art. 12 del GDPR.

3. In particolare, qualora il Responsabile riceva richieste provenienti dagli Interessati, finalizzate all'esercizio dei propri diritti, esso dovrà:

- darne tempestiva comunicazione scritta al Titolare via posta elettronica certificata, allegando copia delle richieste ricevute;

- coordinarsi, ove necessario e per quanto di propria competenza, con le funzioni interne designate dal Titolare per gestire le relazioni con gli Interessati;

### **Articolo 12 - Verifiche circa il rispetto delle regole di protezione dei dati personali**

1. Il Responsabile riconosce al Titolare il diritto di effettuare controlli (audit) relativamente alle operazioni aventi ad oggetto il trattamento dei dati personali per conto del Titolare. A tal fine, il Titolare ha il diritto di disporre – a propria cura e spese – verifiche a campione o specifiche attività di audit o di rendicontazione in ambito protezione dei dati personali e sicurezza, avvalendosi di personale espressamente incaricato a tale scopo, presso le sedi del Responsabile.

2. Il Responsabile del trattamento fornisce al Titolare tutta la documentazione necessaria per dimostrare la conformità a tutti i suoi obblighi e per consentire al Titolare od a qualsiasi soggetto dal medesimo autorizzato o delegato di condurre audit, comprese le ispezioni, e per contribuire a tali verifiche.

3. Il Responsabile del trattamento deve informare e coinvolgere tempestivamente il Titolare in tutte le questioni riguardanti il trattamento dei dati personali ed in particolare nel caso di richieste di informazioni, controlli, ispezioni ed accessi da parte dell'Autorità di controllo;

### **Articolo 13- Manleva e Responsabilità per violazione delle disposizioni**

1. Il Responsabile s'impegna a mantenere indenne il Titolare da qualsiasi responsabilità, danno, incluse le spese legali, od altro onere che possa derivare da pretese, azioni o procedimenti avanzate da terzi a seguito dell'eventuale illiceità o non correttezza delle operazioni di trattamento dei dati personali che sia imputabile a fatto, comportamento od omissione del Responsabile (o di suoi dipendenti e/o collaboratori), ivi incluse le eventuali sanzioni che dovessero essere comminate ai sensi del GDPR.

2. Il Responsabile si impegna a comunicare prontamente al Titolare eventuali situazioni sopravvenute che, per il mutare delle conoscenze acquisite in base al progresso tecnico o per qualsiasi altra ragione, possano incidere sulla propria idoneità alla prestazione dei servizi dedotti nel Contratto.

3. Il Titolare ha il diritto di reclamare dal Responsabile la parte dell'eventuale risarcimento di cui dovesse essere chiamato a rispondere nei confronti di terzi per le violazioni commesse dal Responsabile ai sensi dell'art. 82, paragrafo 5, del GDPR.

4. Fatti salvi gli articoli 82, 83, e 84 del GDPR, in caso di violazione delle disposizioni contenute nella presente Appendice, relative alle finalità e modalità di trattamento dei dati, di azione contraria alle istruzioni ivi contenute od in caso di mancato adempimento agli obblighi specificatamente diretti al Responsabile dal GDPR, il Responsabile sarà considerato quale Titolare del trattamento e ne risponderà direttamente, anche dal punto di vista sanzionatorio.

### **Articolo 14 - Responsabile della Protezione dei dati personali**

1. Il Titolare rende noto di aver provveduto alla nomina del Responsabile della Protezione dei Dati personali (RPD o DPO) in conformità alla previsione contenuta nell'art. 37, par. 1, lett a) del GDPR, individuando quale soggetto idoneo l'Avv. Massimo Ramello e che il medesimo è raggiungibile ai seguenti recapiti:

Telefono: 01311826681 - Pec: [dpo@pec.gdpr.nelcomune.it](mailto:dpo@pec.gdpr.nelcomune.it)

Detto nominativo è stato altresì comunicato all'Autorità Garante per la Protezione dei dati personali con procedura telematica.

### **Articolo 15 – Comunicazioni**

1. Qualsiasi comunicazione relativa al trattamento dei dati personali nel contesto del servizio in oggetto dovrà essere data per iscritto ed a mezzo di posta elettronica certificata, con ricevuta di accettazione e conferma di consegna.

### **Articolo 16 – Disposizioni finali**

1. Per quanto non espressamente qui stabilito, il Titolare ed il Responsabile del trattamento rinviano al GDPR, alle disposizioni nazionali di legge vigenti, nonché ai provvedimenti dell'Autorità di controllo competente e del Comitato Europeo per la Protezione dei Dati Personali (EDPB).

### **PROTEZIONE DEI DATI PERSONALI - ADEMPIMENTI**

1. In conseguenza dell'affidamento del servizio di che trattasi, il fornitore si troverà ad effettuare il trattamento di dati personali per conto dell'Ente (Titolare del trattamento), assumendo la qualifica di Responsabile del trattamento ai sensi e per gli effetti di cui all'articolo 28 del Regolamento (UE) 2016/679 (di seguito, per brevità, "GDPR"). Egli sarà

pertanto autorizzato al compimento delle sole operazioni di trattamento necessarie, con riferimento ai soli dati personali necessari, ad eseguire le prestazioni affidate.

2. In caso di affidamento del servizio, i rapporti tra Titolare e Responsabile saranno regolamentati – ai sensi dell’articolo 28 del GDPR – dalle prescrizioni sopraindicate, che si intendono accettate senza riserve con la presentazione dell’offerta. Le prescrizioni sopraindicate potranno subire modifiche ed integrazioni in conseguenza della valutazione delle informazioni, documenti e dichiarazioni richiesti dal presente articolo. L’esecuzione delle operazioni di trattamento per conto del Titolare costituisce manifestazione espressa della volontà di accettare tutte le prescrizioni da esso impartite.

3. Conseguita l’aggiudicazione provvisoria, il Responsabile dovrà elaborare apposito documento contenente la descrizione del proprio servizio, sotto il profilo del trattamento dei dati personali, avendo cura di precisare:

- a) le categorie di dati personali coinvolte dalle operazioni di trattamento;
- b) le tipologie di soggetti i cui dati personali saranno trattati;
- c) le operazioni di trattamento previste;
- d) le modalità tecniche, tecnologiche ed organizzative di erogazione del servizio;
- e) le modalità, tecniche ed organizzative, mediante le quali intende assistere il Titolare nel dare riscontro alle richieste di esercizio dei diritti da parte dell’interessato, nel rispetto dei termini previsti dall’art. 12 del GDPR;
- f) le attività e gli oneri (esclusi quelli di carattere economico) previsti a carico del Titolare, necessari per consentire la sicurezza del trattamento dei dati personali e la sua conformità alla normativa.
- g) l’esistenza di disposizioni normative o dell’Autorità che impongano una conservazione dei dati personali trattati per conto del Titolare, anche oltre la scadenza del servizio affidato (e relativi tempi di conservazione);

4. Il Responsabile dovrà inoltre dimostrare - mediante la produzione di adeguata documentazione - di possedere esperienza, capacità e affidabilità idonee a garantire il rispetto delle disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza, ed in ogni caso di essere in grado di fornire garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti della normativa e garantisca la tutela dei diritti dell’Interessato.

5. La documentazione di cui al paragrafo precedente dovrà espressamente contenere:

- a) informazioni relative al possesso di certificazioni relative alla protezione dei dati e, più in generale, alla sicurezza ed alla gestione degli stessi (a mero titolo esemplificativo, categoria ISO/IEC 27000);
- b) informazioni relative alla qualificazione e presenza nel catalogo dei servizi cloud qualificati per la PA di AgID e/o relative alla qualificazione e sottoscrizione di un accordo di servizio con PagoPA SpA;
- c) la descrizione (tipologica) delle misure di sicurezza adottate per prevenire perdite di integrità, disponibilità e confidenzialità dei dati personali, con riferimento ai luoghi fisici ove avverranno le operazioni di trattamento;
- d) la descrizione (tipologica) delle misure di sicurezza adottate per prevenire perdite di integrità, disponibilità e confidenzialità dei dati personali, con riferimento all’infrastruttura tecnologica (hardware e software) utilizzata per il trattamento;
- e) la descrizione delle misure organizzative e di formazione adottate con riferimento al personale addetto alle operazioni di trattamento per conto del Titolare;
- f) la descrizione delle procedure di acquisizione dei dati personali presso il Titolare del trattamento e di quelle di riconsegna al termine dell’affidamento;
- g) le modalità, anche tecniche e le procedure mediante le quali il Responsabile intende assicurare l’esattezza, la veridicità, l’aggiornamento, la pertinenza e la non eccedenza dei

dati personali oggetto di trattamento, per conto del Titolare, rispetto alle finalità per le quali sono stati raccolti e saranno successivamente trattati;

h) la dichiarazione di non esser stato destinatario di provvedimenti sanzionatori o correttivi definitivi ad opera del Garante per la protezione dei dati personali o di altra Autorità di controllo o, in alternativa, l'indicazione dei provvedimenti subiti;

i) l'indicazione in merito all'avvenuta designazione del Responsabile per la protezione dei dati personali (RPD o DPO), ovvero dichiarazione di non sottostare a tale obbligo;

l) l'indicazione in merito alla tenuta dei registri delle attività di trattamento, ovvero dichiarazione di non sottostare a tale obbligo;

6. Qualora, in relazione al trattamento di dati personali effettuato dal Responsabile per conto di altro Titolare in fattispecie assimilabile a quella oggetto di affidamento, sia già stata effettuata una valutazione d'impatto sulla protezione dei dati personali - ai sensi dell'articolo 35 del GDPR – il Responsabile ne fornisce indicazione nella propria offerta, impegnandosi a prestare al Titolare la collaborazione necessaria a condurre la propria valutazione.

7. Ove il fornitore intenda trasferire all'estero i dati personali oggetto di trattamento per conto del Titolare, ne dovrà fare espressa menzione, indicando:

a) il paese nel quale s'intendono trasferire i dati personali;

b) le categorie di dati personali oggetto di trasferimento;

c) le tipologie di soggetti i cui dati personali saranno trasferiti;

d) le operazioni di trattamento previste a seguito del trasferimento;

e) ove il trasferimento avvenga verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, l'indicazione circa le modalità ed i termini che garantiscono il rispetto delle disposizioni contenute nel capo V del GDPR.

8. Nel caso il fornitore intenda ricorrere ad altro soggetto ("Sub-responsabile") per eseguire tutte o parte delle operazioni di trattamento per conto del Titolare, ne deve fare espressa menzione, al fine di consentire al Titolare di compiere le valutazioni necessarie al rilascio della prescritta autorizzazione. A tal fine il Responsabile specifica, per ciascun Sub-responsabile:

a) i dati identificativi, fiscali e di contatto del Sub-responsabile;

b) le categorie dei dati personali il cui trattamento avverrà ad opera del Sub-responsabile;

c) le tipologie di soggetti i cui dati personali saranno trattati dal Sub-responsabile;

d) le operazioni di trattamento a carico del Sub-responsabile;

e) il possesso, da parte del Sub-responsabile, di certificazioni, qualificazioni o simili, in relazione al trattamento dei dati;

f) la dichiarazione di aver verificato che il Sub-responsabile presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato;

g) nel caso il trattamento ad opera del Sub-responsabile preveda il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, dovrà essere specificato se tale trasferimento sia conseguente ad una libera scelta imprenditoriale, ovvero imposto dal diritto dell'Unione europea o nazionale cui è soggetto il Responsabile del trattamento (salvo che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico).

9. In relazione alla gestione degli eventi costituenti violazione di dati personali (data breach), il Responsabile dichiara:

a) di aver (o non avere) adottato una apposita procedura di gestione;

b) di aver preso conoscenza dell'apposita procedura di gestione adottata dal Titolare;

c) di aver (o non avere) predisposto e tenuto aggiornato un registro interno delle violazioni di dati personali.

## **PROTEZIONE DEI DATI PERSONALI - INFORMAZIONI**

1. L'Ente tratta i dati personali raccolti in occasione della partecipazione alla presente procedura selettiva, nel pieno rispetto del Regolamento UE 2016/679 e della normativa nazionale di protezione, al solo scopo e per il solo tempo necessari al perseguimento delle proprie finalità istituzionali. In particolare, la raccolta sarà limitata ai dati personali strettamente necessari, i quali saranno oggetto di valutazione al fine di verificare il possesso dei requisiti previsti dalla presente procedura selettiva nonché per istruire il successivo procedimento ed adottare il provvedimento finale.

2. Sono raccolti e, comunque, trattati, i dati relativi alle persone fisiche che, in ragione della propria appartenenza alla struttura organizzativa del partecipante, sono soggetti all'obbligo di fornire documenti, informazioni e dichiarazioni rilevanti ai fini della procedura. I dati personali potranno altresì essere acquisiti presso altre pubbliche amministrazioni o presso banche dati pubbliche.

3. Il trattamento dei dati prescinde il consenso dell'interessato in quanto necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento, ai sensi dell'articolo 6 del Regolamento (UE) 2016/679.

4. I dati personali potranno essere comunicati ad altre pubbliche amministrazioni e potranno essere oggetto di confronto con altri dati già in possesso di questo Ente, nei limiti in cui ciò si renda necessario.

5. I dati personali saranno diffusi, limitatamente a quanto imposto dalle vigenti norme di legge.

6. La conservazione dei dati avverrà per il tempo necessario al perseguimento delle descritte finalità e, comunque, sotto l'osservanza della disciplina in materia di conservazione dei documenti amministrativi.

7. Maggiori e dettagliate informazioni, anche in relazione ai diritti e relative modalità di esercizio, spettanti all'interessato, possono essere reperite sul sito web istituzionale, alla pagina raggiungibile all'indirizzo: <https://www.comune.finalefigure.sv.it/privacy>