ALLEGATO C

Allegato Privacy

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

Il *Fornitore* si impegna a mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato; inoltre il fornitore dichiara di possedere adeguate garanzie in termini di conoscenza specialistica, affidabilità e risorse per mettere in atto le misure tecniche e organizzative di cui sopra.

Pertanto, ai sensi dell'articolo 28 Regolamento Europeo e con la sottoscrizione del C*ontratto* dichiara di essere consapevole, in ragione delle prestazioni da eseguire con lo specifico affidamento, di essere nominato in sede di stipula contrattuale, con documentazione tecnica avente rilevanza contrattuale, Responsabile del trattamento di dati:

- in qualità di Responsabile primario o di Sub – Responsabile - in funzione della designazione fatta da SOGEI in qualità di Titolare ovvero di Responsabile primario dell'Amministrazione Titolare, così come indicato e descritto nel presente Allegato e nei documenti tecnico – funzionali che saranno rilasciati dalla Sogei come ad es. i verbali di affidamento con ulteriore documentazione tecnica avente rilevanza contrattuale;
- in qualità di Responsabile primario in forza della eventuale designazione diretta da parte delle Amministrazioni Titolari del trattamento dei dati e Clienti della SOGEI.

Il mancato rispetto da parte del Responsabile primario o del sub-Responsabile del trattamento delle disposizioni di cui al presente Allegato comporterà l'applicazione delle specifiche previsioni contrattuali in materia.

PREMESSA:

OGGETTO

Il presente Allegato disciplina le istruzioni che il Fornitore (ivi incluso il trattamento ad opera di eventuali sub-Responsabili) si impegna ad osservare nell'ambito dei trattamenti dei dati personali che realizzerà per conto della Sogei e/o delle Amministrazioni Clienti nello svolgimento delle attività oggetto del *Contratto* in essere con Sogei, garantendo il rispetto della normativa vigente in materia di tutela e sicurezza dei dati.

DEFINIZIONI

- "*Dati Personali* ": 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);
- "*Norme in materia di protezione 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.
- "*Contratto*": si intende il *Contratto* n…….stipulato tra la Sogei e il Fornitore, i relativi allegati ivi incluso il presente Allegato, nonché i documenti tecnico – funzionali aventi rilevanza contrattuale.
- "*Misure di Sicurezza*": le misure di sicurezza di natura tecnica e organizzativa adeguate a garantire un livello di sicurezza adeguato al rischio, ivi comprese quelle specificate nel *Contratto*.
- "*Dati Personali*": qualsiasi informazione relativa a una persona fisica identificata o identificabile (interessato) come definita nelle *Norme in materia di Protezione 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; ovverosia Sogei e/o le Amministrazioni Clienti.
- "*Amministrazioni Clienti*": le Amministrazioni e/o altri enti o persone giuridiche destinatarie dei servizi erogati dalla Sogei, anche attraverso il *Contratto*, che rivestono la qualifica di Titolari del Trattamento;
- "*Responsabile primario 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; ovverosia la Sogei in funzione della designazione ricevuta dalle Amministrazioni Clienti o il Fornitore in funzione della designazione ricevuta direttamente dal Titolare SOGEI o dall'Amministrazione cliente;
- "*Sogei*": la SOGEI – Società Generale d'Informatica S.p.A. in qualità di *Titolare* ovvero di *Responsabile primario del trattamento*;
- "*Sub-Responsabile del trattamento*": la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che svolge un trattamento in forza di contratto scritto con altro Responsabile del trattamento; ovvero il Fornitore e il subappaltatore/subfornitore autorizzato da Sogei, in forza del *Contratto*;
- "*Fornitore*": l'Impresa designata quale Responsabile primario o Sub – Responsabile, in funzione della designazione fatta da SOGEI in qualità di Titolare ovvero di Responsabile primario del Titolare, ovvero direttamente dal Titolare Amministrazione cliente;
- "*Persone autorizzate al trattamento dei dati*": persone che in qualità di dipendenti, collaboratori, amministratori o consulenti siano state autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare e/o del Responsabile primario e/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.

SICUREZZA DEI DATI PERSONALI

Il *Fornitore* ottempererà a tutte le *Norme in materia di Protezione dei dati Personali* in relazione al Trattamento dei *Dati Personali* ivi comprese quelle che saranno emanate nel corso di durata del *Contratto* al fine di assicurare, ciascuno 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.

OBBLIGHI E ISTRUZIONI PER IL FORNITORE

I. OBBLIGHI GENERALI DEL FORNITORE

1. Il *Fornitore* è autorizzato a trattare i dati personali necessari per l'esecuzione delle attività di cui all'oggetto del *Contratto*.

2. A tal fine il *Fornitore* si impegna a:

- non determinare o favorire mediante azioni e/o omissioni, direttamente o indirettamente, la violazione da parte di Sogei e/o delle Amministrazioni Clienti delle *Norme in materia di Protezione dei dati Personali*;
- trattare i *Dati Personali* esclusivamente in conformità alle istruzioni documentate da Sogei e/o dalle *Amministrazioni Clienti*, nella misura ragionevolmente necessaria all'esecuzione del *Contratto*, e alle *Norme in materia di Protezione dei dati Personali*;
- mettere in atto e mantenere nell'esecuzione delle attività contrattuali *Misure di sicurezza* indicate nella documentazione tecnica, adeguate a garantire un livello di sicurezza adeguato al rischio per tutta la durata del trattamento 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 *Fornitore*, ricorrendo le condizioni di cui all'art. 37 GDPR, si impegna a designare la figura professionale del Responsabile della protezione dei dati e a comunicarne i dati e i contatti di riferimento tempestivamente a Sogei e/o alle *Amministrazioni Clienti* in ragione dell'attività svolta.

II. ISTRUZIONI PER IL FORNITORE

II.A) Elementi essenziali dei trattamenti che il Fornitore è stato autorizzato a svolgere da Sogei e/o dalle Amministrazioni clienti.

Gli elementi essenziali del trattamento sono contenuti nel presente Allegato, nel *Contratto* e nei suoi allegati, nonché nei documenti tecnico – funzionali che saranno rilasciati dalla Sogei in ragione delle prestazioni richieste in corso di esecuzione contrattuale o in documenti che verranno rilasciati allo scopo dalle *Amministrazioni Clienti*.

In particolare i citati documenti conterranno, per garantire un livello di sicurezza adeguato al rischio connesso alle attività contrattuali, la materia disciplinata, la natura e finalità del trattamento, il tipo di dati personali trattati, le categorie di Interessati. Il presente Allegato potrà avere altri allegati in cui sono riportate le modalità di trattamento dei dati personali secondo le policy di Oracle che troveranno applicazione ove non in contrasto con i documenti tecnico - funzionali forniti dalla Sogei nel corso di esecuzione del *Contratto* o con i documenti che verranno rilasciati allo scopo dalle *Amministrazioni Clienti.*

La durata del trattamento dei dati personali è limitata, dunque coincide, con la durata del *Contratto* e delle sue eventuali proroghe.

II.B) Obblighi del Fornitore del trattamento nei confronti di SOGEI e/o delle Amministrazioni clienti.

Il Fornitore del trattamento si impegna a:

1. Trattare i dati solo per l'esecuzione delle attività di cui all'oggetto del *Contratto*.

2. Trattare i dati conformemente alle istruzioni documentate impartite da SOGEI e/o dalle *Amministrazioni Clienti* con il presente Allegato e con eventuali istruzioni documentate aggiuntive. Qualora il *Fornitore*, reputi che un'istruzione sia, o possa essere, contraria alla *Normativa in materia di protezione dei dati*, ivi incluso il GDPR, deve informarne immediatamente SOGEI e/o le *Amministrazioni Clienti*.

3. Trattare i dati conformemente alle istruzioni documentate fornite dalla SOGEI e/o dalle *Amministrazioni Clienti* 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 *Fornitore*; in tale ultimo caso il Fornitore dovrà informare Sogei e/o le *Amministrazioni Clienti* 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. Il Fornitore non può trasferire i dati personali verso un paese terzo o un'organizzazione internazionale, salvo che non abbia preventivamente ottenuto autorizzazione scritta da parte di Sogei e/o dalle *Amministrazioni Clienti*.

5. 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 per quanto di propria competenza.

6. Garantire la riservatezza dei dati personali trattati per l'esecuzione delle attività del *Contratto*.

7. Garantire che le persone autorizzate a trattare i dati personali in virtù del presente *Contratto*: ***i)*** si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza; ***ii)*** abbiano ricevuto, e ricevano, da parte del *Fornitore* la formazione necessaria in materia di protezione dei dati personali; ***iii)*** accedano e trattino i *dati personali* osservando le istruzioni impartite da Sogei e/o dalle *Amministrazioni Clienti*.

8. Tenere conto nell'esecuzione delle attività contrattuali 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 da Sogei e/o dalle *Amministrazioni Clienti.*

9. Il *Fornitore* si impegna a conferire a SOGEI eventuale copia dei dati personali dei dipendenti, amministratori, consulenti, collaboratori o altro personale del *Fornitore* nel corso delle attività oggetto del *Contratto*[1] esclusivamente per finalità relative all'esecuzione delle attività contrattuali ed amministrativo contabili oltre che per la sicurezza delle sedi e dei sistemi. Il *Fornitore*, con la sottoscrizione del *Contratto* e dei suoi allegati, autorizza Sogei, esclusivamente per le suddette finalità, ad estrarre tali dati personali dai propri sistemi informativi.

II.C) Obblighi del Fornitore nell'ambito dei diritti esercitati dagli Interessati nei confronti di SOGEI e/o delle Amministrazioni clienti.

1. Il *Fornitore* 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 *Fornitore* deve dare supporto, in tale attività, affinché il riscontro alle richieste di esercizio dei diritti degli Interessati avvenga senza ingiustificato ritardo mettendo tempestivamente a disposizione di Sogei e/o delle *Amministrazioni Clienti* tutte le informazioni necessarie.

3. Qualora gli Interessati esercitino un diritto previsto dal GDPR trasmettendo la relativa richiesta al *Fornitore*, quest'ultimo deve inoltrarla tempestivamente, e comunque entro e non oltre 3 giorni dalla ricezione, per posta elettronica a SOGEI e/o alle *Amministrazioni Clienti*.

II.D) Obblighi del Fornitore che ricorre a ulteriori sub –Responsabili

1. Il *Fornitore*, in base alle previsioni del *Contratto*, può ricorrere a Sub-Responsabili per l'esecuzione di specifiche attività di trattamento per conto di Sogei e/o delle *Amministrazioni Clienti* ed esclusivamente nei casi in cui abbia ricevuto espressa autorizzazione scritta dagli stessi, che si intende concessa per i Sub-responsabili.

2. Nell'ipotesi in cui il Fornitore, previa autorizzazione scritta di Sogei e/o delle *Amministrazioni Clienti*, abbia designato un Sub-Responsabile, il Fornitore e il Sub - Responsabile dovranno, in adempimento di quanto previsto all'art. 28 comma 4 del GDPR, essere vincolati da un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri con la previsione degli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il *Titolare del trattamento* e il *Responsabile primario 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 di cui al presente Allegato,

[1] Il Fornitore dovrà a sua volta informare i propri dipendenti, collaboratori, amministratori che i loro dati personali, nel rispetto del principio di pertinenza, saranno comunicati a soggetti terzi, e nel caso che qui rileva a Sogei, per l'esercizio delle attività del Contratto o per il corretto esercizio delle proprie attività.

al *Contratto*, ai relativi Allegati, nonché alle *norme in materia di protezione dei dati personali* e di cui alle ulteriori eventuali istruzioni documentate aggiuntive impartite da Sogei e/o dalle *Amministrazioni Clienti*.

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

In particolare, il *Fornitore* deve garantire che il Sub-Responsabile assicuri l'adozione di misure, tecniche ed organizzative adeguate, nonché alle ulteriori eventuali misure richieste da *Sogei* e/o dalle *Amministrazioni Clienti* di cui al successivo paragrafo IV.A. Tali misure devono essere altresì conformi alle norme in materia di protezione dei dati personali, alla regolamentazione in materia e alle istruzioni impartite da Sogei e/o dalle *Amministrazioni Clienti* in materia di protezione dei dati personali.

4. Resta, in ogni caso, ferma la successiva facoltà di *Sogei* e/o dalle *Amministrazioni Clienti* di opporsi all'aggiunta o sostituzione del Sub-Responsabile con altri Sub-Responsabili.

5. Le istruzioni impartite dal *Fornitore* a qualsiasi Sub-Responsabile dovranno avere il medesimo contenuto e perseguire i medesimi obiettivi delle istruzioni date da Sogei e/o dalle *Amministrazioni Clienti* al Fornitore stesso.

6. Se il Sub - Responsabile del trattamento non adempie alle proprie obbligazioni in materia di protezione dei dati o alle istruzioni ricevute dal Fornitore, e/o realizzi, mediante azioni e/o omissioni, incidenti di sicurezza e/o violazioni delle *Norme in materia di dati personali*, il Fornitore ne risponde interamente nei confronti di Sogei e/o delle *Amministrazioni Clienti*.

A tal fine, Sogei e/o dalle *Amministrazioni Clienti* possono, in qualsiasi momento, verificare le garanzie e le misure tecniche ed organizzative del Sub-Responsabile, anche per mezzo di audit, assessment, sopralluoghi e ispezioni svolti mediante il proprio personale oppure tramite soggetti terzi incaricati, che non saranno concorrenti diretti del *Fornitore* per quanto riguarda i Servizi e si impegneranno a sottostare ad idoneo vincolo di riservatezza. Nel caso in cui tali garanzie risultassero insussistenti SOGEI, in conformità a quanto contrattualmente previsto, può risolvere il *Contratto* con il *Fornitore*. Nel caso in cui all'esito delle verifiche, ispezioni, audit e assessment risultasse che le attività di trattamento di dati personali da parte del *Fornitore* vengano svolte in modo non conforme alle *Norme in materia di Trattamento dei Dati* e si verificasse che le misure di sicurezza tecniche e organizzative non siano state messe in atto oppure messe in atto non completamente e/o non correttamente, Sogei applicherà al *Fornitore* una penale come contrattualmente previste e diffiderà lo stesso a far adottare al Sub-Responsabile gli interventi necessari a mettere in atto misure di sicurezza adeguate entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento da parte del Fornitore e del Sub-Responsabile a tale diffida la SOGEI potrà applicare le specifiche previsioni contrattuali in materia.

IL REGISTRO DEI TRATTAMENTI DEL FORNITORE

1. Il *Fornitore* è obbligato a predisporre, conservare, aggiornare un registro anche in formato elettronico di tutte le categorie di attività relative al trattamento (o ai trattamenti) svolti per conto dei/del *Titolare del Trattamento*, come prevede l'art. 30, comma 2, del GDPR.

2. Su richiesta il *Fornitore* mette tale registro, contenente le informazioni di cui all'art. 30, comma 2, del GDPR, a disposizione dell'Autorità di controllo dandone al contempo informazione a Sogei e/o alle *Amministrazioni Clienti*.

III. OBBLIGHI DI SUPPORTO, COLLABORAZIONE E COORDINAMENTO DEL FORNITORE DEL TRATTAMENTO

Il *Fornitore* del trattamento assiste e collabora pienamente con Sogei e/o con le *Amministrazioni Clienti* 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 *Fornitore* 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. Tali misure 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.

Il *Fornitore* si obbliga ad adottare le misure di sicurezza previste da codici di condotta di settore, ove esistenti, ai quali abbia aderito e dalle certificazioni ove acquisite (art. 40 - 43 GDPR).

Nel valutare l'adeguatezza del livello di sicurezza il Fornitore devono 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.

Le modalità di svolgimento delle attività di privacy by design e privacy impact assessment da parte del *Fornitore* per l'individuazione delle misure di sicurezza di cui all'art. 32 del Regolamento, dovranno essere conformi al:

- Regolamento UE n. 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla protezione dei dati);
- Documento WP 243 – Linee guida sui responsabili della protezione dei dati (RPD) del 13 dicembre 2016;
- Documento WP 248 rev. 0.1 – Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 del 4 ottobre 2017;

Nonché seguire i principi di cui ai seguenti Standard:

- Standard ISO/IEC 29134:2017 Information technology -- Security techniques -- Guidelines for privacy impact assessment;
- Standard ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems;
- Standard ISO/IEC 31000:2018 Risk management – Guidelines.

In particolare, le attività da svolgersi dovranno soddisfare i seguenti criteri comunque soggetti a possibili aggiornamenti e modifiche da parte della Sogei e/o delle *Amministrazioni Clienti*:

a) analisi preliminare delle informazioni del trattamento in oggetto presenti nel Registro del titolare;
b) individuazione dei dati che rientrano nel trattamento secondo il principio di privacy by default, definizione di un modello concettuale e classificazione delle entità, relativamente a riservatezza, integrità e categoria di dati personali
c) definizione delle funzionalità che compongono il servizio ICT;
d) classificazione del servizio ICT in termini di caratteristiche privacy (finalità, liceità, interessati, …), e valutazione del rischio per l'organizzazione (riservatezza, integrità e disponibilità);
e) valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
f) valutazione dei rischi per i diritti e le libertà dell'interessato relativi alla tipologia dei dati trattati;
g) valutazione dei rischi per i diritti e le libertà dell'interessato relativi alla tipologia di trattamento, come previsto dalle linee guida WP 248;
h) in caso di un'alta valutazione dei rischi per i diritti e le libertà dell'interessato, individuazione delle misure di sicurezza specifiche per PIA e relativa valutazione di adeguatezza;

i) valutazione del rischio intrinseco complessivo per il servizio ICT (per l'organizzazione e per l'interessato) e individuazione delle misure di sicurezza idonee secondo il principio di privacy by design e relativa valutazione di adeguatezza;

j) redazione del documento contenente l'analisi dei rischi, le relative misure di sicurezza e la relativa valutazione di adeguatezza da proporre al Titolare secondo lo standard Sogei; recepimento delle eventuali osservazioni del Titolare, DPO, Garante privacy e Autorità.

All'esito dell'analisi dei rischi, le misure di sicurezza adeguate ai sensi dell'art. 32 del GDPR devono essere condivise e approvate dal Titolare e/o dal Responsabile primario.

I risultati dell'analisi del rischi per l'individuazione delle misure di sicurezza adeguate andranno riportati dalle Parti 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.

In particolare, il Fornitore analizza il rischio per l'individuazione delle misure di sicurezza adeguate riportando le informazioni di cui sopra.

Il Titolare e/o il Responsabile primario si riservano di richiedere misure di sicurezza ulteriori rispetto a quelle ritenute adeguate dal Fornitore.

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, del GDPR il *Fornitore* 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 Fornitore nelle ipotesi di "data breach"

Il *Fornitore* deve assistere e collaborare pienamente con SOGEI e/o con le *Amministrazioni Clienti* 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 *Fornitore* deve:

- predisporre e aggiornare un registro contenente tutte le violazioni dei dati personali sia dai trattamenti eseguiti al fine di facilitare SOGEI e/o le *Amministrazioni Clienti* nelle attività di indagine a seguito di data breach;
- comunicare a SOGEI e/o alle *Amministrazioni Clienti*, tempestivamente e in ogni caso senza ingiustificato ritardo, che si è verificata una violazione dei dati personali da quando il Fornitore o il suo sub-Responsabile, 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 a SOGEI e/o alle Amministrazioni Clienti affinché il *Titolare* del trattamento, se necessario, possa 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 SOGEI /o le *Amministrazioni Clienti* nelle attività di indagine, mitigando per quanto possibile 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 di SOGEI e/o delle *Amministrazioni Clienti* per la riduzione tempestiva delle probabilità che una violazione simile di dati personali possa ripetersi.

IV.C) Obblighi del Fornitore nella valutazione d'impatto del rischio di violazioni dei Dati Personali.

1. Il *Fornitore* si impegna ad assistere SOGEI e/o le *Amministrazioni Clienti* per il tramite di SOGEI, 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.

2. I risultati della valutazione d'impatto ex art. 35 del GDPR per l'individuazione delle misure di sicurezza necessarie andranno riportati dal *Fornitore* nel documento di analisi del rischio di cui al precedente paragrafo IV.A). In particolare, il *Fornitore* terrà conto dei risultati della valutazione d'impatto ex art. 35 del GDPR per l'individuazione delle ulteriori misure di sicurezza ritenute da SOGEI e/o dalle *Amministrazioni Clienti* necessarie come precisato al precedente paragrafo IV.A).

3. Il Fornitore si impegna altresì ad assistere SOGEI e/o le *Amministrazioni Clienti* nell'attività di consultazione preventiva dell'Autorità di controllo ai sensi dell'articolo 36 del GDPR.

IV. ULTERIORI OBBLIGHI DI GARANZIA DEL FORNITORE DEL TRATTAMENTO.

1. Il *Fornitore* si impegna ad operare adottando tutte le misure tecniche e organizzative, di cui al precedente art. IV A, 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 *Fornitore*, o da un suo sub-Responsabile, nella misura in cui il Fornitore sia in grado di operare in tal senso.

2. Il *Fornitore* si impegna a trasmettere a SOGEI e/o alle *Amministrazioni Clienti*, per il tramite di Sogei, tutte le informazioni e la documentazione che potranno ragionevolmente essere richieste durante il *Contratto* al fine di verificare la conformità dell'operato del Fornitore e dei sub-Responsabili con il presente Allegato, le *Norme in materia di Protezione dei dati Personali* e le *Misure di sicurezza*.

3. Il *Fornitore* acconsente e collabora con SOGEI e/o le *Amministrazioni Clienti* al regolare svolgimento delle attività di audit, incluse le ispezioni, effettuate da queste ovvero da propri rappresentanti debitamente autorizzati sulle attività di trattamento di dati personali nei confronti del *Fornitore* e/o di suoi *Sub-Responsabili*, ivi incluso l'operato degli eventuali amministratori di sistema, allo scopo di verificarne la conformità con il *Contratto,* nelle parti che riguardano il Trattamento di dati personali, (ivi inclusi i rispettivi Allegati), con le Istruzioni di *SOGEI* e/o delle *Amministrazioni Clienti*, e le *Norme in materia di protezione dei Dati* secondo quanto di seguito definito:

(i) il *Fornitore*, su richiesta scritta di *SOGEI* e/o delle *Amministrazioni Clienti*, fornirà a queste ultime o al rispettivo rappresentante autorizzato, tutte le informazioni necessarie per adempiere ad obblighi di audit o contrattuali o organizzativi o normativi o ad una richiesta dell'Autorità di Controllo o Vigilanza, dando, tra l'altro, evidenza delle certificazioni più recenti e/o di eventuali rapporti inerenti ad attività di audit riguardanti il Fornitore stesso o richieste dal quest'ultimo ai propri *Sub-Responsabili,* anche al fine di testare e verificare periodicamente l'efficacia delle misure di sicurezza.

(ii) resta ferma la facoltà per la *SOGEI* e/o per le *Amministrazioni Clienti,* o i rispettivi rappresentanti autorizzati, di effettuare una visita onsite presso le strutture deputate a fornire il servizio oggetto del *Contratto*. Le parti concorderanno le tempistiche e le modalità di tale visita.

Nel caso in cui all'esito delle verifiche, ispezioni, audit e assessment risultasse che le attività di trattamento di dati personali da parte del *Fornitore* e/o dei suoi *Sub-Responsabili* vengano svolte in modo non conforme al *Contratto* (ivi inclusi i rispettivi Allegati), alle Istruzioni di SOGEI e/o delle *Amministrazioni Clienti*, ed alle *Norme in materia di Protezione dei dati Personali* e si verificasse che le misure di sicurezza tecniche e organizzative non siano state messe in atto oppure messe in atto non completamente e/o non correttamente, Sogei applicherà al *Fornitore* una penale come contrattualmente previste e diffiderà lo stesso a far adottare al Sub- Responsabile gli interventi necessari a mettere in atto misure di sicurezza adeguate entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento da parte del Sub- Responsabile e/o del

Fornitore a tale diffida la Sogei potrà risolvere il *Contratto* ed escutere la garanzia definitiva, fatto salvo il risarcimento del maggior danno.

4. Fatto salvo quanto previsto al successivo paragrafo V il Fornitore non può trasferire i *Dati Personali* verso un paese terzo o un'organizzazione internazionale, salvo che non abbia preventivamente ottenuto autorizzazione scritta da parte di SOGEI e/o delle *Amministrazioni Clienti*.

5. Il Fornitore si impegna a notificare tempestivamente a SOGEI e/o alle *Amministrazioni Clienti*, ogni provvedimento di un'Autorità di controllo, o dell'Autorità giudiziaria relativo ai *Dati Personali* trattati a meno che tale comunicazione non sia vietata dal provvedimento o dalla legge.

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

7. Il *Fornitore* prende atto e riconosce che, nell'eventualità di una violazione delle Norme in materia di Protezione dei dati Personali nonché delle disposizioni di cui al presente documento e ai suoi allegati, oltre all'applicazione delle clausole di risoluzione del *Contratto* e delle penali oltre all'eventuale risarcimento del maggior danno, SOGEI 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 *Fornitore* manleverà e terrà indenne SOGEI e/o le *Amministrazioni Clienti* da ogni perdita, contestazione, responsabilità, spese sostenute nonché dei costi subiti in relazione anche ad una sola violazione delle *Norme in materia di protezione di dati Personali* o del presente Allegato C (inclusi gli Allegati) e/o del *Contratto* nelle parti che riguardano il Trattamento di dati personali (inclusi gli Allegati) comunque derivata dalla condotta (attiva e/o omissiva) sua e/o dei sub-Responsabili. Ai sensi dell'art.28 comma 4 del GDPR, il *Fornitore* rimarrà responsabile nei confronti di Sogei e/o delle Amministrazioni Clienti anche per l'eventuale inadempimento da parte dei suoi sub-Responsabili agli obblighi in materia di protezione dei dati.

V. **TRASFERIMENTI DEI DATI PERSONALI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI**

1. SOGEI e/o le *Amministrazioni Clienti* possono autorizzare per iscritto il Fornitore o un suo sub- Responsabile al trasferimento dei *Dati personali* (o parte di tali dati), ove necessario per l'esecuzione del *Contratto*, verso paesi terzi o organizzazioni internazionali nelle sole ipotesi in cui il paese terzo o l'organizzazione internazionale sia stata oggetto di una valutazione di adeguatezza da parte della Commissione Europea ai sensi dell'art. 45 del GDPR, oppure, in alternativa, previo rilascio della valutazione di adeguatezza svolta dal *Titolare* ai sensi dell'art. 46 del GDPR.

2. Nel caso in cui SOGEI e/o le Amministrazioni Clienti in relazione all'esecuzione da parte del Fornitore del trattamento dei suoi servizi e/o all'adempimento degli obblighi assunti con il *Contratto*, consenta al Fornitore o un suo sub- Responsabile, il trasferimento dei *dati Personali verso paesi terzi o organizzazioni internazionali,* il Fornitore deve:

- convenire (e impegnarsi affinché i suoi sub- Responsabili convengano) di ottemperare agli obblighi in materia di Trattamento di Dati Personali previsti nel presente Allegato e nelle clausole del *Contratto*;
- inserire nell'accordo di trasferimento dei *Dati personali* le disposizioni delle clausole contrattuali e delle *Norme applicabili in materia di Trattamento dei Dati Personali*.

3. Con la sottoscrizione del presente Allegato C le Parti concordano che ai sensi dell'art. 46 del GDPR costituiscono garanzia adeguata per il trasferimento dei dati personali le clausole tipo di protezione dei dati adottate dalla Commissione Europea, alle quali sarà data applicazione in caso di trattamento di dati da parte dei Sub- Responsabili del F*ornitore* che le ha sottoscritte con tutti i suoi Sub- Responsabili al presente documento.

VI. OBBLIGHI DEL FORNITORE DEL TRATTAMENTO AL TERMINE DEL CONTRATTO.

1. Il Fornitore si impegna a non conservare - nonché a garantire che i sub-Responsabili 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 di cui al *Contratto*, o così come richiesto o permesso dalla legge applicabile.

2. Alla scadenza del *Contratto* o al termine della fornitura dei servizi relativi al *Trattamento dei Dati* il Fornitore dovrà cancellare o restituire in modo sicuro a SOGEI e/o alle Amministrazioni Clienti tutti i *Dati Personali* nonché cancellare tutte le relative copie esistenti, fatto salvo quanto diversamente disposto dalle *Norme in materia di Protezione dei dati Personali.*

3. Il Fornitore deve documentare per iscritto a SOGEI e/o alle Amministrazioni Clienti tale cancellazione.

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

Nell'eventualità di qualsivoglia modifica delle *Norme in materia di Protezione 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 *Fornitore* collaborerà con SOGEI e/o le *Amministrazioni Clienti* 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*.