Allegato 13 – 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.
Il Fornitore ha dichiarato, nell'ambito della procedura ad evidenza pubblica, di essere in grado di assicurare idonee ed adeguate garanzie in termini di conoscenza specialistica, affidabilità, risorse, nonché in ordine all'adozione di misure tecniche, logiche ed organizzative per assicurare che i trattamenti dei dati personali siano conformi alle esigenze del Regolamento Europeo e, dunque, ai sensi dell'articolo 28 Regolamento Europeo e con la sottoscrizione del contratto dichiara altresì di essere consapevole, in ragione delle prestazioni da eseguire con lo specifico affidamento, di poter essere nominato in corso di esecuzione contrattuale, con documentazione tecnica avente rilevanza contrattuale, come Responsabile esterno dei trattamenti 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 del Titolare, così come indicati e descritti nel presente Allegato e nei documenti tecnico – funzionali che saranno rilasciati dalla Sogei con ulteriore documentazione tecnica avente rilevanza contrattuale.

Il mancato rispetto da parte del Responsabile primario o del sub-Responsabile del trattamento delle disposizioni di cui al presente Allegato sarà considerato un grave inadempimento del Contratto

Ai fini del presente Atto con il termine "Fornitore" si individua l'Impresa appaltatrice designata quale Responsabile primario o Sub – Responsabile, in funzione della designazione fatta da SOGEI in qualità di Titolare ovvero di Responsabile primario del Titolare (le Amministrazioni pubbliche che si avvalgono di Sogei per la realizzazione e l'erogazione dei servizi informatici) in ragione delle prestazioni richieste in corso di esecuzione contrattuale.

PREMESSA:

OGGETTO

1. Il presente Allegato disciplina le istruzioni che il Fornitore (ivi incluso il trattamento ad opera di eventuale sub-appaltatore o sub-fornitore) si impegna ad osservare nell'ambito dei trattamenti dei dati personali che realizzerà per conto della SOGEI quale Titolare/Responsabile primario (di seguito "Sogei") 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), concessi in licenza o diversamente messi a disposizione, trasmessi, gestiti, controllati o comunque trattati da Sogei (anche per conto delle Amministrazioni pubbliche Clienti di Sogei);
- "*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.
- "Contratto": si intende il contratto n. _____ stipulato tra la Sogei e _____ avente ad oggetto _____ - id 2169.

- "*Misure di Sicurezza*": le misure di sicurezza di natura fisica, logica, tecnica e organizzativa adeguate a garantire un livello di sicurezza adeguato al rischio, ivi comprese quelle specificate nel *Contratto*, unitamente ai suoi Allegati.
- "*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 Sogei o l'Amministrazione Cliente _____ .
- "*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; ovvero la Sogei o il Fornitore nel caso di Sogei *Titolare del trattamento*;
- "*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 anche denominato il Fornitore ovvero il subappaltatore o subfornitore autorizzato da SOGEI;
- "*Fornitore*": l'Impresa appaltatrice designata quale Responsabile primario o Sub – Responsabile, in funzione della designazione fatta da SOGEI in qualità di Titolare ovvero di Responsabile primario del Titolare (ovverosia le Amministrazioni pubbliche che si avvalgono di Sogei per la realizzazione e l'erogazione dei servizi informatici);
- "*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 Fornitore 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.

SICUREZZA DEI DATI PERSONALI

1. Il Fornitore 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 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 per conto di SOGEI (Titolare/Responsabile primario) 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 o del *Titolare del trattamento* delle *Norme in materia di Trattamento dei Dati Personali*;
- trattare i *Dati Personali* esclusivamente in conformità alle istruzioni documentate di Sogei, 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 Fornitore 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 a Sogei, 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

1. Gli elementi essenziali deltrattamento sono contenuti nel presente documento, 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.
2. 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.
3. 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

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 - che, a loro volta, saranno istruzioni conformi e adeguate, nel corso del Contratto, alle istruzioni impartite dal Titolare del trattamento (nel caso in cui il Titolare sia una Amministrazione pubblica o un cliente di Sogei) - 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.

3. Trattare i dati conformemente alle istruzioni documentate della SOGEI 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 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 del *Contratto*.

6. 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.

7. 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 dal *Titolare del trattamento.*

8. 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 presente contratto, autorizza Sogei, esclusivamente per le suddette finalità, ad estrarre tali dati personali dai propri sistemi informativi.

9. Qualora richiesto dalle *Norme in materia di Trattamento dei Dati Personali*, la SOGEI e il Fornitore 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 Fornitore nell'ambito dei diritti esercitati dagli Interessati nei confronti di SOGEI.

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 giustificato ritardo.
3. A tal fine il Fornitore deve adottare e aggiornare un registro di tutte le attività di trattamento eseguite per conto di Sogei completo di tutte le informazioni previste all'art. 30 del GDPR (cfr. successivo paragrafo III del presente Allegato) e mettere tale registro a disposizione di Sogei 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 Fornitore, quest'ultimo deve inoltrarla tempestivamente, e comunque entro e non oltre 3 giorni dalla ricezione, per posta elettronica a SOGEI.

II.D) Obblighi del Fornitore che ricorre a *Terzi Autorizzati*

1. Il Fornitore può ricorrere a Terzi Autorizzati per l'esecuzione di specifiche attività di trattamento esclusivamente nei casi in cui abbia ricevuto espressa autorizzazione scritta da Sogei

[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.

2. Nell'ipotesi in cui il Fornitore, previa autorizzazione scritta di Sogei, abbia designato un Terzo Autorizzato, il Fornitore e il Terzo autorizzato dovranno essere vincolati da un accordo scritto recante tutti gli obblighi in materia di protezione dei dati di cui al presente Contratto e relativi Allegati e di cui alle ulteriori eventuali istruzioni documentate aggiuntive impartite dalla SOGEI.
3. Il Fornitore deve formulare per iscritto a Sogei 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 Fornitore deve garantire che il Terzo Autorizzato assicuri l'adozione di misure, logiche, tecniche ed organizzative adeguate di cui al presente contratto ed alla normativa e regolamentazione in materia ed alle istruzioni impartite dalla SOGEI in materia di protezione dei dati personali.
5. Resta, in ogni caso, ferma la successiva facoltà di Sogei di opporsi all'aggiunta o sostituzione del Terzo Autorizzato con altri soggetti Terzi.
6. Le istruzioni impartite dal Fornitore a qualsiasi Terzo dovranno avere il medesimo contenuto e perseguire i medesimi obiettivi delle istruzioni fornite al Fornitore da Sogei nei limiti dei trattamenti autorizzati in capo al Terzo.
7. A tal fine, Sogei 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 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 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*, Sogei applicherà al Fornitore una penale come contrattualmente previste 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 Fornitore a tale diffida la SOGEI potrà risolvere il Contratto ed escutere la garanzia definitiva, fatto salvo il risarcimento del maggior danno.

III. IL REGISTRO DEI TRATTAMENTI DEL FORNITORE

1. Il Fornitore 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 Fornitore dei trattamenti svolti per conto di SOGEI deve contenere:
   - ***i)*** il nome e i dati di contatto del Fornitore (e, se del caso, di Terzi Autorizzati) del trattamento, di ogni *Titolare del trattamento* per conto del quale il Fornitore agisce, del rappresentante (eventuale) del Fornitore 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 FORNITORE DEL TRATTAMENTO NELL'ATTUAZIONE DEGLI OBBLIGHI DI SOGEI

1. Il Fornitore del trattamento assiste e collabora pienamente con SOGEI 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.

1. 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. I criteri per la valutazione del rischio devono essere previamente condivisi e approvati da Sogei. 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.

2. Il Fornitore 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)].*

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

4. 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 a:

- 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;
- 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;

5. In particolare le attività da svolgersi dovranno soddisfare i seguenti criteri comunque soggetti a possibili aggiornamenti e modifiche da parte della Sogei:

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.

6. All'esito dell'analisi dei rischi, le misure di sicurezza adeguate ai sensi dell'art. 32 del GDPR devono essere condivise ed approvate da Sogei e dal Titolare (nel caso in cui il Titolare sia una Amministrazione pubblica cliente di Sogei).

7. I risultati dell'analisi del rischi per l'individuazione delle misure di sicurezza adeguate andranno riportati dal Fornitore 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.

8. 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.

9. Ai sensi dell'art. 32, comma 4, 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"

1. Il Fornitore deve assistere e collaborare pienamente con SOGEI ed i suoi Titolari del trattamento, nelle attività di adempimento di cui agli articoli 33 e 34 del GDPR in materia di violazioni di dati personali, ovvero di data breach.

2. In particolare, il Fornitore deve:

- predisporre e aggiornare un registro contenente tutte le violazioni dei dati personali sia dai trattamenti eseguiti per conto di SOGEI, al fine di facilitare quest'ultima nelle attività di indagine a seguito di data breach;
- comunicare a SOGEI, tempestivamente e in ogni caso senza ingiustificato ritardo, che si è verificata una violazione dei dati personali da quando il Fornitore, 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 a SOGEI per consentirle di notificare, senza ingiustificato ritardo al Titolare, (nel caso in cui il Titolare sia una Amministrazione pubblica cliente di

Sogei), la violazione dei dati affinchè 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 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 di SOGEI e/o del Titolare, nel caso in cui il Titolare sia una Amministrazione pubblica cliente di Sogei, per la riduzione tempestiva delle probabilità che una violazione simile di dati personali possa ripetersi;
- nel caso in cui SOGEI debba fornire informazioni (inclusi i dettagli relativi ai servizi prestati dal Fornitore) al Titolare e/o all'Autorità di controllo il Fornitore supporterà SOGEI 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 Fornitore 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 SOGEI può consultarsi con il proprio Responsabile della protezione dei dati (art. 35, comma 2, del GDPR).

2. Il Fornitore del trattamento si impegna ad assistere SOGEI e il Titolare (nel caso in cui il Titolare sia una Amministrazione pubblica cliente di Sogei) 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.

3. 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 art. IV.A).

4. Il Fornitore si impegna altresì ad assistere SOGEI nell'attività di consultazione preventiva dell'Autorità di controllo ai sensi dell'articolo 36 del GDPR.

V. ULTERIORI OBBLIGHI DI GARANZIA DEL FORNITORE DEL TRATTAMENTO.

1. Il Fornitore 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 Fornitore, o da un Terzo da lui autorizzato, nella misura in cui il Fornitore sia in grado di operare in tal senso.

2. Il Fornitore si impegna a trasmettere a SOGEI tutte le informazioni e la documentazione che quest'ultima potrà ragionevolmente richiedere durante il *Contratto* al fine di verificare la conformità del Fornitore (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 Fornitore garantisce a SOGEI, 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 da SOGEI, delle attività di trattamento dei *Dati Personali* eseguite dal medesimo Fornitore, 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 di SOGEI e le *Norme in materia di Trattamento dei Dati*. Il Fornitore deve mettere a disposizione di SOGEI, senza alcun ritardo e/o omissione, tutte le informazioni necessarie per dimostrare la sua conformità con gli obblighi previsti nel *Contratto*. 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, SOGEI applicherà al Fornitore le penali previste dal Contratto 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 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 VI 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 del Titolare.

5. Il Fornitore si impegna a notificare tempestivamente a SOGEI e al Titolare nel caso in cui il Titolare sia una Amministrazione pubblica cliente di Sogei, ogni provvedimento di un'Autorità di controllo, o dell'Autorità giudiziaria relativo ai *Dati Personali di Sogei* 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 Fornitore deve: *i)* informare Sogei e/o il Titolare tempestivamente, e comunque entro 24 ore dal ricevimento della richiesta di ostensione; *ii)* collaborare con Sogei e/o il Titolare, 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 Trattamento dei Dati Personali nonché delle disposizioni di cui al presente Allegato, 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 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

1. SOGEI o un Titolare del Trattamento (Cliente Sogei) possono autorizzare per iscritto il Fornitore, o un suo Terzo Autorizzato, al trasferimento dei *Dati personali* (o parte di tali dati) 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 o un Titolare del trattamento (Cliente di Sogei), 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 a un sub-fornitore) il trasferimento dei *dati Personali verso paesi terzi o organizzazioni internazionali,* il Fornitore deve:

- convenire (e impegnarsi affinché i suoi sub-fornitori convengano) di ottemperare agli obblighi previsti nelle clausole del *Contratto*;
- garantire che, prima di tale trasferimento, Sogei o il titolare e/o il Fornitore stipulino un accordo per l'accesso ai dati come indicato dalla Commissione Europea;

- inserire nell'accordo di trasferimento dei *Dati personali* le disposizioni delle clausole contrattuali e delle *Norme applicabili in materia di Trattamento dei Dati Personali*.

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

1. Il Fornitore 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 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 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 Fornitore deve documentare per iscritto a SOGEI tale cancellazione.

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

1. 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 Fornitore collaborerà con SOGEI, 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*.