ALLEGATO PRIVACY

CONTRATTO N. REP. _____

1. SCOPO E OGGETTO DEL DOCUMENTO 2
2. DEFINIZIONI 2
3. OBBLIGHI E ISTRUZIONI PER IL FORNITORE 4
I. OBBLIGHI GENERALI 4
I.A) Elementi essenziali del trattamento 6
I.B) Richieste e Diritti degli Interessati 6
I.C) Sub-Responsabili del trattamento 6
II. REGISTRO DEI TRATTAMENTI 7
III. OBBLIGHI DI SUPPORTO, COLLABORAZIONE E COORDINAMENTO 7
III.A) Analisi dei rischi e Valutazione di impatto 7
III.B) Obblighi in caso di "data breach" 8
IV. ULTERIORI OBBLIGHI DEL FORNITORE 9
V. TRASFERIMENTI DEI DATI PERSONALI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI 10
VI. OBBLIGHI DEL FORNITORE AL TERMINE DEL CONTRATTO 10
VII. MODIFICHE DELLE NORME IN MATERIA DI PROTEZIONE DEI DATI PERSONALI 11

1. SCOPO E OGGETTO DEL DOCUMENTO

Il presente documento ("*Allegato Privacy*"), ai sensi dell'art. 28 del Regolamento, intende disciplinare gli obblighi e le istruzioni che il *Fornitore* è tenuto ad osservare qualora l'esecuzione del *Contratto*, ivi incluse eventuali modifiche e/o integrazioni, comporti il *Trattamento di Dati Personali* per conto di *Sogei*.

In tal caso, *Sogei* potrebbe rivestire il ruolo di autonomo *Titolare* ovvero di *Responsabile del trattamento* per conto dell'*Amministrazione Cliente*. Di conseguenza, il *Fornitore* viene designato (i) *Responsabile del trattamento*, qualora *Sogei* rivesta il ruolo di *Titolare del trattamento*, ovvero (ii) *Sub-Responsabile del trattamento,* qualora *Sogei* rivesta il ruolo di *Responsabile del trattamento* per conto dell'*Amministrazione Cliente*.

La presente nomina si intende accettata dal *Fornitore* (i) vuoi nel momento in cui il presente *Allegato Privacy* verrà fatto pervenire a *Sogei* debitamente sottoscritto, (ii) vuoi, ai sensi e per gli effetti dell'art. 1327 c.c., con l'adempimento delle prestazioni inerenti al *Contratto* e comunque con l'avvio delle attività di *Trattamento*, indifferentemente da quale dei due eventi si realizzi per primo.

Il presente *Allegato Privacy*, ivi inclusi gli eventuali allegati, costituisce parte integrante e sostanziale del *Contratto* tra *Sogei* e il *Fornitore*.

Nel caso di Raggruppamento temporaneo di imprese (RTI), il *Fornitore*, nominato Responsabile o Sub-Responsabile del trattamento, in qualità di mandatario del RTI, deve provvedere alla designazione delle società mandanti che effettuano operazioni di trattamento sui dati personali quali proprie Sub-Responsabili del trattamento.

Rimane inteso che il presente *Allegato Privacy* non trova applicazione nei casi in cui l'esecuzione del *Contratto* non comporti, da parte del *Fornitore*, il *Trattamento di Dati Personali* ovvero nel caso in cui tale *Trattamento* sarà effettuato dal *Fornitore* in qualità di autonomo *Titolare del trattamento* o in regime di contitolarità con *Sogei* ai sensi dell'art. 26 del Regolamento, caso quest'ultimo in cui verrà stipulato tra le parti un idoneo accordo di contitolarità.

2. DEFINIZIONI

I termini utilizzati nel presente *Allegato Privacy* devono essere intesi esclusivamente secondo il significato risultante dalle definizioni di seguito precisate e/o secondo le ulteriori definizioni di volta in volta rinvenibili nello stesso:

- "*Amministrazione Cliente*": le Amministrazioni e/o altri enti o persone giuridiche destinatarie dei servizi erogati da *Sogei*, anche attraverso il *Contratto*, e che potrebbero rivestire la qualifica di *Titolari del Trattamento*.
- "*Contratto*": si intende il contratto, comprensivo dei suoi allegati, stipulato tra la *Sogei* e il *Fornitore*.
- *"Dati Personali*": qualsiasi informazione relativa a una persona fisica identificata o identificabile (interessato) come definita nelle *Norme in materia di Protezione dei Dati Personali* (inclusi i dati appartenenti alle categorie particolari di dati personali di cui all'art. 9 e relativi a condanne penali e a reati di cui all'art. 10 del Regolamento), messi a disposizione, trasmessi, gestiti, controllati o comunque trattati da *Sogei* in qualità di *Titolare* o di *Responsabile del trattamento* per conto delle *Amministrazioni Clienti*.
- *"Direttore dell'Esecuzione (DDE)":* soggetto a cui è attribuita con nomina la responsabilità della fase di esecuzione e dell'intero iter tecnico-amministrativo della gestione del contratto stesso;

- *"Elementi essenziali del trattamento"*: gli elementi di cui all'art. 28, paragrafo 3, primo capoverso del Regolamento.
- "*Fornitore*": l'Impresa appaltatrice che, in forza del presente *Allegato Privacy*, viene designata da *Sogei* quale *Responsabile* o *Sub-Responsabile del trattamento.*
- "*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, la violazione e/o il malfunzionamento di *Misure di Sicurezza*, di strumenti elettronici, hardware o software a protezione dei dati e delle informazioni.
- "*Misure di Sicurezza*": le misure di sicurezza di natura fisica, logica, tecnica e organizzativa atte a garantire un livello di sicurezza adeguato al rischio, ivi comprese quelle eventualmente specificate nel *Contratto* e/o nella ulteriore documentazione di rilevanza contrattuale.
- "*Norme in materia di Protezione dei Dati Personali*": le leggi, regolamenti, e, in generale, le norme nazionali ed europee, anche di soft law, applicabili in relazione al trattamento e/o alla protezione e alla sicurezza dei Dati Personali, così come modificate di volta in volta, ivi incluso, a titolo esemplificativo e non esaustivo, il Regolamento (UE) 2016/679 ("Regolamento" o "GDPR"), il D.Lgs. 196/2003 come novellato dalla normativa di adeguamento italiana di cui al D.Lgs. 101/2018, circolari, pareri e direttive dell'Autorità di Controllo nazionali e comunitarie.
- "*Persone autorizzate al trattamento dei dati*": persone che in qualità di dipendenti, collaboratori, amministratori o consulenti del *Fornitore* siano state autorizzate al *Trattamento dei Dati Personali* e operano sotto l'autorità diretta del *Responsabile* o del *Sub-Responsabile* o del *Titolare autonomo*.
- "*Responsabile del trattamento*" o "*Responsabile*": la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del *Titolare del trattamento*.
- "*Responsabile della protezione dei dati (RPD)*": il soggetto designato dal Titolare ai sensi degli art. 37 e ss. del Regolamento anche denominato Data Protection Officer (DPO).
- "*Responsabile unico del procedimento (RUP*)": il RUP dell'esecuzione è il soggetto nominato con apposito atto che svolge, in coordinamento con il DDE, le attività di controllo e vigilanza sull'esecuzione del contratto in aderenza alle Direttive aziendali e secondo quanto previsto nel contratto stesso. Il RUP dell'esecuzione, in assenza della espressa nomina del DDE, svolge i compiti e le attività a quest'ultimo attribuiti.
- "*Sogei*": la SOGEI – Società Generale d'Informatica S.p.A. in qualità di *Titolare* ovvero di *Responsabile del trattamento*.
- "*Sub-Responsabile del trattamento*" o "*Sub-Responsabile*": la persona fisica o giuridica o altro organismo pubblico o privato che tratta dati personali in forza di un accordo scritto con altro *Responsabile del trattamento*. *Sub-Responsabile del trattamento* può indicare il *Fornitore* quando *Sogei* agisce in qualità di *Responsabile del trattamento* per conto dell'*Amministrazione Cliente*, ovvero il soggetto a cui il *Fornitore*, autorizzato da *Sogei*, abbia delegato l'esecuzione di specifiche attività di *Trattamento*.
- "*Titolare del trattamento*" o "*Titolare*": 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 ovverosia *Sogei* o l'*Amministrazione Cliente*; 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.

- "*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.
- "*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.

3. OBBLIGHI E ISTRUZIONI PER IL FORNITORE

Il *Fornitore*, nella sua qualità di *Responsabile del trattamento* o di *Sub-responsabile del trattamento*, si impegna a trattare i *Dati Personali* esclusivamente in conformità alle istruzioni previste nel *Contratto* e nel presente *Allegato Privacy* e alle ulteriori istruzioni che potranno essere eventualmente impartite da *Sogei*, nel rispetto degli obblighi ivi previsti e delle *Norme in materia di Protezione dei Dati Personali*.

Le disposizioni di seguito riportate si riferiscono agli obblighi assunti dal Fornitore e alle istruzioni che quest'ultimo si impegna a rispettare in relazione al *Trattamento dei Dati Personali* connesso all'esecuzione del *Contratto*. Le prescrizioni del presente *Allegato Privacy* possono essere integrate e derogate solo sulla base di ulteriori e specifici atti di istruzione e/o di nomina di *Sogei*.

Ove il Fornitore rilevi la sua impossibilità nel rispettare le condizioni e le istruzioni contenute nel presente *Allegato Privacy*, anche per caso fortuito o forza maggiore, dovrà attuare tutte le possibili e ragionevoli misure per garantire la sicurezza dei *Trattamenti* e avvertire immediatamente *Sogei*, concordando con quest'ultima eventuali azioni e/o l'adozione di ulteriori *Misure di Sicurezza*.

I. OBBLIGHI GENERALI

1. Il *Fornitore* è autorizzato a trattare esclusivamente i *Dati Personali* necessari per l'esecuzione delle attività oggetto del *Contratto* e nella misura necessaria a tal fine.

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 dell'*Amministrazione Cliente* (nel caso in cui quest'ultima sia il *Titolare*) delle *Norme in materia di Protezione dei Dati Personali*;
  – informare tempestivamente *Sogei* nel caso in cui venga a conoscenza che tali *Dati Personali* siano inesatti e obsoleti;
  – adottare, aggiornare e implementare *Misure di sicurezza* adeguate a garantire un adeguato livello di sicurezza, inclusa la riservatezza, in modo tale da ridurre al minimo il rischio di *Incidenti di sicurezza* e/o di *Violazione dei dati personali*.

3. Il *Fornitore* si impegna inoltre a:
  a) informare immediatamente *Sogei* nel caso in cui reputasse che le istruzioni impartitegli con il presente *Allegato Privacy* e/o attraverso ulteriori documenti siano, o possano essere, contrari alla *Norme in materia di Protezione dei Dati Personali*;
  b) garantire la riservatezza dei *Dati Personali* trattati per l'esecuzione delle attività del *Contratto*;
  c) non diffondere e non comunicare i *Dati Personali* oggetto di *Trattamento*, senza autorizzazione scritta di *Sogei* e/o dell'*Amministrazione Cliente* (ove quest'ultima sia il *Titolare del*

trattamento), fatte salve le particolari esigenze di riservatezza espressamente esplicitate dall'Autorità Giudiziaria;

d) prima dell'avvio delle operazioni di *Trattamento*, designare per iscritto e istruire adeguatamente le *Persone autorizzate al trattamento*, anche per settori o categorie omogenee, individuando gli ambiti di operatività consentiti e garantendo l'accesso ai soli *Dati Personali* strettamente necessari per l'esecuzione del *Contratto*. Il *Fornitore* garantisce che le *Persone autorizzate al trattamento* siano in possesso dei requisiti di esperienza, capacità e affidabilità sufficienti ad assicurare lo svolgimento del *Trattamento* in conformità alle *Norme in materia di Protezione dei Dati Personali*;

e) garantire che le *Persone autorizzate* a trattare i dati personali in virtù del *Contratto* e del presente *Allegato Privacy* ricevano adeguate istruzioni in merito alle modalità del trattamento, nel rispetto delle *Norme in materia di Protezione dei Dati*. Il *Fornitore* dovrà altresì garantire che tali soggetti: ***(i)*** abbiano esclusivamente accesso ai *Dati Personali* necessari allo svolgimento delle attività affidategli; ***(ii)*** si siano impegnati alla riservatezza o abbiano un adeguato obbligo legale di riservatezza, anche per il periodo successivo alla cessazione del *Trattamento*; ***(iii)*** abbiano ricevuto, e ricevano, da parte del *Fornitore* la formazione necessaria in materia di protezione dei *Dati Personali;*

f) adottare e/o utilizzare un idoneo sistema di identificazione, autenticazione e autorizzazione di accesso ai *Dati personali* per le *Persone autorizzate al Trattamento*;

g) individuare e nominare, qualora ne ricorrano i presupposti, quali "*Amministratori di Sistema*" ("*AdS*") le persone fisiche incaricate della gestione e manutenzione dei sistemi conformemente a quanto previsto nel Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 ("*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*") e successive modificazioni e integrazioni. In tal caso, il *Fornitore* dovrà predisporre e mantenere aggiornato un elenco di tali soggetti e, ove applicabile, in considerazione delle modalità di svolgimento delle prestazioni oggetto del *Contratto*, monitorarne le relative attività conformemente a quanto indicato nel provvedimento da ultimo richiamato;

h) ove richiesto da *Sogei*, eventualmente anche su istruzione dell'*Amministrazione Cliente* (ove quest'ultima sia il *Titolare del trattamento*), rendere l'informativa agli Interessati, sulla base di un modello concordato con *Sogei* o fornito direttamente da quest'ultima;

i) ove necessario e applicabile, supportare *Sogei* e/o l'*Amministrazione Cliente* (nel caso in cui quest'ultima sia il *Titolare del trattamento*) nella gestione dei meccanismi e/o sistemi per l'acquisizione e registrazione dei consensi degli Interessati;

j) fornire, su richiesta, eventuale copia dei *Dati Personali* dei dipendenti, amministratori, consulenti, collaboratori o altro personale del *Fornitore* autorizzato al trattamento, nel corso delle attività oggetto del *Contratto* esclusivamente per finalità relative all'esecuzione delle attività contrattuali ed amministrativo-contabili, oltre che per la sicurezza delle sedi e dei sistemi. Il *Fornitore*, pertanto, autorizza *Sogei* ad estrarre tali *Dati Personali* dai suoi sistemi informativi esclusivamente per le predette finalità e garantisce di aver correttamente adempiuto, ai sensi dell'art. 13 del Regolamento, all'obbligo di informare i propri dipendenti, collaboratori, amministratori o altro personale 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.

4. Il *Fornitore*, ricorrendo le condizioni di cui all'art. 37 del Regolamento, si impegna a designare la figura professionale del *Responsabile della protezione dei dati (RPD)* e a comunicarne tempestivamente i dati di contatto a *Sogei*.

I.A) *Elementi essenziali del trattamento*

1. Gli *Elementi essenziali del trattamento* di cui all'art. 28, paragrafo 3, primo capoverso, del Regolamento saranno condivisi con il *Fornitore*, per il tramite del *DDE*, nel corso dell'esecuzione del *Contratto* e, in ogni caso, prima dell'avvio delle attività di Trattamento.
2. Gli *Elementi essenziali del trattamento* inizialmente comunicati potranno essere oggetto di integrazione, variazione o modifica con idonea comunicazione da inviarsi da parte di *Sogei* con le medesime modalità sopra indicate.
3. Rimane comunque inteso che le istruzioni fornite con il presente *Allegato Privacy* sono valide per ogni *Trattamento* di ogni categoria di *Dati Personali* riferibili ad ogni categoria di Interessati e, pertanto, idonee a consentire al *Fornitore* lo svolgimento del *Trattamento* delegato in esecuzione del *Contratto*.

I.B) *Richieste e Diritti degli Interessati*

1. Qualora il *Fornitore* riceva reclami e/o gli *Interessati* esercitassero i propri diritti trasmettendo la relativa richiesta direttamente al *Fornitore*, quest'ultimo deve inoltrarla tempestivamente, e comunque entro e non oltre 3 giorni lavorativi dalla ricezione, a *Sogei* attraverso l'indirizzo di posta elettronica certificata dpo@pec.sogei.it.
2. Il *Fornitore* sarà tenuto a riscontrare le istanze degli Interessati solo qualora sia stato autorizzato da *Sogei* e/o dall'*Amministrazione Cliente* (nel caso in cui quest'ultima sia il *Titolare del trattamento*).
3. Ove richiesto, il *Fornitore* presta il proprio supporto e la propria collaborazione nel dare riscontro scritto, anche di mero diniego, alle richieste degli Interessati e alle istanze degli stessi per l'esercizio dei diritti previsti dagli artt. 15-22 del Regolamento, attenendosi alle istruzioni ricevute da *Sogei* e/o dall'*Amministrazione Cliente* (nel caso in cui quest'ultima sia il *Titolare del trattamento*).
4. In ogni caso, il *Fornitore* deve fornire tutto il supporto necessario affinché il riscontro agli Interessati avvenga senza ingiustificato ritardo e comunque entro e non oltre il termine utile e/o di legge previsto per dare riscontro alle richieste/istanze ricevute.

I.C) *Sub-Responsabili del trattamento*

1. Il *Fornitore* può ricorrere a *Sub-Responsabili* per l'esecuzione di specifici *Trattamenti*. Prima dell'inizio delle attività di *Trattamento*, il *Fornitore* comunica a *Sogei*, nella figura del *DDE*, i nominativi e la ragione sociale dei *Sub-Responsabili* di cui intende avvalersi, nonché le attività di *Trattamento* da delegare, dando così l'opportunità a *Sogei* di opporsi ai *Sub-Responsabili* individuati. Il *Fornitore* si impegna altresì a comunicare tempestivamente a *Sogei*, nella figura del *DDE*, eventuali aggiunte o sostituzioni dei *Sub-Responsabili,* al fine di consentire a *Sogei* di opporsi a tali aggiunte o sostituzioni.
2. Nell'ipotesi in cui il *Fornitore* abbia designato un *Sub-Responsabile del trattamento*, il *Fornitore* e il *Sub-Responsabile* dovranno, in adempimento a quanto previsto dall'art. 28, par. 4 del Regolamento, essere vincolati da un accordo scritto recante tutti gli obblighi e le istruzioni in materia di protezione dei dati previsti nel *Contratto* e nel presente *Allegato Privacy*, nonché tutte le ulteriori ed eventuali istruzioni documentate impartite da *Sogei*. Ove richiesto, il *Fornitore* si impegna a trasmettere l'atto di designazione dei *Sub-Responsabili* e ogni successiva modifica. Il *Fornitore*, nella misura necessaria

a proteggere segreti aziendali o altre informazioni riservate, compresi i *Dati Personali*, potrà espungere informazioni dal suddetto atto di designazione prima di trasmetterne copia.

3. Le istruzioni impartite dal *Fornitore* ai *Sub-Responsabili del trattamento* dovranno comunque avere il medesimo contenuto e perseguire i medesimi obiettivi delle istruzioni fornitegli da *Sogei*, con riferimento ai trattamenti effettuati dal *Sub-Responsabile*. In particolare, il *Fornitore* garantisce che il *Sub-Responsabile del trattamento* assicuri l'adozione di tutte le *Misure di Sicurezza* in conformità a quanto previsto nel *Contratto*, nel presente *Allegato Privacy* e nelle *Norme in materia di Protezione dei Dati Personali* e alle eventuali ulteriori istruzioni impartite da *Sogei*.

4. Il *Fornitore* si impegna a comunicare a *Sogei* se il *Sub-Responsabile del trattamento* non dovesse adempiere alle proprie obbligazioni o alle istruzioni ricevute e/o realizzi, mediante azioni e/o omissioni, *Incidenti di sicurezza* e/o violazioni delle *Norme in materia di Protezione dei Dati Personali*, fermo restando che il *Fornitore* ne risponderà interamente nei confronti di *Sogei*, non potendo in alcun modo opporre che detto inadempimento è dovuto, in tutto o in parte, al *Sub-Responsabile*.

Il *Fornitore* concorda con il *Sub-Responsabile del trattamento* una clausola del terzo beneficiario secondo la quale, qualora il *Fornitore* stesso sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, *Sogei* ha il diritto di sostituirsi nei rapporti verso il *Sub-Responsabile*, risolvendo il contratto e ordinando a quest'ultimo di procedere con la cancellazione e restituzione dei dati personali.

II. REGISTRO DEI TRATTAMENTI

1. Il *Fornitore* è obbligato a predisporre, conservare, anche in formato elettronico, e aggiornare - anche con l'ausilio del proprio *RPD* - un registro di tutte le attività di *Trattamento* svolte in qualità di *Responsabile* o di *Sub-Responsabile del trattamento* (di seguito "***Registro***"), conformemente a quanto previsto dall'art. 30, paragrafo 2, del Regolamento.

2. Su richiesta dell'Autorità di controllo, il *Fornitore* metterà a disposizione il *Registro* all'Autorità stessa dandone al contempo informazione a *Sogei*.

3. Il *Fornitore*, ove richiesto, si impegna a supportare *Sogei* nelle attività di censimento dei *Trattamenti* inerenti al *Contratto*.

III. OBBLIGHI DI SUPPORTO, COLLABORAZIONE E COORDINAMENTO

Il *Fornitore* presta la propria assistenza e collaborazione nel garantire il rispetto degli obblighi di cui agli articoli 31, 32, 33, 34, 35 e 36 del Regolamento, come di seguito descritto.

III.A) Analisi dei rischi e Valutazione di impatto

1. Il *Fornitore* deve mettere in atto *Misure di Sicurezza* per garantire un livello di sicurezza adeguato al rischio e nel rispetto degli obblighi di cui all'art. 32 del Regolamento, tenuto conto dello stato dell'arte, del progresso e dello sviluppo tecnico e tecnologico in materia. A tal fine, il *Fornitore* svolge l'analisi dei rischi tenendo conto, in special modo, dei rischi che derivano dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale ai *Dati Personali*.

2. Le modalità di svolgimento, da parte del *Fornitore*, delle attività di analisi e individuazione delle *Misure di Sicurezza* dovranno essere conformi alle *Norme in materia di Protezione dei Dati Personali,* ivi inclusi gli standard applicabili in materia di *cybersecurity,* nonché ai codici di condotta di settore e/o dalle certificazioni, ove esistenti e/o acquisite ai sensi degli artt. 40 - 43 del Regolamento. In particolare, ai fini della verifica circa il corretto svolgimento delle attività di analisi dei rischi, sarà

tenuta in considerazione la circostanza che le stesse siano improntate ai principi ed alle indicazioni presenti negli standard di qualità ISO del settore ed in particolare:

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

3. Il *Fornitore* si impegna ad assistere, su richiesta, *Sogei* e/o l'*Amministrazione Cliente* (nel caso in cui quest'ultima sia il *Titolare del trattamento*) ai fini di una periodica valutazione circa l'efficacia delle *Misure di Sicurezza* adottate.

4. Il *Fornitore* si impegna ad assistere *Sogei* e/o l'*Amministrazione Cliente* (nel caso in cui quest'ultima sia il *Titolare del trattamento*) per il tramite di *Sogei* sia a livello tecnico che organizzativo nello svolgimento della valutazione di impatto sulla protezione dei dati personali ("*DPIA*"), così come disciplinata dall'art. 35 del Regolamento, in tutte le ipotesi in cui il *Trattamento* preveda, necessiti o imponga lo svolgimento e/o l'aggiornamento della stessa. Il *Fornitore* presterà la propria assistenza nell'attività di consultazione preventiva dell'Autorità di controllo ai sensi dell'art. 36 del Regolamento fornendo tutte le informazioni all'uopo necessarie.

5. Nello svolgimento delle attività di cui al presente paragrafo **III.A)** e, più in generale, nell'esecuzione delle attività contrattuali che comportino il *Trattamento di Dati Personali*, il *Fornitore* tiene conto dei principi della protezione dei dati fin dalla progettazione e per impostazione predefinita ("*privacy by design*" e "*by default*") anche mediante l'ausilio delle istruzioni ricevute; nel caso in cui le attività oggetto del *Contratto* prevedano lo sviluppo di software, il *Fornitore* si impegna comunque a supportare *Sogei* nell'applicazione di tali principi attenendosi ai processi e ai metodi aziendali adottati dalla stessa *Sogei*.

III.B) *Obblighi in caso di "data breach"*

1. Il *Fornitore* deve prestare la propria assistenza e collaborazione nell'adempimento di cui agli artt. 33 e 34 del Regolamento.

2. In particolare, il *Fornitore* deve:

a) documentare gli *Incidenti di Sicurezza* e le Violazioni di dati personali riferibili ai *Trattamenti* delegati da *Sogei*, ad esempio predisponendo un apposito registro, includendo le informazioni di cui all'art. 33 del Regolamento e si impegna, su richiesta, a rendere tale documentazione disponibile a *Sogei*;
b) comunicare a Sogei, immediatamente e, in ogni caso, non oltre le 24 h, ogni *Violazione dei dati personali* da quando il *Fornitore*, o un suo *Sub-Responsabile*, ne ha avuto conoscenza o ha avuto elementi per sospettare che sia avvenuta una Violazione. Tale comunicazione deve essere redatta in forma scritta e contenere tutte le informazioni richiamate all'art. 33 del Regolamento ed essere trasmessa a *Sogei* attraverso l'indirizzo di posta elettronica certificata cert@pec.sogei.it, insieme a tutta la documentazione necessaria per consentire al *Titolare* (*Sogei* o l'*Amministrazione Cliente*) di notificare, eventualmente in via preliminare, detta Violazione all'Autorità di controllo competente entro i termini di legge;
c) collaborare con *Sogei* e/o con l'*Amministrazione Cliente* (nel caso in cui quest'ultima sia il *Titolare del trattamento*), anche al fine di consentire il completamento del processo di notifica all'Autorità di controllo, nelle ***(i)*** attività di indagine, al fine rilevare tutte le evidenze necessarie a valutare le cause, la natura e gli effetti della *Violazione dei dati personali*, nonché ***(ii)***

nell'adozione delle azioni necessarie a mitigare qualsivoglia danno o conseguenza lesiva per i diritti e delle libertà degli Interessati e ***(iii)*** nella predisposizione e implementazione, previa approvazione di *Sogei*, di un piano di misure per la riduzione tempestiva delle probabilità che una *Violazione dei dati personali* simile a quella occorsa possa ripetersi in futuro;

d) in ogni caso in cui *Sogei* debba fornire informazioni (inclusi i dettagli relativi ai servizi prestati dal *Fornitore*) all'*Amministrazione Cliente* (nel caso in cui quest'ultima sia *Titolare del trattamento*) e/o all'Autorità di controllo, il *Fornitore* supporterà *Sogei* nella misura in cui le informazioni richieste e/o necessarie siano esclusivamente in possesso del *Fornitore* e/o di suoi *Sub-Responsabili*.

IV. ULTERIORI OBBLIGHI DEL FORNITORE

1. Il *Fornitore* si impegna a trasmettere tutte le informazioni e la documentazione che *Sogei* potrà ragionevolmente richiedergli durante l'esecuzione del *Contratto,* per verificare il rispetto, da parte del *Fornitore* o dei suoi *Sub-Responsabili del trattamento*, delle previsioni del presente *Allegato Privacy* e delle *Norme in materia di Protezione dei Dati Personali* e delle istruzioni ricevute.

2. Il *Fornitore* garantisce che *Sogei* possa svolgere presso lo stesso e/o i suoi *Sub-Responsabili*, anche per mezzo di terzi autorizzati e con ragionevole preavviso, attività di controllo e valutazione, anche mediante ispezioni e sopralluoghi nei locali o nelle strutture fisiche del *Fornitore*, delle attività di *Trattamento dei Dati Personali* eseguite dal medesimo *Fornitore*, ivi incluso l'operato degli eventuali *AdS*, allo scopo di verificarne la conformità al *Contratto*, al presente *Allegato Privacy* e alle *Norme in materia di Protezione dei Dati Personali* e alle istruzioni ricevute. Il *Fornitore* deve mettere a disposizione, senza alcun ritardo e/o omissione, tutte le informazioni necessarie per dimostrare la sua conformità con i suddetti obblighi, incluse eventuali certificazioni in suo possesso. Nel caso in cui all'esito di detti controlli, le *Misure di Sicurezza* risultino inadeguate e/o inidonee ad assicurare l'applicazione delle *Norme in materia di Protezione dei Dati Personali*, *Sogei* diffiderà il *Fornitore* 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), fatti salvi i rimedi esperibili ai sensi del *Contratto* e/o della legge.

3. Il *Fornitore* dovrà rendere immediatamente edotto e coadiuvare *Sogei* e/o l'*Amministrazione Cliente* (nel caso in cui quest'ultima sia il *Titolare del trattamento*) in caso di ispezioni, di eventuali misure adottate nei suoi confronti o in caso di procedure dinnanzi alle Autorità per la protezione dei dati personali, nazionali ed europee, e/o all'Autorità Giudiziaria in relazione ai *Trattamenti* demandatigli e salvo il caso in cui tale comunicazione non sia vietata dal provvedimento o dalla legge.

4. In simili circostanze, salvo divieti previsti dalla legge, il *Fornitore* deve: ***i)*** informare *Sogei* tempestivamente, e comunque entro e non oltre 24 ore dal ricevimento della richiesta di ostensione; ***ii)*** collaborare con *Sogei* e/o con l'*Amministrazione Cliente* (ove quest'ultima sia il *Titolare del trattamento*), nell'eventualità in cui gli stessi intendano opporsi legalmente a tale comunicazione; ***iii)*** garantire il trattamento riservato di tali informazioni;

5. Qualora *Sogei* e/o l'*Amministrazione Cliente* (ove quest'ultima sia il *Titolare del trattamento*) abbia/no necessità, per lo svolgimento di compiti istituzionali, di accedere ai *Dati Personali* oggetto di *Trattamento* che non siano disponibili attraverso i servizi applicativi, il *Fornitore* si impegna, anche per conto dei suoi *Sub-responsabili*, a rendere disponibili tali *Dati Personali* secondo linee guida da

concordare nel corso dell'esecuzione del *Contratto* e, in ogni caso, prima dell'avvio delle attività di *Trattamento*.

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

1. Il *Fornitore* dovrà garantire che i *Dati Personali* siano trattati su infrastrutture – ivi ricomprese le infrastrutture deputate alle funzioni di business continuity e di disaster recovery, anche se esternalizzate – localizzate all'interno dell'UE, salvo motivate ragioni di natura normativa o tecnica.
2. Nel caso di servizi di assistenza/manutenzione da remoto il cui espletamento implichi comunque il trasferimento al di fuori dell'UE di tracciati di dati connessi al servizio stesso, gli eventuali *Dati Personali* contenuti nel tracciato devono essere opportunamente anonimizzati a cura del *Fornitore*.
3. Nel caso si renda necessario un trasferimento di *Dati Personali* al di fuori dell'UE per l'erogazione di servizi connessi al *Contratto* – da intendersi anche come accesso ai dati da un paese terzo – il *Fornitore* potrà procedere al trasferimento dei dati verso un paese terzo o un'organizzazione internazionale al di fuori dell'UE o dello Spazio Economico Europeo che siano coperti da una decisione di adeguatezza resa dalla Commissione europea ai sensi dell'art. 45 Regolamento o da altre garanzie adeguate di cui agli artt. 46 e ss. del Regolamento stesso (es. utilizzo delle clausole contrattuali tipo adottate dalla Commissione europea ai sensi dell'art. 46, par. 2, lett. c) del Regolamento, utilizzo delle norme vincolanti d'impresa Binding Corporate Rules - BCR), fatta salva la necessità valutata preventivamente tra le parti di adottare eventuali misure supplementari per garantire l'efficacia di tali garanzie.
4. Il *Fornitore* trasmette a *Sogei*, nella persona del *DDE*, la lista dei trasferimenti di dati extra-UE che intende effettuare alla data di sottoscrizione del *Contratto* – contenente l'indicazione del soggetto che riceve i dati, del paese di destinazione e delle adeguate garanzie su cui si fonda il trasferimento. Attraverso apposita comunicazione al *DDE*, il *Fornitore* si impegna ad informare *Sogei* e l'*Amministrazione Cliente* (nel caso in cui quest'ultima sia il *Titolare*) della cessazione o dell'intenzione di avviare nuovi trasferimenti di dati al di fuori dell'UE nel corso della durata del *Contratto.*
5. Nel caso in cui il trasferimento si renda necessario per adempiere a un requisito specifico a norma del diritto dell'Unione europea o italiano cui è soggetto il *Fornitore*, quest'ultimo è tenuto ad informare *Sogei* circa tale obbligo giuridico, prima del *Trattamento*, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.
6. Qualora dovessero risultare trasferimenti di dati extra-UE in assenza delle adeguate garanzie di cui sopra, il *Fornitore* verrà diffidato all'immediata interruzione del trasferimento di dati non autorizzato, fatti salvi i rimedi previsti dalla legge e/o dal *Contratto*.

VI. OBBLIGHI DEL FORNITORE AL TERMINE DEL CONTRATTO

1. La durata del *Trattamento* dei *Dati Personali* è limitata e coincide con la durata del *Contratto* e delle sue eventuali proroghe.
2. Al termine o alla cessazione del *Trattamento* per qualsiasi causa, il *Fornitore* si impegna, per sé e anche per i propri *Sub-Responsabili*, a restituire a *Sogei* i dati di cui siano venuti in possesso in esecuzione del *Contratto* e, successivamente, a cancellarne tutte le copie esistenti da qualsivoglia supporto informatico, *online* ed *offline*, utilizzato per la gestione e conservazione degli stessi. Sono fatti salvi i casi in cui la conservazione dei medesimi sia necessaria per adempiere ad obblighi di legge.

VII. MODIFICHE DELLE NORME IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

1. In ogni caso, qualora, durante la vigenza del *Contratto*, dovesse intervenire una modifica delle *Norme in materia di Protezione dei Dati Personali* che determini la necessità di ulteriori adempimenti, anche sotto il profilo delle *Misure di Sicurezza*, il *Fornitore* collaborerà con *Sogei*, nei limiti delle proprie risorse e delle proprie competenze tecnico-organizzative, affinché siano sviluppate, adottate e implementate le necessarie misure correttive e/o di adeguamento.