Comune di Sestu

Città Metropolitana di Cagliari

Informativa sul trattamento dei dati personali (Art. 13 del Regolamento UE 679/2016)

Allegato Privacy

Il presente Allegato è redatto in conformità a quanto previsto all'art. 28 del Regolamento (UE) 2016/679 e forma parte integrante e sostanziale del Contratto stipulato tra le Parti.

Ti ricordiamo che per trattamento di dati personali deve intendersi qualunque operazione o complesso di operazioni, effettuati con o senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati, anche se non registrati in una banca dati.

La presente informativa si applica quando visiti il nostro sito web; quando usi i nostri servizi e utilizzi i nostri moduli; quando richiedi la nostra assistenza oppure sei un fornitore, partner, consulente o qualsiasi altro soggetto che abbia rapporti con il Comune di Sestu.

Le informazioni ed i dati da te forniti saranno trattati nel rispetto delle vigenti norme e Regolamenti in materia (incluso, a titolo esemplificativo ma non limitativo, il Regolamento Generale sulla Protezione dei Dati - Regolamento UE 2016/679 - General Data Protection Regulation o "GDPR").

Il soggetto accreditato si impegna a presentare all'Amministrazione garanzie in termini di conoscenza specialistica, affidabilità, risorse, nonché in ordine all'adozione di misure tecniche, logiche ed organizzative adeguate per assicurare che i trattamenti dei dati personali siano conformi alle esigenze del Regolamento Europeo e, dunque, ai sensi dell'articolo 28 del Regolamento Europeo e con la sottoscrizione del patto di accreditamento dichiara di essere consapevole, in ragione delle prestazioni da eseguire con lo specifico affidamento.

Il mancato rispetto del trattamento delle disposizioni di cui al presente Allegato sarà considerato un grave inadempimento del patto stesso.

PREMESSA:

OGGETTO

Il presente documento disciplina le istruzioni che il soggetto accreditato si impegna ad osservare nell'ambito dei trattamenti dei dati personali che realizzerà per conto del Comune di Sestu quale Titolare (nel presente documento anche solo "**Amministrazione**") nello svolgimento delle attività in essere con l'Amministrazione, garantendo il rispetto della normativa vigente in materia di tutela e sicurezza dei dati.

DEFINIZIONI

- "*Dati Personali dell'Amministrazione*": i Dati Personali (nonché i dati appartenenti alle categorie particolari di dati personali di cui all'art. 9 e 10 del Regolamento UE 2016/679), concessi in licenza o diversamente messi a disposizione, trasmessi, gestiti, controllati o comunque trattati dall'Amministrazione;

- "*Norme in materia di Trattamento dei Dati Personali*": tutte le leggi, disposizioni e direttive normative applicabili in relazione al trattamento e/o alla protezione dei Dati Personali, così come modificate di volta in volta, ivi incluso, ma non limitatamente, il Regolamento UE 2016/679 (GDPR), la normativa di adeguamento italiana, circolari, pareri e direttive dell'Autorità di Controllo nazionale, le decisioni interpretative adottate dallo European Data Protection Board;

- "*Misure di Sicurezza*": le misure di sicurezza di natura fisica, logica, tecnica e organizzativa adeguate a garantire un livello di sicurezza adeguato al rischio;

- "*Dati Personali*": qualsiasi informazione relativa a una persona fisica identificata o identificabile (interessato) come definita nelle Norme in materia di Trattamento dei Dati Personali;

- "*Trattamento*": qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a Dati Personali o insieme di Dati Personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o, qualsiasi altra forma messa a disposizione, il raffronto o l'interconnessione, la limitazione, allineamento o combinazione, la cancellazione o la distruzione;

- "*Titolare del trattamento*": la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione europea o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri; ovvero l'Amministrazione;

- "*Responsabile del trattamento*": la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare o del Contitolare del trattamento; ovvero il soggetto accreditato;

- "*Sub-Responsabile del trattamento*": la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che svolge in forza di contratto scritto con altro Responsabile del trattamento; ovvero il subappaltatore o subfornitore autorizzato dall'Amministrazione;

- “*Soggetto accreditato*”: soggetto accreditato designato quale Responsabile primario, in funzione della designazione fatta dall’Amministrazione in qualità di Titolare;

- “*Persone autorizzate al trattamento dei dati*”: persone che in qualità di dipendenti, collaboratori, amministratori o consulenti del responsabile e/o del sub-responsabile siano state autorizzate al trattamento dei dati personali sotto l’autorità diretta del Responsabile primario o del Sub responsabile;

- “*Terzi autorizzati*”: persone terze, ovvero la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento, che in qualità di dipendenti, collaboratori, amministratori (anche amministratori di sistema) o consulenti del soggetto accreditato siano state autorizzate al trattamento dei dati personali sotto l'autorità diretta del Responsabile primario o del Sub- Responsabile;

- “Violazione dei dati personali (data breach)”: la violazione di sicurezza che comporta 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;

- “Incidente di sicurezza”: la violazione di sicurezza che comporta la perdita, la modifica, la divulgazione non autorizzata o l’accesso a dati e/o informazioni riservate (non dati personali), la violazione e/o il malfunzionamento di misure di sicurezza, di strumenti elettronici, hardware o software a protezione dei dati e delle informazioni.

Finalità del trattamento e base giuridica

I dati di natura personale forniti, saranno trattati nel rispetto delle condizioni di liceità ex art. 6 Reg. UE 2016/679, per le seguenti finalità:

erogazione delle prestazioni integrative, finalizzate all’assistenza domiciliare di supporto alla non autosufficienza e allo stato di fragilità, in favore dei soggetti beneficiari del **Progetto Home Care Premium 2025-2028**, nonché per l’adempimento di ogni altro obbligo derivante.

Titolare del trattamento dei dati

Titolare del trattamento dei dati è il Comune di Sestu, con sede in Sestu (CA), in Via Scipione, n. 1, C.F. 80004890929, P.I. 01098920927, tel: 0702360287, al quale ci si potrà rivolgere per esercitare i diritti degli interessati. Indirizzo email del Titolare: protocollo.sestu@pec.it; Posta Elettronica certificata (PEC): protocollo.sestu@pec.it

Responsabile della protezione dei dati

Il Responsabile della Protezione dei Dati o “Data Protection Officer” (RPD/DPO) nominato è contattabile ai seguenti recapiti:
• Email: privacy@comune.it
• PEC: privacy@pec.comune.it
I dati di contatto del RPD/DPO (comprensivi di nominativo ecc.) sono altresì pubblicati in alcune sezioni del sito internet istituzionale dell’Ente, quali la sezione “privacy” accessibile già dalla homepage, quella relativa all’”organigramma dell’Ente e relativi dati di contatto”, nonché nella sezione amministrazione trasparente.

Dati degli utenti

Al fine di poter consentire l’erogazione dei servizi previsti, ed ottemperare gli obblighi previsti dalle normative vigenti, il Comune di Sestu raccoglierà i seguenti dati relativi ai clienti: Nome – Cognome - Ragione sociale (in caso di soggetto diverso dal privato) - Codice fiscale - Partita Iva (in caso di soggetto diverso dal privato) - Indirizzo - Città - Cap - Provincia - Recapiti Telefonici - Indirizzi Email e altri dati necessari all'espletamento del servizio. Tali dati verranno conservati per le finalità di erogazione dei servizi, per la durata di 10 anni a decorrere dalla cessazione del rapporto. Per scopi di natura fiscale e per gli altri obblighi previsti dalla legge, gli stessi dati verranno conservati per 10 anni, salvo che la legge non permetta un periodo di conservazione più lungo, anche in ragione del maturare della prescrizione di eventuali diritti vantati da terzi.

Dati dei soggetti accreditati

Al fine di garantire la regolare erogazione delle prestazioni integrative ci occorrono i dati di contatto dei soggetti pertinenti che operano (come nomi, cognomi, numeri di telefono ed indirizzi e-mail. Per le finalità suddette, i dati verranno conservati per la durata di un anno a decorrere dalla cessazione del Progetto HCP 2025-2028. Per scopi di natura fiscale e per gli altri obblighi previsti dalla legge, i dati verranno conservati per 10 anni, salvo che la legge non permetta un periodo di conservazione più lungo, anche in ragione del maturare della prescrizione di eventuali diritti vantati da terzi.

SICUREZZA DEI DATI PERSONALI

L'affidatario ottempererà a tutte le norme in materia di Trattamento dei Dati Personali in relazione al Trattamento dei Dati Personali ivi comprese quelle che saranno emanate nel corso della durata del Progetto HCP 2025-2028 al fine di assicurare, nell'ambito delle proprie attività e competenze specifiche, un adeguato livello di sicurezza dei trattamenti, inclusa la riservatezza, in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, modifica, divulgazione non autorizzata, nonché di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta.

Obbligo di conferimento dei dati

Qualora il conferimento al trattamento dei dati personali non costituisca obbligo di legge o contrattuale, il mancato conferimento potrebbe comportare difficoltà, per la competente Struttura, di erogare la prestazione richiesta.

Destinatari del trattamento

I destinatari dei dati personali raccolti sono:

soggetti che forniscono i servizi connessi alla riscossione dei pagamenti (ad esempio bonifico bancario, carta di credito);

altri enti, consulenti o autorità cui, per motivi o obblighi di legge, sia necessario comunicare i dati personali;

I dati di natura personale forniti saranno comunicati a destinatari, che tratteranno i dati in qualità di responsabili (art. 28 del Reg. UE 2016/679) e/o in qualità di persone fisiche che agiscono sotto l'autorità del Titolare e del Responsabile (art. 29 del Reg. UE 2016/679), per le finalità sopra elencate. Precisamente, i dati saranno comunicati a:

Comuni del PLUS 21

INPS

I soggetti appartenenti alle categorie suddette svolgono la funzione di Responsabile del trattamento dei dati, oppure operano in totale autonomia, come distinti Titolari del trattamento.

OBBLIGHI E ISTRUZIONI PER IL SOGGETTO ACCREDITATO

I. OBBLIGHI GENERALI DEL SOGGETTO ACCREDITATO

1. Il Soggetto accreditato è autorizzato a trattare per conto dell'Amministrazione i dati personali necessari per l'esecuzione delle attività di cui all'oggetto del Programma Home Care 2025-2028.

2. A tal fine il soggetto accreditato si impegna a:

- non determinare o favorire mediante azioni e/o omissioni, direttamente o indirettamente, la violazione da parte dell'Amministrazione delle Norme in materia di Trattamento dei Dati Personali;

- trattare i Dati Personali esclusivamente in conformità alle istruzioni documentate dell'Amministrazione, nella misura ragionevolmente necessaria all'esecuzione del Contratto, e alle Norme in materia di Trattamento dei Dati Personali;

- adottare, implementare e aggiornare Misure di sicurezza adeguate a garantire la protezione e la sicurezza dei Dati Personali al fine di prevenire a titolo indicativo e non esaustivo:

• incidenti di sicurezza; violazioni dei dati personali (Data Breach);

• ogni violazione delle Misure di sicurezza;

• tutte le altre forme di Trattamento dei dati non autorizzate o illecite.

3. Il soggetto accreditato si impegna a designare la figura professionale del Responsabile della protezione dei dati di cui all'art. 37 GDPR e a comunicarne i dati e i contatti di riferimento tempestivamente all'Amministrazione, in ragione dell'attività svolta.

II. ISTRUZIONI PER IL SOGGETTO ACCREDITATO.

II.A) Elementi essenziali dei trattamenti che il soggetto accreditato è stato autorizzato a svolgere dall'Amministrazione.

Gli elementi essenziali del trattamento sono contenuti nel presente documento, nonché nei documenti tecnico – funzionali che saranno rilasciati dall'Amministrazione in ragione delle prestazioni richieste in corso di esecuzione.

In particolare i citati documenti conterranno la materia disciplinata, la natura e finalità del trattamento, il tipo di dati personali trattati e le categorie di Interessati.

Salvo quanto dovesse essere previsto nei documenti di cui al presente paragrafo, le Parti si danno reciprocamente atto che, alla Data di Efficacia del presente Allegato le attività che prevedono il trattamento dei dati dell'Amministrazione sono: la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione

• la durata del trattamento dei dati personali è limitata, dunque coincide, con la durata del Progetto HCP 2025-2028 e delle sue eventuali proroghe;

- la natura e lo scopo del trattamento, tenuti conto i requisiti di legittimità stabiliti dalle leggi vigenti in materia di protezione dei dati, è l'erogazione degli interventi di cui al programma HOME CARE PREMIUM 2025-2028;

- i Dati Personali dell'Amministrazione sono i dati del sistema informativo dallo stesso trattati per lo svolgimento delle attività di cui al Programma Home Care Premium 2025-2028;

i dati connessi alla gestione del programma Home Care Premium 2025-2028, sono quelli di seguito elencati:

- dati identificativi dell'interessato (nome, cognome, C.F. cittadinanza);

- dati situazione economica e reddituale

- dati di contatto (indirizzo di residenza, e-mail, telefono)

- composizione nucleo familiare anagrafico

- condizione socio sanitaria

- il soggetto accreditato, al temine delle attività affidate e comunque entro il termine della durata programmata, come eventualmente prorogato, elimina, con tecniche adeguate e sicure, i dati dal sistema informatico in suo possesso;

- Titolare del trattamento dei dati è il Comune di Sestu, con sede in Sestu (CA), in Via Scipione, n. 1, C.F. 80004890929, P.I. 01098920927, tel: 0702360287, al quale ci si potrà rivolgere per esercitare i diritti degli interessati. Indirizzo e-mail del titolare: protocollo.sestu@pec.it; Posta Elettronica certificata (PEC): protocollo.sestu@pec.it. Il Responsabile della Protezione dei Dati o "Data Protection Officer" (RPD/DPO) nominato è contattabile ai seguenti recapiti:
- e-mail: privacy@comune.it
- pec: privacy@pec.comune.it

II.B) Obblighi del Responsabile del trattamento nei confronti dell'Amministrazione.

Il Responsabile del trattamento si impegna a:

1. trattare i dati solo per l'esecuzione delle attività di cui all'oggetto dell'Avviso di accreditamento;

2. trattare i dati conformemente alle istruzioni documentate impartite dall'Amministrazione con il presente Allegato e con eventuali istruzioni documentate aggiuntive. Qualora il soggetto accreditato reputi che un'istruzione sia, o possa essere, contraria alla Normativa in materia di protezione dei dati, ivi incluso il GDPR, deve informarne immediatamente l'Amministrazione;

3. trattare i dati conformemente alle istruzioni documentate dell'Amministrazione di cui al precedente comma anche nei casi di trasferimento dei dati verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il soggetto accreditato; in tale ultimo caso il soggetto accreditato dovrà informare l'Amministrazione di tale obbligo giuridico prima che il trattamento abbia inizio, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.

4. garantire che il trattamento dei Dati Personali sia effettuato in modo lecito, corretto, adeguato, pertinente e avvenga nel rispetto dei principi di cui all'artt. 5 e ss. del GDPR;

5. garantire la riservatezza dei dati personali trattati per l'esecuzione delle attività connesse al

programma HCP 2025-2028;

6. garantire che le persone autorizzate a trattare i dati personali in virtù dell'accreditamento: **i)** si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza; **ii)** abbiano ricevuto, e ricevano, da parte del soggetto accreditato accreditato la formazione necessaria in materia di protezione dei dati personali; **iii)** accedano e trattino i dati personali osservando le istruzioni impartite dall'Amministrazione.

7. tenere conto nell'esecuzione delle attività previste dei principi della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (privacy by design e by default) anche mediante l'ausilio delle istruzioni documentate impartite dal Titolare del trattamento;

8. conferire all'Amministrazione eventuale copia dei dati personali dei dipendenti, amministratori, consulenti, collaboratori o altro personale del soggetto accreditato nel corso delle attività oggetto del programma HCP 2025-2028 esclusivamente per finalità relative all'esecuzione delle attività previste oltre che per la sicurezza delle sedi e dei sistemi. Il soggetto accreditato, con la sottoscrizione dell'Addendum, autorizza l'Amministrazione, esclusivamente per le suddette finalità, ad estrarre tali dati personali dai propri sistemi informativi.

Qualora richiesto dalle Norme in materia di Trattamento dei Dati Personali, l'Amministrazione e il soggetto accreditato convengono di sottoscrivere un accordo aggiuntivo, di modifica o di aggiornamento che potrà essere necessario anche per consentire il trasferimento di tali dati personali qualora non rientrino nella sua giurisdizione di origine ai sensi delle Norme sul Trattamento dei Dati Personali.

II.C) Obblighi del soggetto accreditato nell'ambito dei diritti esercitati dagli Interessati nei confronti dell'Amministrazione.

1. Il soggetto accreditato deve collaborare e supportare nel dare riscontro scritto, anche di mero diniego, alle istanze trasmesse dagli Interessati nell'esercizio dei diritti previsti dagli artt. 15-23 del GDPR, ovverosia alle istanze per l'esercizio del diritto di accesso, di rettifica, di integrazione, di cancellazione e di opposizione, diritto alla limitazione del trattamento, diritto alla portabilità dei dati, diritto a non essere oggetto di un processo decisionale automatizzato, compresa la profilazione.

2. Il soggetto accreditato deve dare supporto, in tale attività, affinché il riscontro alle richieste di esercizio dei diritti degli Interessati avvenga senza giustificato ritardo.

3. A tal fine il soggetto accreditato deve adottare e aggiornare un registro di tutte le attività di trattamento eseguite per conto dell'Amministrazione completo di tutte le informazioni previste all'art. 30 del GDPR (cfr. successivo paragrafo III del presente Allegato) e mettere tale registro a disposizione dell'Amministrazione affinché si possa ottemperare senza ingiustificati ritardi alle istanze formulate dagli Interessati ai sensi degli artt. 15-23 del GDPR.

4. Qualora gli Interessati esercitino un diritto previsto dal GDPR trasmettendo la relativa richiesta al soggetto accreditato, quest'ultimo deve inoltrarla tempestivamente, e comunque entro e non oltre 3 giorni dalla ricezione, per posta elettronica all'Amministrazione.

II.D) Obblighi del soggetto accreditato che ricorre a Terzi Autorizzati.

1. Il soggetto accreditato può ricorrere a Terzi Autorizzati per l'esecuzione di specifiche attività di trattamento esclusivamente nei casi in cui abbia ricevuto espressa autorizzazione scritta dall'Amministrazione.

2. Nell'ipotesi in cui il soggetto accreditato, previa autorizzazione scritta dell'Amministrazione, abbia designato un Terzo Autorizzato, il soggetto accreditato e il Terzo autorizzato dovranno essere vincolati da un accordo scritto recante tutti gli obblighi in materia di protezione dei dati di cui all'Avviso di accreditamento e di cui alle ulteriori eventuali istruzioni documentate aggiuntive impartite dall'Amministrazione.

3. Il soggetto accreditato deve formulare per iscritto all'Amministrazione la domanda di autorizzazione alla nomina di un Terzo Autorizzato, specificando: i) le attività di trattamento da delegare; ii) il nominativo/ragione sociale e gli indirizzi del Terzo; iii) i requisiti di affidabilità ed esperienza - anche in termini di competenze professionali, tecniche e organizzative nonché con riferimento alle misure di sicurezza - del Terzo in materia di trattamento dei dati personali; iv) il contenuto del relativo contratto tra il Fornitore e il Terzo autorizzato.

4. In particolare, il soggetto accreditato deve garantire che il Terzo Autorizzato assicuri l'adozione di misure, logiche, tecniche ed organizzative adeguate alla normativa e regolamentazione in materia ed alle istruzioni impartite dall'Amministrazione in materia di protezione dei dati personali.

5. Resta, in ogni caso, ferma la successiva facoltà dell'Amministrazione di opporsi all'aggiunta o sostituzione del Terzo Autorizzato con altri soggetti Terzi.

6. Le istruzioni impartite dal soggetto accreditato a qualsiasi Terzo dovranno avere il medesimo contenuto e perseguire i medesimi obiettivi delle istruzioni fornite dall'Amministrazione nei limiti dei trattamenti autorizzati in capo al Terzo.

7. A tal fine, l'Amministrazione può in qualsiasi momento verificare le garanzie e le misure tecniche ed organizzative del Terzo Autorizzato, anche per mezzo di audit, assessment, sopralluoghi e ispezioni svolti mediante il proprio personale oppure tramite soggetti terzi. Nel caso in cui tali garanzie risultassero insussistenti l'Amministrazione, in conformità a quanto contrattualmente previsto, può risolvere il contratto con il soggetto accreditato. Nel caso in cui all'esito delle verifiche, ispezioni, audit e assessment le misure di sicurezza dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione delle Norme in materia di protezione dei dati personali, l'Amministrazione applicherà al soggetto accreditato una penale come contrattualmente previsto e diffiderà lo stesso a far adottare al Terzo Autorizzato tutte le misure più opportune entro un termine congruo che sarà all'occorrenza fissato (tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, della tipologia dei dati e della categoria dei soggetti interessati coinvolti nonché del livello di rischio relativo alla violazione dei dati, alla gravità della violazione verificatasi e degli incidenti di sicurezza). In caso di mancato adeguamento da parte del Terzo Autorizzato e/o del soggetto accreditato a tale diffida l'Amministrazione potrà risolvere il Contratto ed escutere la garanzia definitiva, fatto salvo il risarcimento del maggior danno.

III. IL REGISTRO DEI TRATTAMENTI DEL SOGGETTO ACCREDITATO.

1. Il soggetto accreditato è obbligato a predisporre, conservare, aggiornare - anche con l'ausilio del proprio Responsabile della protezione dei dati - un registro, in formato elettronico di tutte le categorie di attività relative al trattamento (o ai trattamenti) svolti per conto del Titolare del Trattamento, come prevede l'art. 30, comma 2, del GDPR.

2. In particolare, il Registro del soggetto accrediato dei trattamenti svolti per conto dell'Amministrazione deve contenere:

i) il nome e i dati di contatto del soggetto accreditato (e, se del caso, di Terzi Autorizzati) del trattamento, di ogni Titolare del trattamento per conto del quale il soggetto accreditato agisce, del rappresentante (eventuale) del soggetto accreditato e del Terzo Autorizzato, nonché del Responsabile della protezione dei dati (DPO); **ii)** le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;

iii) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49 del GDPR, la documentazione delle garanzie adeguate;

iv) una descrizione generale delle misure di sicurezza tecniche e organizzative messe in atto per un trattamento corretto e sicuro ai sensi dell'articolo 32 del GDPR.

IV. OBBLIGHI DI SUPPORTO, COLLABORAZIONE E COORDINAMENTO DEL RESPONSABILE DEL TRATTAMENTO NELL'ATTUAZIONE DEGLI OBBLIGHI DELL'AMMINISTRAZIONE.

Il Responsabile del trattamento assiste e collabora pienamente con l'Amministrazione nel garantire il rispetto degli obblighi di cui agli articoli 31, 32, 33, 34, 35 e 36 del GDPR, come di seguito descritto.

IV.A) Misure di sicurezza.

Il soggetto accreditato deve mettere in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio e garantire il rispetto degli obblighi di cui all'art. 32 del GDPR. I criteri per la valutazione del rischio devono essere previamente condivisi e approvati dall'Amministrazione. Tali misure comprendono tra le altre:

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.

Il soggetto accreditato si obbliga ad adottare le misure di sicurezza previste da codici di condotta di settore ove esistenti e dalle certificazioni ove acquisite (art. 40 -43 GDPR).

Nel valutare l'adeguatezza del livello di sicurezza il soggetto accreditato deve tenere conto in special modo dei rischi presentati dal trattamento (o dai trattamenti), che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, o dal trattamento non consentito o non conforme alle finalità della raccolta, ai dati personali trasmessi, conservati o comunque trattati.

Nell’effettuare l’analisi dei rischi il soggetto accreditato utilizza i criteri di valutazione del rischio condivisi ed approvati dall’Amministrazione. All’esito dell’analisi dei rischi, le misure di sicurezza adeguate ai sensi dell’art. 32 del GDPR devono essere condivise ed approvate dall’Amministrazione.

I risultati dell’analisi del rischi per l’individuazione delle misure di sicurezza adeguate andranno riportati dal soggetto accreditato in un apposito documento contenente almeno le seguenti informazioni: identificazione e classificazione dei dati personali trattati anche in termini di riservatezza ed integrità; classificazione del trattamento anche in termini di disponibilità; valutazione dei rischi per l’interessato e inerenti il trattamento stesso; l’identificazione delle misure di sicurezza così come richieste ai sensi dell’articolo 32 del GDPR.

L’attività di identificazione dei dati personali oggetto del trattamento dovrà seguire i criteri di privacy by default di cui all’art. 25 del GDPR.

Ai sensi dell’art. 32, comma 4, GDPR il soggetto accreditato deve garantire che chiunque agisca sotto la sua autorità e abbia accesso ai Dati Personali non tratti tali dati se non debitamente istruito, salvo che lo richieda il diritto dell’Unione o degli Stati membri.

IV.B) Obblighi del soggetto accreditato nelle ipotesi di “data breach”.

Il soggetto accreditato deve assistere e collaborare pienamente con l’Amministrazione, nelle attività di adempimento di cui agli articoli 33 e 34 del GDPR in materia di violazioni di dati personali, ovvero di data breach.

In particolare, il soggetto accreditato deve:

- predisporre e aggiornare un registro contenente tutte le violazioni dei dati personali sia dai trattamenti eseguiti per conto dell’Amministrazione, al fine di facilitare quest’ultima nelle attività di indagine a seguito di data breach;

- comunicare all’Amministrazione, tempestivamente e in ogni caso senza ingiustificato ritardo, che si è verificata una violazione dei dati personali da quando il soggetto accreditato, o un suo Terzo Autorizzato, ne ha avuto conoscenza o ha avuto elementi per sospettarne la sussistenza. Tale comunicazione deve essere redatta in forma scritta, in modo conforme ai criteri previsti dall’art. 33 del GDPR e deve essere trasmessa unitamente a ogni documentazione utile all’Amministrazione per consentirle di notificare la violazione all’Autorità di controllo competente entro e non oltre il termine di 72 ore da quando ne ha avuto conoscenza;

- indagare sulla violazione di dati personali adottando tutte le misure tecniche e organizzative e le misure rimediali necessarie a eliminare o contenere l’esposizione al rischio, collaborare con l’Amministrazione nelle attività di indagine, mitigando qualsivoglia danno o conseguenza lesiva dei diritti e delle libertà degli Interessati (misure di mitigazione) nonché ponendo in atto un piano di misure, previa approvazione dell’Amministrazione, per la riduzione tempestiva delle probabilità che una violazione simile di dati personali possa ripetersi;

- nel caso in cui l’Amministrazione debba fornire informazioni (inclusi i dettagli relativi ai servizi prestati dal Fornitore) all’Autorità di controllo il soggetto accreditato supporterà l’Amministrazione nella misura in cui le informazioni richieste e/o necessarie per l’Autorità di controllo siano esclusivamente in possesso del Fornitore e/o di suoi Terzi Autorizzati.

IV.C) Obblighi del soggetto accreditato nella valutazione d’impatto del rischio di violazioni dei Dati Personali.

1. Per svolgere la valutazione d'impatto dei trattamenti sulla protezione dei dati personali l'Amministrazione può consultarsi con il proprio Responsabile della protezione dei dati (art. 35, comma 2, del GDPR).

2. Il Responsabile del trattamento si impegna ad assistere l'Amministrazione, a livello tecnico e organizzativo, nello svolgimento della valutazione d'impatto, così come disciplinata dall'art. 35 del GDPR, in tutte le ipotesi in cui il trattamento preveda o necessiti della preliminare valutazione di impatto sulla protezione dei dati personali (di seguito anche "**PIA**") o dell'aggiornamento della PIA.

3. I risultati della valutazione d'impatto ex art. 35 del GDPR per l'individuazione delle misure di sicurezza necessarie andranno riportati dal nel documento di analisi del rischio di cui al precedente art. **IV.A).**

4. Il soggetto accreditato si impegna altresì ad assistere l'Amministrazione nell'attività di consultazione preventiva dell'Autorità di controllo ai sensi dell'articolo 36 del GDPR.

V. ULTERIORI OBBLIGHI DI GARANZIA DEL SOGGETTO ACCREDITATO DEL TRATTAMENTO.

1. Il soggetto accreditato si impegna ad operare adottando tutte le misure tecniche e organizzative, le attività di formazione, informazione e aggiornamento ragionevolmente necessarie per garantire che i Dati Personali siano precisi, corretti e aggiornati durante l'intera durata del trattamento - anche qualora il trattamento consista nella mera custodia o attività di controllo dei dati - eseguito dal soggetto accreditato, o da un Terzo da lui autorizzato, nella misura in cui il soggetto accreditato sia in grado di operare in tal senso.

2. Il soggetto accreditato si impegna a trasmettere all'Amministrazione tutte le informazioni e la documentazione che quest'ultima potrà ragionevolmente richiedere fine di verificare la conformità del soggetto accreditato (o del Terzo Autorizzato come sub-appaltatore e sub-fornitore) con il presente Allegato, le Norme in materia di Trattamento dei Dati Personali e le Misure di sicurezza.

3. Il soggetto accreditato garantisce all'Amministrazione, o ai suoi rappresentanti debitamente autorizzati, la possibilità di svolgere, con ragionevole preavviso, attività di controllo e valutazione, anche mediante ispezioni e sopralluoghi condotte da soggetti autorizzati e incaricati dall'Amministrazione, delle attività di trattamento dei Dati Personali eseguite dal medesimo soggetto accreditato, ivi incluso l'operato degli eventuali amministratori di sistema, allo scopo di verificarne la conformità con il Contratto (ivi inclusi i rispettivi Allegati), con le Istruzioni dell'Amministrazione e le Norme in materia di Trattamento dei Dati. Il soggetto accreditato deve mettere a disposizione dell'Amministrazione senza alcun ritardo e/o omissione, tutte le informazioni necessarie per dimostrare la sua conformità con gli obblighi previsti. Nel caso in cui all'esito delle verifiche periodiche, delle ispezioni, audit e assessment le misure tecniche, organizzative e/o di sicurezza risultino inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, l'Amministrazione applicherà al soggetto accreditato le penali diffidandolo ad adottare le misure necessarie entro un termine congruo che sarà all'occorrenza fissato (tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, della tipologia dei dati e della categoria dei soggetti interessati coinvolti nonché del livello di rischio violazione e/o della gravità della violazione verificatasi). In caso di mancato adeguamento da parte del soggetto accreditato a tale diffida l'Amministrazione potrà risolvere il Contratto ed escutere la garanzia definitiva, fatto salvo il risarcimento del maggior danno.

4. Fatto salvo quanto previsto al successivo paragrafo VI il soggetto accreditato non può trasferire i Dati Personali verso un paese terzo o un'organizzazione internazionale, salvo che non abbia preventivamente ottenuto autorizzazione scritta da parte dell'Amministrazione.

5. Il soggetto accreditato si impegna a notificare tempestivamente all'Amministrazione ogni provvedimento di un'Autorità di controllo, o dell'Autorità giudiziaria relativo ai Dati Personali dell'Amministrazione salvo il caso in cui tale comunicazione non sia vietata dal provvedimento o dalla legge.

6. In simili circostanze, salvo divieti previsti dalla legge, il soggetto accreditato deve: i) informare l'Amministrazione tempestivamente, e comunque entro 24 ore dal ricevimento della richiesta di ostensione; ii) collaborare con l'Amministrazione, nell'eventualità in cui lo stesso intenda opporsi legalmente a tale comunicazione; iii) garantire il trattamento riservato di tali informazioni.

7. Il soggetto accreditato prende atto e riconosce che, nell'eventualità di una violazione delle disposizioni del presente Allegato, oltre all'applicazione delle clausole di risoluzione del contratto e delle penali, nonché all'eventuale risarcimento del maggior danno, l'Amministrazione avrà la facoltà di ricorrere a provvedimenti cautelari, ingiuntivi e sommari o ad altro rimedio equitativo, allo scopo di interrompere immediatamente, impedire o limitare il trattamento, l'utilizzo o la divulgazione dei Dati Personali.

8. Il soggetto accreditato manleverà e terrà indenne l'Amministrazione da ogni perdita, contestazione, responsabilità, spese sostenute nonché dei costi subiti (anche in termini di danno reputazionale) in relazione anche ad una sola violazione delle Norme in materia di Trattamento Personali e/o del Contratto (inclusi gli Allegati) comunque derivata dalla condotta (attiva e/o omissiva) sua e/o dei suoi agenti e/o Terzi autorizzati (sub-fornitori).

VI. TRASFERIMENTI DEI DATI PERSONALI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI.

La presente raccolta di dati non prevede il trasferimento di questi all'estero.

VII. OBBLIGHI DEL SOGGETTO ACCREDITATO DEL TRATTAMENTO AL TERMINE DEL CONTRATTO.

1. Il soggetto accreditato si impegna a non conservare - nonché a garantire che i Terzi autorizzati non conservino - i Dati Personali per un periodo di tempo ulteriore al limite di durata strettamente necessario per l'esecuzione dei servizi e/o l'adempimento degli obblighi, o così come richiesto o permesso dalla legge applicabile.

2. Alla scadenza del programma o al termine della fornitura dei servizi relativi al Trattamento dei Dati il soggetto accreditato dovrà cancellare o restituire in modo sicuro all'Amministrazione tutti i Dati Personali nonché cancellare tutte le relative copie esistenti, fatto salvo quanto diversamente disposto dalle Norme in materia di Trattamento dei Dati Personali.

3. Il soggetto accreditato deve documentare per iscritto all'Amministrazione tale cancellazione.

VIII. MODIFICHE DELLE LEGGI IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI

Nell'eventualità di qualsivoglia modifica delle Norme in materia di Trattamento dei Dati Personali applicabili al trattamento dei Dati Personali, che generi nuovi requisiti (ivi incluse nuove misure di natura fisica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), il soggetto accreditato collaborerà con l'Amministrazione, nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse, affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti durante l'esecuzione del Contratto.