ALLEGATO PRIVACY

PREMESSA

1. 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 dalla *Sogei*, anche attraverso il *Contratto*, che rivestono la qualifica di *Titolari del Trattamento* e per cui *Sogei* riveste la qualifica di *Responsabile primario del trattamento*. In tal caso il Fornitore rivestirà la qualifica di *Sub-Responsabile 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'10 del Regolamento UE 2016/679), messi a disposizione, trasmessi, gestiti, controllati o comunque trattati da *Sogei* (anche per conto delle Amministrazioni pubbliche Clienti di *Sogei*).
- *"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 UE.
- "*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* (ovvero le Amministrazioni pubbliche che si avvalgono di *Sogei* per la realizzazione e l'erogazione dei servizi informatici) o, ricorrendone le condizioni, con riferimento alle attività oggetto del *Contratto*, quale *Titolare autonomo 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 (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.
- "*Misure di Sicurezza*": le misure di sicurezza di natura tecnica e organizzativa atte a garantire un livello di sicurezza adeguato al rischio, ivi comprese quelle specificate nel *Contratto*, unitamente ai suoi Allegati.
- "*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 ("REGOLAMENTO UE"), 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 nazionale, nonché le linee guida e i provvedimenti interpretativi adottati dallo European Data Protection Board.
- "*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 sotto l'autorità diretta del *Responsabile primario* o del *Sub-responsabile* o del *Titolare autonomo*.
- "*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 del trattamento* (ovverosia la *Sogei* nel caso di dati di titolarità delle *Amministrazioni clienti* o il *Fornitore* nel caso di dati di cui *Sogei* è Titolare del trattamento).
- "*Responsabile della protezione dei dati (RDP)*": il soggetto designato dal Titolare ai sensi degli art. 37 e ss. del Regolamento UE anche denominato Data Protection Officer (DPO).
- "*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 tratta dati personali in forza di un accordo scritto con altro *Responsabile primario del trattamento*, ovvero il *Fornitore* o il subappaltatore/*Sub-Responsabile* autorizzato da *Sogei*.
- "*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* e o in taluni casi, ricorrendone le condizioni, il *Fornitore* qualora possa qualificarsi come *Titolare autonomo del trattamento*.
- "*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.

2. OGGETTO

Il presente documento (di seguito "***Allegato Privacy***"), costituisce parte integrante e sostanziale del *Contratto* tra *Sogei* e il *Fornitore*.

Il presente *Allegato Privacy* è redatto in conformità a quanto previsto all'art. 28 del Regolamento (UE) 2016/679 (di seguito "***Regolamento UE***") e disciplina le istruzioni che il *Fornitore* si impegna ad osservare nell'ambito dei *Trattamenti* dei *Dati Personali* che realizzerà nello svolgimento delle attività oggetto del *Contratto*, garantendo il rispetto della normativa vigente in materia di protezione e sicurezza dei dati.

Nell'ambito della procedura ad evidenza pubblica, il *Fornitore* ha dichiarato di essere in grado di assicurare idonee ed adeguate garanzie in termini di conoscenza specialistica, affidabilità, risorse, anche in ordine all'adozione di misure tecniche e organizzative per assicurare che i *Trattamenti* dei *Dati Personali* siano conformi alle *Norme in materia di Protezione dei Dati Personali*.

Con la sottoscrizione del *Contratto* e del presente *Allegato* Privacy, che forma parte integrante dello stesso, il *Fornitore* conferma la sua diretta ed approfondita conoscenza degli obblighi che si assume anche in relazione al *Contratto* e a quanto disposto dalle *Norme in materia di Protezione dei Dati Personali;* il Fornitore pertanto accetta, in funzione della attribuzione del ruolo e degli obblighi di cui all'art. 28 del *Regolamento UE* (d'ora in poi "nomina" o "designazione"), di essere designato quale *Responsabile primario* o *Sub – Responsabile del trattamento* dei *Dati Personali* salvo che, con riferimento alle attività oggetto del Contratto e ricorrendone le condizioni, il Fornitore , non sia Titolare autonomo del trattamento.

Rimane comunque inteso che ove le attività oggetto del *Contratto* non comportino il trattamento di *Dati* Personali o il Fornitore agisca in qualità di Titolare autonomo del trattamento, la nomina del *Fornitore* quale *Responsabile del trattamento* risulterà priva di efficacia.

Il presente documento contiene, inoltre, gli obblighi e le istruzioni per il *Trattamento* dei *Dati Personali* che il *Fornitore* e/o i suoi *Sub-Responsabili* si impegnano ad osservare nell'ambito dei *Trattamenti* effettuati in esecuzione del *Contratto*, garantendo il rispetto della normativa vigente in materia. 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 ulteriori *Misure di sicurezza* e di protezione.

Rimane comunque inteso che il mancato rispetto delle disposizioni del *Contratto* e del presente *Allegato Privacy* da parte del *Fornitore* sarà considerato quale grave inadempimento e determinerà la risoluzione del *Contratto* e gli effetti ad essa connessi conformemente a quanto previsto nel *Contratto* medesimo.

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

3. RUOLO DEL FORNITORE

Gli obblighi e le istruzioni riportate nel presente *Allegato Privacy* sono da considerarsi applicabili al *Fornitore* al di là del ruolo assunto nelle attività di *Trattamento* e possono essere integrate e derogate solo sulla base di ulteriori e specifici atti di istruzione e/o di nomina di *Sogei* e/o della *Amministrazione Cliente*. I successivi articoli, quindi, si riferiscono agli obblighi assunti dal *Fornitore* in relazione al *Trattamento* dei *Dati Personali* connessi all'esecuzione del *Contratto.*

Nell'ipotesi in cui nel *Contratto*, nei relativi Allegati o nei documenti rilasciati dalla *Sogei* sia specificato che, con riferimento alle attività in esso dedotte, il *Fornitore* assume la qualifica di *Titolare autonomo del trattamento*, quest'ultimo si impegna comunque ad osservare gli obblighi previsti nel *Contratto*, dalle *Norme in materia di Protezione dei Dati Personali* e, per quanto applicabili, dal presente *Allegato Privacy*.

Qualora nel *Contratto*, nei relativi Allegati o nei documenti rilasciati dalla *Sogei* sia specificato che, con riferimento ai *Dati Personali* trattati dal *Fornitore* in esecuzione del *Contratto*, *Sogei* riveste il ruolo di *Titolare del trattamento*, il *Fornitore* si impegna ad osservare tutti gli obblighi e le istruzioni previste nel *Contratto* e nel presente *Allegato Privacy* e nelle ulteriori istruzioni che saranno rilasciate allo stesso nei documenti tecnico-funzionali aventi rilevanza contrattuale.

Qualora nel *Contratto*, nei relativi Allegati o nei documenti rilasciati dalla *SOGEI* sia specificato che, con riferimento ai *Dati Personali* trattati dal *Fornitore* in esecuzione del *Contratto*, *Sogei* riveste il ruolo di *Responsabile primario del trattamento*, il *Fornitore* assumerà il ruolo di *Sub-Responsabile del trattamento*. In tal caso, il *Fornitore* si impegna ad osservare tutti gli obblighi e le istruzioni previste nel *Contratto* e nel presente *Allegato Privacy*, nonché tutte le eventuali ulteriori istruzioni impartite da *Sogei* in conformità a quanto ricevuto dal *Titolare del trattamento* e che imporranno al *Fornitore* gli stessi obblighi previsti in capo alla *Sogei* dell'*Amministrazione Cliente* rispetto al *Trattamento* dei *Dati Personali*.

In appendice sub. 2) si riportano, ai sensi dell'articolo 28, comma 4 del *Regolamento,* le Istruzioni Generali impartite dal *Titolare/Titolari* a *Sogei* in qualità di *Responsabile primario del trattamento* e che il *Fornitore* è tenuto ad osservare nell'esecuzione delle attività previste nel *Contratto*. Resta inteso che, in caso di contrasto, le istruzioni impartite dal *Titolare/Titolari* come previste dall'appendice sub. 2) prevarranno su quelle impartite dalla *Sogei* con il presente atto. Qualora le attività dedotte in *Contratto* fossero svolte dal *Fornitore* in favore di più *Titolari* prevarranno le Istruzioni Generali impartite dal *Titolare* nel cui interesse sono svolte le attività di *Trattamento* di *Dati Personali*.

Le *Amministrazioni Clienti*, inoltre, con riferimento alle attività oggetto del *Contratto*, possono designare direttamente il *Fornitore* quale *Responsabile primario del trattamento* ove quest'ultimo sia coinvolto in attività di *Trattamento* di *Dati Personali* di cui le *Amministrazioni Clienti* sono *Titolari*. In tal caso, il *Fornitore* si impegna ad osservare tutti gli obblighi e le istruzioni al *Trattamento* contenute nel Contratto e nel presente *Allegato Privacy*, nonché le ulteriori istruzioni impartitegli direttamente dalle *Amministrazioni Clienti*.

Rimane comunque inteso che ove le attività dedotte nel *Contratto* non comportino il trattamento di *Dati Personali*, la nomina del *Fornitore* quale *Responsabile del trattamento/Subresponsabile* risulterà priva di efficacia.

OBBLIGHI E ISTRUZIONI PER IL FORNITORE

I. CODICE ETICO

1. Il Fornitore si impegna al pieno rispetto di quanto previsto nel Codice Etico adottato da *Sogei* (presente sul sito www.sogei.it), obbligandosi al rispetto di quanto ivi indicato, delle norme sanzionatorie previste dalle *Norme in materia di Protezione dei Dati Personali* nonché dalle norme del codice penale in quanto applicabili, per tutti i *Dati Personali* che *Sogei* o suoi collaboratori dovessero comunicare ovvero per notizie, informazioni o documenti relativi all'attività svolta da *Sogei* per conto dell'*Amministrazione Cliente* di cui il *Fornitore* o i suoi collaboratori dovessero venire a conoscenza nell'esecuzione delle attività oggetto del *Contratto*.

II. OBBLIGHI DEL *FORNITORE*

1. Il *Fornitore* è autorizzato a trattare esclusivamente i *Dati Personali* necessari per l'esecuzione delle attività oggetto del *Contratto*.

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

- a garantire il pieno rispetto di quanto contenuto nel presente *Allegato* nonchè negli ulteriori documenti come previsto al successivo paragrafo II.A);
- non determinare o favorire mediante azioni e/o omissioni, direttamente o indirettamente, la violazione, da parte di *Sogei* e/o dell'*Amministrazione Cliente* delle *Norme in materia di Protezione dei Dati Personali*;
- trattare i *Dati Personali* esclusivamente in conformità alle istruzioni ricevute da *Sogei* e dalle *Amministrazioni Clienti*, nella misura necessaria all'esecuzione del *Contratto* e nel rispetto delle *Norme in materia di Protezione dei Dati Personali*;
- adottare, aggiornare e implementare *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* e/o *data breach*;
  - ogni violazione delle *Misure di sicurezza*;
  - tutte le altre forme di *Trattamento* non autorizzate o illecite.

3. Il *Fornitore* dovrà osservare tutte le *Norme in materia di Protezione dei Dati Personali*, ivi comprese quelle che saranno emanate nel corso dell'esecuzione del *Contratto* per assicurare 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, di accesso non autorizzato, anche accidentale o illegale, o *Trattamenti* non consentiti o non conformi alle finalità del *Trattamento*.

4. Il *Fornitore*, ricorrendo le condizioni di cui all'art. 37 del Regolamento UE, si impegna a designare la figura professionale del Responsabile della protezione dei dati (di seguito "***RPD***") e a comunicarne tempestivamente i dati di contatto a *Sogei* e all'*Amministrazione Cliente* (nel caso in cui il *Titolare* sia una *Amministrazione Cliente*).

II.A) Elementi essenziali del trattamento che il Fornitore è stato autorizzato a svolgere

1. Gli *elementi essenziali del Trattamento* di cui all'art. 28, paragrafo 3, primo capoverso, del Regolamento UE sono contenuti nel *Contratto*, nei suoi allegati, nel presente *Allegato Privacy* nonché nell'appendice sub 1 dello stesso.

2. Gli elementi essenziali del trattamento sono indicati in modo generico se riferiti a qualsivoglia tipologia di dati personali e di interessati e potranno coesistere con l'indicazione di elementi essenziali del trattamento più specifici (puntuali) se nell'ambito dell'esecuzione contrattuale si prevede lo svolgimento di attività di cui sono già noti i trattamenti di dati personali con un maggiore dettaglio.

3. Rimane comunque inteso tra le Parti che nel corso dell'esecuzione del *Contratto*, gli elementi essenziali del *Trattamento* potranno essere oggetto di integrazione, variazione o modifica da parte di *Sogei* o del *Titolare* (nel caso in cui il *Titolare* sia una *Amministrazione Cliente*).

4. Ove gli elementi essenziali del trattamento puntuali non siano conosciuti al momento della sottoscrizione del Contratto, gli stessi potranno essere forniti successivamente.

5. Rimane inteso che ove il Contratto preveda la prestazione di servizi con funzioni di "Amministratore di sistema" (di seguito "*AdS*"), il personale addetto del Fornitore potrebbe avere accesso e/o entrare in contatto con alcuni dei dati personali presenti nei sistemi di Sogei e/o delle *Amministrazioni Clienti*. Pertanto, il Fornitore sarà nominato Responsabile o Sub-responsabile del trattamento con riferimento alle operazioni di trattamento eventuali e coessenziali allo svolgimento dei servizi dedotti nel Contratto e provvederà a nominare individualmente le persone fisiche che svolgono le mansioni di AdS, come specificato nel successivo paragrafo II.B), in conformità al Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e successive modificazioni, autorizzandoli a svolgere esclusivamente le operazioni di trattamento strettamente attinenti agli ambiti affidati.

6. La durata del *Trattamento* dei *Dati Personali* è limitata e coincide con la durata del *Contratto* e delle sue eventuali proroghe e/o a specifici obblighi di legge.

II.B) Obblighi del *Fornitore*

1. Il *Fornitore* si impegna inoltre a:

- trattare solo i dati necessari per l'esecuzione delle attività oggetto del *Contratto*;
- informare immediatamente *Sogei* e il *Titolare* (nel caso in cui il *Titolare* sia una *Amministrazione Cliente*) 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*;
- 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 Regolamento UE;
- garantire la riservatezza dei *Dati Personali* trattati per l'esecuzione delle attività del *Contratto*;
- designare per iscritto le *Persone autorizzate al trattamento* individuando puntualmente gli ambiti di operatività consentiti. Il *Fornitore* deve tenere un elenco aggiornato contenente tutti i nominativi delle *Persone autorizzate al trattamento* dei dati e i relativi profili di autorizzazione e di accesso, con riferimento ai quali *Sogei* e/o l'*Amministrazione Cliente* potranno effettuare controlli periodici anche a mezzo di propri soggetti terzi all'uopo autorizzati;
- 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 dal *Fornitore*; ***iv)*** non lascino incustodita la postazione di lavoro ed evitino di lasciare incustoditi dispositivi hardware o documenti cartacei contenenti *Dati personali* o riservati; ***v)*** mantengano segrete le componenti riservate delle credenziali di autenticazione (password, pin, ecc.) che consentono l'espletamento delle attività; ***vi)*** non utilizzino alcun dispositivo rimovibile (CD, DVD, periferica USB) per la memorizzazione dei *Dati Personali* o riservati; ***vii)*** non estraggano *Dati Personali* su eventuali PC di "pool" (desktop o portatili) ovvero, nel caso ciò sia indispensabile in funzione della attività svolta, provvedano provvedere alla immediata cancellazione degli stessi; ***viii)*** in caso di dismissione di supporti rimovibili contenenti *Dati Personali* o riservati, provvedano alla loro formattazione in modo da rendere indisponibili i *Dati Personali* in essi contenuti, procedendo, in caso di impossibilità, alla loro distruzione; ***ix)*** riconsegnino qualsiasi dispositivo che contenga *Dati Personali* o riservati e mantengano riservata ogni informazione di cui fossero venuti a conoscenza nell'espletamento delle proprie attività;

- adottare e/o utilizzare un idoneo sistema di identificazione, autenticazione e autorizzazione di accesso ai *Dati personali* per le *Persone autorizzate al Trattamento*. Le operazioni effettuate dalle *Persone autorizzate* devono essere registrate e risultare consultabili, anche da *Sogei* e/o dal *Titolare* (nel caso in cui il *Titolare* sia una *Amministrazione Cliente*) nell'ambito dei propri compiti di vigilanza, nel rispetto della vigente normativa in materia di controllo a distanza dei lavoratori (art. 4 legge n. 300/1970);
- individuare e nominare, qualora ne ricorrano i presupposti, quali "Amministratori di Sistema" 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 monitorarne, ove applicabile, le relative attività conformemente a quanto indicato nel provvedimento da ultimo richiamato. In relazione alle attività di controllo dell'operato delle attività degli ADS, come previste nel suddetto provvedimento, il *Fornitore* potrà richiedere a Sogei le informazioni relative agli accessi logici, ove non nella sua diretta disponibilità. Tale elenco costantemente aggiornato dovrà essere inviato a *Sogei* nella figura del Direttore dell'esecuzione contrattuale (DDE) e/o del *Titolare* (nel caso in cui il *Titolare* sia una *Amministrazione Cliente*);
- garantire che le *Persone autorizzate* a trattare i dati personali in virtù del presente Contratto sono in possesso dei requisiti di moralità, esperienza, capacità e affidabilità richiesti dalle *Norme in Materia di Protezione dei Dati Personali*;
- ricorrendone i presupposti, adempiere agli obblighi di rilascio dell'informativa e di richiesta del consenso, ove necessario, nei confronti degli *Interessati*;
- 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 ricevute;
- 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[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*, pertanto, autorizza *Sogei* ad estrarre tali *Dati Personali* dai propri sistemi informativi esclusivamente per le predette finalità.

II.C) Obblighi del *Fornitore* con riferimento ai diritti esercitati dagli *Interessati*

1. Il *Fornitore* presta il proprio supporto e la propria collaborazione nel dare riscontro scritto, anche di mero diniego, alle istanze trasmesse dagli Interessati nell'esercizio dei diritti previsti dagli artt. 15-23 del Regolamento UE, ovverosia alle istanze per l'esercizio del diritto di accesso, rettifica, integrazione, cancellazione e di opposizione, di limitazione del trattamento, alla portabilità dei dati, nonché per l'esercizio del diritto a non essere oggetto di un processo decisionale automatizzato, compresa la profilazione.

2. Il *Fornitore* deve fornire tutto il supporto necessario affinché il riscontro fornito 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 provenienti dagli Interessati.

3. 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 dalla

[1] Il Fornitore dovrà a sua volta 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.

ricezione, per posta elettronica a *Sogei* e/o all'*Amministrazione Cliente* (nel caso in cui la stessa provveda a designare direttamente il *Fornitore* quale *Responsabile primario del trattamento)*.

II.D) Obblighi del *Fornitore* che ricorre a *Sub-Responsabili del trattamento*

1. Il *Fornitore* può ricorrere a *Sub-Responsabili* per l'esecuzione di specifici *Trattamenti* dando comunicazione tempestiva, e comunque prima dell'inizio delle attività di trattamento, a *Sogei* o, ove richiesto, al *Titolare* (nel caso in cui il *Titolare* sia una *Amministrazione Cliente*) dei nominativi/ragione sociale e delle attività di *Trattamento* da delegare; inoltre si impegna a trasmettere, ove richiesto, l'atto di designazione dei Sub-Responsabili. In caso di richiesta di subappalto l'impegno a nominare il sub appaltatore dovrà essere indicato nell'istanza di subappalto e dovrà essere formalizzato successivamente all'autorizzazione al subappalto rilasciata da Sogei.

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 UE, essere vincolati da un accordo scritto recante tutti gli obblighi 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* e/o dall'*Amministrazione Cliente*.

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* e dal *Titolare* (nel caso in cui il *Titolare* sia una *Amministrazione Cliente*), 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* e/o dall'*Amministrazione Cliente*.

4. A tal fine, *Sogei* e/o l'*Amministrazione Cliente* possono verificare in qualsiasi momento le garanzie e le misure tecniche ed organizzative adottate dal *Sub-Responsabile*, anche per mezzo di audit, assessment, sopralluoghi e ispezioni svolti mediante il proprio personale oppure tramite soggetti terzi all'uopo autorizzati. Nel caso in cui tali garanzie risultassero insussistenti e/o inadeguate, *Sogei*, in conformità a quanto contrattualmente previsto, potrà risolvere il *Contratto* con il *Fornitore*.

5. Nel caso in cui all'esito delle verifiche, ispezioni, audit e assessment le *Misure di Sicurezza* dovessero risultare inadeguate rispetto al rischio o, comunque, inidonee ad assicurare la protezione dei dati oggetto di *Trattamento*, *Sogei* applicherà al *Fornitore* una penale, come contrattualmente previsto, e diffiderà lo stesso a far adottare al *Sub-Responsabile* tutte le misure più opportune entro un termine congruo che sarà fissato all'occorrenza (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 *Sub-Responsabile* e/o del *Fornitore* a tale diffida, *Sogei* potrà risolvere il *Contratto* ed escutere la garanzia definitiva, fatto comunque salvo il risarcimento del maggior danno.

6. In ogni caso, rimane ferma la facoltà di *Sogei* o dell'*Amministrazione Cliente* di opporsi all'aggiunta o sostituzione del *Sub-Responsabile del trattamento* con altri *Sub-Responsabili*.

7. Qualora 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*, il Fornitore ne risponderà interamente nei confronti di *Sogei* e/o dell'*Amministrazione Cliente*, non potendo in alcun modo opporre che detto inadempimento è dovuto, in tutto o in parte, al *Sub-Responsabile*.

III. IL REGISTRO DEI TRATTAMENTI DEL FORNITORE

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 primario* o di *Sub-Responsabile del trattamento* (di seguito "***Registro***"), conformemente a quanto previsto dall'art. 30, comma 2, del Regolamento UE.

2. Su richiesta dell'Autorità di controllo, il *Fornitore* metterà a disposizione il *Registro* all'Autorità stessa dandone al contempo informazione a *Sogei* o al *Titolare* (nel caso in cui il *Titolare* sia una *Amministrazione Cliente*).

IV. OBBLIGHI DI SUPPORTO, COLLABORAZIONE E COORDINAMENTO DEL FORNITORE DEL TRATTAMENTO NELL'ATTUAZIONE DEGLI OBBLIGHI DI SOGEI

1. 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 UE, 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 il rispetto degli obblighi di cui all'art. 32 del Regolamento UE. 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 e/o dalle certificazioni, ove esistenti e/o acquisite ai sensi degli artt. 40 -43 Regolamento UE.

3. Il *Fornitore* svolge l'analisi dei rischi necessaria per valutare il livello di sicurezza e le *Misure di Sicurezza* necessarie per il *Trattamento*. Nello svolgimento di tale analisi, il *Fornitore* deve tenere conto, in special modo, dei rischi presentati dal *Trattamento* e che derivano, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, dal *Trattamento* non consentito o non conforme alle finalità del *Trattamento*.

4. Le modalità di svolgimento, da parte del *Fornitore*, delle suddette attività dovranno essere conformi:

- alle *Norme in materia di Protezione dei Dati Personali* e, in particolare, al Regolamento UE;
- al Documento WP 243 rev.01 – Linee guida sui responsabili della protezione dei dati (RPD) del 13 dicembre 2016;
- al 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.

5. Lo svolgimento di dette attività dovrà altresì improntarsi ai principi ed alle indicazioni presenti nei 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.

6. Rimane comunque inteso che ogni richiamo agli standard e/o Linee Guida indicate ai precedenti punti 4) e 5) deve intendersi riferito alla versione più recente, ove esistente.

7. In particolare, le attività da svolgersi dovranno soddisfare i criteri riportati di seguito, i quali potranno comunque essere soggetti a possibili aggiornamenti e modifiche:

a) analisi preliminare delle informazioni del *Trattamento* in oggetto;

b) individuazione dei dati strettamente necessari per il trattamento secondo i principi 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 attività che compongono il *Trattamento* (o funzionalità nel caso di servizio ICT);

d) classificazione del *Trattamento* in termini di caratteristiche privacy (finalità, liceità, interessati, ecc.),

e) valutazione del rischio per l'organizzazione (riservatezza, integrità e disponibilità);

f) valutazione della necessità e proporzionalità del *Trattamento* in relazione alle finalità;

g) valutazione dei rischi per i diritti e le libertà dell'*Interessato* relativi alla tipologia dei dati trattati;

h) valutazione dei rischi per i diritti e le libertà dell'*Interessato* relativi alla tipologia di *Trattamento*, come previsto dalle linee guida WP 248;

i) in caso di necessità di procedere a valutazione d'impatto, individuazione di misure di sicurezza specifiche e relativa valutazione di adeguatezza;

j) valutazione del rischio intrinseco complessivo per il *Trattamento* (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 conformemente agli standard richiamati al punto precedente;

k) redazione del documento contenente l'analisi dei rischi, le relative *Misure di Sicurezza* e la relativa valutazione di adeguatezza da proporre a *Sogei* e o al *Titolare* (nel caso in cui il *Titolare* sia una *Amministrazione Cliente*) secondo il modello documentale definito da *Sogei*; recepimento delle eventuali osservazioni di Sogei, del *Titolare*, RPD, Garante privacy e Autorità.

8. 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: ***i)*** identificazione e classificazione dei *Dati Personali* trattati anche in termini di riservatezza e integrità; ***ii)*** classificazione del *Trattamento* anche in termini di disponibilità; ***iii)*** valutazione dei rischi per l'*Interessato* e inerenti il *Trattamento*; ***iv)*** identificazione delle *Misure di Sicurezza* così come richieste ai sensi dell'articolo 32 del Regolamento UE.

9. Il *Fornitore*, ai sensi dell'art. 32, comma 4 del Regolamento UE, garantisce 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* 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 UE.

2. In particolare, il *Fornitore* deve:

- predisporre e aggiornare un registro contenente tutte le *Violazioni dei dati personali* e renderlo disponibile su richiesta;
- comunicare a *Sogei* e/o al *Titolare* (nel caso in cui il *Titolare* sia una *Amministrazione Cliente*), immediatamente e, in ogni caso, senza ingiustificato ritardo, ogni *Violazione di 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 UE ed essere trasmessa insieme a tutta la documentazione necessaria per consentire a *Sogei* e/o al *Titolare* (nel caso in cui il *Titolare* sia una *Amministrazione Cliente*) di notificare, senza ingiustificato ritardo, detta *Violazione* all'Autorità di controllo competente entro e non oltre il termine di 48 ore da quando ne ha avuto conoscenza;
- indagare sulla *Violazione dei dati personali* adottando tutte le misure tecniche e organizzative necessarie per eliminare o contenere l'esposizione al rischio e collaborare con *Sogei* e/o con il *Titolare* (nel caso in cui il *Titolare* sia una *Amministrazione Cliente*) nelle attività di indagine, mitigando qualsivoglia danno o conseguenza lesiva per i

diritti e delle libertà degli *Interessati* (c.d. "Misure di mitigazione") nonché ponendo in atto, previa approvazione di *Sogei* e/o dell'*Amministrazione Cliente*, un piano di misure per la riduzione tempestiva delle probabilità che una *Violazione* simile possa ripetersi in futuro;

- 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 *Sub-Responsabili*.

IV.C) Obblighi del *Fornitore* nella valutazione d'impatto

1. Per svolgere la valutazione d'impatto sulla protezione dei dati personali (di seguito "***DPIA***"), *Sogei* e il *Titolare* (nel caso in cui il *Titolare* sia una *Amministrazione Cliente*) devono consultarsi con il proprio RPD (art. 35, comma 2, del Regolamento UE).

2. Il Fornitore si impegna ad assistere *Sogei* e/o il *Titolare* (nel caso in cui il *Titolare* sia una *Amministrazione Cliente*), per il tramite di *Sogei*, sia a livello tecnico che organizzativo, nello svolgimento della DPIA, così come disciplinata dall'art. 35 del Regolamento UE, in tutte le ipotesi in cui il *Trattamento* preveda, necessiti o imponga lo svolgimento e/o l'aggiornamento della stessa.

3. I risultati della DPIA, anche per l'individuazione delle necessarie *Misure di Sicurezza*, andranno riportati dal *Fornitore* nel documento di analisi del rischio di cui al precedente art. IV.A) del presente *Allegato Privacy*.

4. Il *Fornitore* presterà la propria assistenza nell'attività di consultazione preventiva dell'Autorità di controllo ai sensi dell'art. 36 del Regolamento UE fornendo tutte le informazioni all'uopo necessarie.

V. ULTERIORI OBBLIGHI DI GARANZIA DEL FORNITORE DEL TRATTAMENTO

1. Il *Fornitore* si impegna ad adottare tutte le *Misure di Sicurezza* necessarie e a svolgere tutte le attività di formazione, informazione e aggiornamento ragionevolmente necessarie per garantire che il *Trattamento* riguardi sempre *Dati Personali* precisi, corretti e aggiornati - anche qualora il *Trattamento* consista nella mera custodia o attività di controllo dei dati - eseguito dal *Fornitore* o dai suoi *Sub-Responsabili*.

2. Il *Fornitore* si impegna a trasmettere tutte le informazioni e la documentazione che *Sogei* e/o il *Titolare* (nel caso in cui il *Titolare* sia una *Amministrazione Cliente*) potranno 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 *Contratto*, del presente *Allegato Privacy* e delle *Norme in materia di Protezione dei Dati Personali* e delle istruzioni ricevute, anche sotto il profilo delle *Misure di Sicurezza*.

3. Il *Fornitore* garantisce la possibilità che possano essere svolte presso lo stesso, anche per mezzo di terzi autorizzati e con ragionevole preavviso, attività di controllo e valutazione, anche mediante ispezioni e sopralluoghi, 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 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. 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* 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, *Sogei* potrà risolvere il *Contratto* ed escutere la garanzia definitiva, fatto salvo il risarcimento del maggior danno.

4. Il *Fornitore* dovrà rendere immediatamente edotto e coadiuvare *Sogei* e/o il *Titolare* (nel caso in cui il *Titolare* sia una *Amministrazione Cliente*) 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.

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

6. Il *Fornitore* prende atto e riconosce che, nell'eventualità di una violazione delle *Norme in materia di Protezione dei Dati Personali* nonché delle disposizioni del presente *Allegato Privacy*, oltre all'applicazione delle clausole relative alla risoluzione del *Contratto*, delle relative penali e dell'eventuale risarcimento del maggior danno, è fatta comunque salva la facoltà di *Sogei* di ricorrere, anche giudizialmente, a provvedimenti cautelari, ingiuntivi e sommari o ad altro rimedio equitativo, allo scopo di interrompere immediatamente, impedire o limitare il *Trattamento* o qualsivoglia utilizzo divulgazione dei *Dati Personali*.

7. Il *Fornitore* si impegna a tenere indenne e manlevata *Sogei* e il *Titolare* (nel caso in cui il *Titolare* sia una *Amministrazione Cliente*) da qualsiasi danno materiale, immateriale e reputazionale, diretto o indiretto, nonché da qualsivoglia costo, spesa (ivi incluse le spese legali), onere, interesse e/o sanzione che quest'ultima dovesse patire in conseguenza dell'inadempimento agli obblighi assunti con il *Contratto* e con il presente *Allegato Privacy* dallo stesso, dai suoi *Sub-Responsabili* o dai suoi agenti, dipendenti, collaboratori, nonché di ogni altro soggetto da esso incaricato di eseguire le prestazioni dedotte nel *Contratto*.

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

1. Il *Fornitore* si obbliga a rispettare le istruzioni ricevute per il *Trattamento* anche nei casi di trasferimento verso un Paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui quest'ultimo è soggetto o rilevanti motivi di interesse pubblico; in tale ultimo caso, il *Fornitore* dovrà comunque rispettare le *Norme in materia di Protezione dei Dati Personali* e informare *Sogei* e/o il *Titolare* (nel caso in cui il *Titolare* sia una *Amministrazione Cliente*) di tale obbligo giuridico prima che il *Trattamento* abbia inizio, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.

2. Fatto salvo quanto sopra, *Sogei* o il *Titolare* (nel caso in cui il *Titolare* sia una *Amministrazione Cliente*) possono autorizzare per iscritto il *Fornitore*, o un suo *Sub-Responsabile del trattamento*, al trasferimento, anche parziale, dei *Dati personali* verso Paesi terzi od 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 Regolamento UE, oppure, in alternativa, previa valutazione della sussistenza delle garanzie adeguate di cui all'art. 46 del Regolamento UE da parte del *Titolare del trattamento*. Ove richiesto dalle *Norme in materia di Protezione dei Dati Personali*.

3. Nel caso in cui *Sogei* e/o le *Amministrazioni Clienti*, in relazione all'esecuzione degli obblighi assunti con il *Contratto*, consentissero al *Fornitore* o un suo *Sub- Responsabile* il trasferimento dei *Dati Personali* verso paesi terzi o organizzazioni internazionali, il *Fornitore* deve:

(i). convenire (e impegnarsi affinché i suoi *sub- Responsabili* convengano) di ottemperare agli obblighi in materia di *Trattamento* di *Dati Personali* previsti nel presente *Allegato Privacy* e nelle clausole del *Contratto* e nelle clausole contrattuali tipo di protezione dei dati adottate dalla Commissione Ue;

(ii). inserire nell'accordo di trasferimento con il *Sub - Responsabile* dei *Dati Personali* le disposizioni delle clausole del *Contratto*, delle clausole contrattuali tipo della Commissione Ue e delle *Norme applicabili in materia di Trattamento dei Dati Personali;*

(iii). adottare tutte le *Misure di Sicurezza* necessarie a garanzia dei dati oggetto di trasferimento.

Con la sottoscrizione del presente documento le Parti concordano che ai sensi dell'art. 46 del GDPR costituiscono garanzia adeguata per il trasferimento dei dati le clausole tipo di protezione dei dati adottate dalla Commissione e che il Fornitore ha sottoscritto tali clausole tipo di protezione dei dati adottate dalla Commissione con tutti i suoi Sub-Responsabili.

VII. OBBLIGHI DEL FORNITORE AL TERMINE DEL CONTRATTO

1. Al termine o alla cessazione del *Trattamento* per qualsiasi causa, il *Fornitore* si impegna, per sé e anche per i propri *Sub-Responsabili*, a non conservare e a distruggere in modo sicuro tutti i dati trattati in esecuzione del *Contratto*, cancellando tutte le copie esistenti in suo possesso, salvo i casi in cui la conservazione dei medesimi sia richiesta per adempiere ad obblighi di legge.

2. Il *Fornitore* e i suoi *Sub-Responsabili* devono documentare per iscritto detta cancellazione. Il *Fornitore*, previa richiesta, provvederà a rilasciare un'apposita dichiarazione scritta contenente l'attestazione che presso lo stesso o presso i suoi *Sub-Responsabili* non esiste alcuna copia di dati e/o informazioni di cui siano venuti in possesso in esecuzione del *Contratto*, salvo quelli la cui conservazione è necessaria in virtù della normativa applicabile. *Sogei* e/o il *Titolare* (nel caso in cui il *Titolare* sia una *Amministrazione Cliente*) si riservano il diritto di effettuare controlli e verifiche volte ad accertare la veridicità di detta dichiarazione.

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

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* e con il *Titolare* (nel caso in cui il *Titolare* sia una *Amministrazione Cliente*), nei limiti delle proprie risorse e delle proprie competenze tecnico-organizzative, affinché siano sviluppate, adottate e implementate misure correttive di adeguamento necessarie per l'adempimento delle prestazioni dedotte nel *Contratto*.

APPENDICE 1

ELEMENTI ESSENZIALI DEL TRATTAMENTO

Per elementi essenziali del trattamento di cui all'art. 28, paragrafo 3, del GDPR si intendono, con riferimento al *Contratto*, la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi ed i diritti del Titolare del trattamento.

Gran parte di tali elementi possono dedursi dal *Contratto* e dai suoi allegati e, pertanto, di seguito vengono comunicati i soli elementi essenziali non deducibili da tale documentazione ovverosia la natura e finalità del trattamento, il tipo di dati personali trattati, le categorie di interessati.

Gli elementi essenziali del trattamento sono indicati in modo generico se riferiti a qualsivoglia tipologia di dati personali e di interessati e potranno coesistere con l'indicazione di elementi essenziali del trattamento più specifici (puntuali) se nell'ambito dell'esecuzione contrattuale si prevede lo svolgimento di attività di cui sono già noti i trattamenti di dati personali con un maggiore dettaglio.

Si precisa che ai fini dell'esecuzione delle attività previste dal sopra citato *Contratto* codesta Società è autorizzata ad operare, nell'ambito dei Trattamenti/Servizi Ict/Servizi tecnici di seguito elencati in qualità di Responsabile ovverosia se i trattamenti sono svolti per la Sogei.

Elementi essenziali del trattamento - Generici				
Natura del Trattamento	**Finalità del trattamento**	**Macro-categorie di Dati personali**	**Categorie interessati**	**Per chi viene effettuato il trattamento**
Automatizzato	Informazione, formazione, cultura	Dati personali generici	Cittadini, dipendenti, Rappresentanti e dipendenti di enti/istituzioni, Operatori economici, Professionisti, intermediari	Sogei e Amministrazioni clienti Agenzia delle entrate Ragioneria Generale dello Stato - Sanità

APPENDICE 2

ISTRUZIONI IMPOSTE AL SUB-RESPONSABILE DEL TRATTAMENTO EX ART. 28, PAR. 4 DEL REGOLAMENTO

Ad integrazione di quanto previsto nell'*Allegato Privacy* e in virtù del ruolo di *Sub-Responsabile del trattamento* acquisito dal *Fornitore* nell'ambito dell'esecuzione del *Contratto*, la presente Appendice contiene le direttive, le istruzioni e gli obblighi imposti in materia di protezione dei *Dati Personali* a *Sogei* dal *Titolare del trattamento* e a cui il *Fornitore* dovrà attenersi conformemente a quanto indicato previsto dall'art. 28, parr. 2 e 4 dal predetto *Allegato Privacy*.

ISTRUZIONI GENERALI

1. ELEMENTI COMUNI

1.1 Il *Sub-Responsabile* è autorizzato a trattare, per conto dell'*Amministrazione Cliente*, tutti i *Dati Personali* di titolarità di quest'ultima e necessari per la corretta esecuzione del *Contratto*, escludendo i *Trattamenti* non autorizzati e comunque ulteriori a quelli esclusivamente necessari per l'esecuzione dell'incarico affidatogli. Gli *Elementi essenziali del trattamento* sono riportati nell'*Allegato Privacy*.

1.2 Il *Sub-Responsabile* si impegna a rispettare, nei limiti degli obblighi assunti con la sottoscrizione del *Contratto* e delle disposizioni del *Regolamento*, le istruzioni generali e specifiche contenute nella presente Appendice o comunicate per iscritto in un momento successivo, al riguardo vincolando anche le persone autorizzate al *Trattamento* ed eventuali fornitori *Sub-Responsabili* nel caso in cui ciò si renda necessario. Il *Titolare*, anche per il tramite di *Sogei*, comunicherà al *Sub-Responsabile* qualsiasi variazione si dovesse rendere necessaria nelle operazioni di *Trattamento*. Il *Sub-Responsabile* e le persone dallo stesso autorizzate al *Trattamento* non potranno effettuare nessuna operazione di *Trattamento* al di fuori di quelle ad esso demandate e delle eventuali variazioni richieste per iscritto dal *Titolare* o, su indicazione di questo, da *Sogei*.

1.3 Il *Sub-Responsabile*, conformemente anche a quanto indicato nell'*Allegato Privacy*, mette in atto le misure tecniche ed organizzative adeguate a garantire un livello di sicurezza commisurato al rischio presentato dal *Trattamento*, nel rispetto delle previsioni del *Contratto* e sulla base delle esigenze del *Titolare*, in particolare di distruzione, perdita, modifica, divulgazione non autorizzata o accesso, accidentale o illegale, di tali *Dati Personali* quando trasmessi, conservati o comunque trattati.

1.4 Il *Sub-Responsabile*, incluso chiunque agisca sotto la sua autorità ed abbia accesso ai *Dati Personali*, è tenuto alla riservatezza delle informazioni acquisite durante lo svolgimento delle attività per conto di *Sogei* e in favore del *Titolare del trattamento*.

1.5 La validità delle presenti istruzioni e dell'autorizzazione ad effettuare i *Trattamenti* di *Dati Personali* in favore del *Titolare* coincide con la durata del *Contratto*, ovvero di sue eventuali proroghe, fatti salvi l'adempimento di specifici obblighi di legge o di ulteriori documentate istruzioni impartite al *Sub-Responsabile del trattamento*.

***2.* OBBLIGHI DEL SUB-RESPONSABILE**

2.1 Il *Sub-Responsabile*, fatto comunque salvo quanto prescritto nell'*Allegato Privacy*, deve:

- trattare i *Dati Personali* esclusivamente per l'esecuzione delle prestazioni previste dal *Contratto* e per le relative finalità, nonché in modo lecito, corretto, trasparente e nel rispetto di tutti i principi di cui all'art. 5 del *Regolamento*.
- trattare i *Dati Personali* conformemente alle istruzioni, generali e specifiche, impartitegli dal *Titolare* e/o da *Sogei*;
- informare *Sogei* di ogni richiesta ricevuta a qualsiasi titolo direttamente dal *Titolare del Trattamento*;
- trattare i *Dati Personali* soltanto su istruzione documentata del *Titolare* o, su indicazione di questo, da *Sogei*, anche in caso di trasferimento di *Dati Personali* verso un Paese Terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il *Sub-Responsabile*; in tal caso esso 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;;
- informare immediatamente *Sogei* e/o il *Titolare del trattamento* qualora reputi che un'istruzione violi le *Norme in materia di protezione dei dati personali*, ovvero sia divenuto impossibile rispettarla, adottando comunque ogni possibile e ragionevole misura temporanea di salvaguardia, nonché concordando eventuali e ulteriori misure di protezione;
- informare tempestivamente e senza ingiustificato ritardo *Sogei* e/o il *Titolare* in caso di ispezioni o di richieste di informazioni e di documentazione da parte dell'Autorità di controllo relativamente alle attività di *Trattamento* demandate al *Sub-Responsabile*;
- prestare la propria assistenza al *Titolare*, sotto il profilo tecnico, per l'adempimento dell'obbligo sussistente in capo a quest'ultimo ai sensi degli artt. 13 e 14 del *Regolamento*;

- adempiere agli obblighi di cui all'art. 30, parr. da 2 a 4, del *Regolamento*, in relazione alle attività di *Trattamento* svolte per conto del *Titolare* e all'eventuale normativa specifica applicabile ai dati oggetto di *Trattamento*. Il *Sub-Responsabile* assicura la coerenza del proprio registro con quello di *Sogei* e del *Titolare*, nonché lo mette a disposizione dell'Autorità di controllo, ove richiesto, dandone al contempo informazione al *Titolare* e a *Sogei*;
- durante tutta l'esecuzione del *Contratto*, supportare il *Titolare*, anche tramite *Sogei*, nel tener conto dei principi della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita, anche nell'ambito dei servizi di sviluppo applicativo/MEV e infrastrutturale fin dalla fase di analisi dei requisiti;
- supportare *Sogei* nell'invio, anche per conto di quest'ultima, al *Titolare* di ogni documento richiesto da quest'ultimo per l'esecuzione dei servizi oggetto del *Contratto*, nonché raccogliere, registrare, organizzare, consultare ed eventualmente cancellare e distruggere i *Dati Personali* trattati per le finalità e lo svolgimento delle attività previste nel *Contratto* medesimo;
- qualora il *Contratto* avesse ad oggetto la fornitura di un *Servizio ICT*, procedere, nel rispetto delle modalità e degli obblighi da esso previsti, agli aggiornamenti periodici dei sistemi operativi e dei programmi per elaboratore volti a prevenire le vulnerabilità degli strumenti elettronici attraverso i quali è effettuato il *Trattamento* e a correggerne difetti, individuando anche quelli più confacenti ai tipi di dati e alle operazioni di *Trattamento* eseguibili con essi, secondo le indicazioni, le politiche e le linee guida definite dal *Titolare* e *Sogei* in materia di sicurezza delle informazioni.

2.2 Con specifico riferimento all'individuazione e all'istruzione delle persone autorizzate al *Trattamento*, il *Sub-Responsabile* deve:

- prevedere che esse agiscano conformemente all'ambito dell'operatività consentita in base agli accordi in essere, potendo effettuare le operazioni funzionali alla realizzazione e gestione delle attività demandate, senza eseguire *Trattamenti* di *Dati Personali* che non siano necessari o funzionali rispetto alle finalità perseguite e alle mansioni svolte;
- permettergli di accedere alle banche dati elettroniche e/o dai *Dati* del *Titolare* solo ed esclusivamente per l'esecuzione delle mansioni commissionate, ivi incluse le ragioni di sicurezza, operatività e manutenzione degli eventuali sistemi oggetto del *Contratto*. Le persone autorizzate al *Trattamento* non possono asportare supporti informatici contenenti *Dati Personali* senza espressa e preventiva autorizzazione;
- fare in modo che tali soggetti non creino nuove banche dati senza espressa autorizzazione e mantengano l'assoluto riserbo sui dati personali conosciuti, anche incidentalmente, in ragione dell'esercizio delle funzioni assegnategli. A tal fine, il *Sub-Responsabile* garantisce che le persone autorizzate al trattamento operanti sotto la sua autorità si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- fornirgli la formazione necessaria in materia di protezione dei *Dati Personali* e adottare tutte le misure necessarie affinché questi ultimi possano avere la piena conoscenza delle istruzioni impartitegli*;*
- vigilare affinché gli autorizzati al *Trattamento* rispettino le istruzioni loro impartite e le misure tecniche e organizzative predisposte, nonché richiamare gli stessi al rispetto delle predette istruzioni in caso di eventuali violazioni od ogni volta che ciò dovesse rendersi necessario;
- su richiesta del *Titolare*, mettere a disposizione una lista delle persone autorizzate al trattamento.

3. **FORNITURA DEI DATI AL TITOLARE**

3.1 Qualora il *Titolare* o soggetto/funzione da esso incaricata avesse necessità, per lo svolgimento dei propri compiti istituzionali, di accedere a *Dati* non disponibili attraverso i servizi applicativi, questi potranno essere richiesti per iscritto al *Sub-Responsabile* esplicitando la tipologia dei dati, la tempistica e la modalità di fornitura. Il *Sub-Responsabile* è tenuto a rendere disponibili tali dati eventualmente secondo linee guida da concordare.

3.2 Le eventuali richieste di fornitura dei dati e le relative risposte sono scambiate mediante comunicazioni protocollate. Il *Sub-Responsabile* è informato circa il/i soggetto/i autorizzati a richiedere la predetta fornitura dei *Dati*, con eventuali limitazioni di ambito.

4. **DESIGNAZIONE DEGLI AMMINISTRATORI DI SISTEMA**

4.1 Il *Sub-Responsabile*, fatto comunque salvo quanto prescritto nell'*Allegato Privacy*, deve:

- individuare gli *Amministratori di Sistema* e conformarsi alle prescrizioni contenute nel Provvedimento dell'Autorità Garante per la protezione dei dati personali del 27 novembre 2008 e s.m.i. in quanto compatibili con il *Regolamento* fino a nuova emanazione o revoca da parte dell'Autorità stessa;
- autorizzare formalmente ed in maniera tracciabile gli *Amministratori di Sistema*, impartendo loro adeguate istruzioni in relazione alle attività svolte sui sistemi e sui *Dati*, tenendo in considerazione gli ambiti di operatività agli stessi consentiti in base al profilo di autorizzazione;
- vigilare sul rispetto delle istruzioni impartite agli *Amministratori di Sistema*, sovrintendendo alle operazioni loro affidate in base agli ambiti di operatività consentiti dal profilo di autorizzazione;
- conservare e mantenere aggiornato un elenco degli *Amministratori di Sistema* che riepiloghi le funzioni e gli ambiti di operatività consentiti;

- mantenere segrete e custodire le credenziali di autenticazione assegnate alle persone fisiche abilitate ed utilizzate per l'accesso in qualità di *Amministratori di Sistema*;
- verificare, anche a campione e almeno annualmente, l'operato degli *Amministratori di Sistema* al fine di: (i) accertare il mantenimento dei requisiti soggettivi allo svolgimento dei compiti loro affidati; (ii) verificare la rispondenza del loro operato alle *Misure di Sicurezza* poste in essere per i *Trattamenti* di *Dati Personali*;
- adottare, nei limiti degli obblighi previsti dal *Contratto*, un idoneo sistema di identificazione, autentificazione, autorizzazione di qualsiasi tipo di accesso degli *Amministratori di Sistema*. L'accesso ai dati e le operazioni effettuate dagli Amministratori di Sistema devono essere tracciate e risultare consultabili dal *Sub-responsabile*, dal *Titolare* e/o da *Sogei* nell'ambito dei propri compiti di vigilanza e di audit. Le registrazioni degli accessi ai dati devono: (i) avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità; (ii) comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate; (iii) essere adeguate al raggiungimento dello scopo di verifica per cui sono state richieste; (iii) essere conservate per un congruo periodo di tempo comunque non inferiore a sei mesi.

5. SUPPORTO E COLLABORAZIONE DEL SUB-RESPONSABILE

5.1 Tenendo conto della natura del *Trattamento* e delle informazioni a sua disposizione, il *Sub-responsabile*, nei limiti e secondo le previsioni del *Contratto* e delle istruzioni contenute nell'*Allegato Privacy*, presta la propria assistenza per garantire il rispetto degli obblighi di cui agli artt. da 32 a 36 del *Regolamento*.

5.2 Il *Sub-Responsabile* coopera con i RPD designato rispettivamente dal *Titolare* e da *Sogei* nell'esecuzione dei compiti di cui all'art. 39 del *Regolamento*.

5.3 Il *Sub-responsabile* deve altresì:

- cooperare per fornire tutte le informazioni, i dati e la documentazione necessaria affinché il *Titolare* possa adempiere alle richieste dell'Autorità di controllo, ovvero qualora si rendessero necessarie informazioni in caso di verifiche ispettive, procedure precontenziose e contenziose. In tali casi, gli oneri economici relativi al soddisfacimento delle richieste non potranno essere addebitate né al *Titolare* né a *Sogei*;
- non diffondere i *Dati Personali* oggetto di *Trattamento*, con ciò intendendosi il dare conoscenza dei *Dati* medesimi a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- non comunicare i *Dati Personali* oggetto di *Trattamento* senza l'esplicita autorizzazione del Titolare, fatte salve le particolari esigenze di riservatezza espressamente esplicitate dall'Autorità Giudiziaria.
- assistere *Sogei* e/o il *Titolare* per sviluppare strategie di contrasto e di mitigazione dei rischi atte a ridurre, eliminare o accettare i rischi individuati in relazione a un *Trattamento*. Tali strategie devono tenere conto del contesto ove si svolge il *Trattamento*, delle categorie di *Dati* e di *Interessati*, nonché dei *Trattamenti* effettuati e del relativo progresso tecnologico;
- concordare, su richiesta, un piano di verifica e controllo sistematico del rispetto delle istruzioni, generali e specifiche, impartite in relazione ai *Trattamenti* di *Dati Personali* effettuati in favore del *Titolare*. Il *Sub-Responsabile* fornisce evidenza dell'attuazione del piano per mezzo di una relazione annuale, ove richiesta;
- tenere conto dei principi di protezione dei dati fin dalla progettazione e per impostazione predefinita, anche in caso di richieste di intervento di manutenzione evolutiva dei sistemi e delle applicazioni oggetto del *Contratto* su cui il *Sub-Responsabile* è autorizzato ad operare.

6. SUB-RESPONSABILI DEL TRATTAMENTO

6.1 Per l'esecuzione delle attività previste dal *Contratto*, il *Sub-Responsabile*, ove necessario, potrà ricorrere, ai sensi dell'art. 28, par. 2 del Regolamento, ad altri *Sub-Responsabili.* In tal caso, i *Sub-Responsabili* dovranno rispettare gli obblighi imposti dalle *Norme in materia di protezione dei dati personali* e contenuti nella presente Appendice, nonché nelle eventuali e ulteriori istruzioni eventualmente fornite dal *Titolare* in un momento successivo.

6.2 Il *Sub-Responsabile* informa *Sogei* circa eventuali modifiche riguardanti l'aggiunta o la sostituzione di eventuali *Sub-Responsabili* coinvolti nel *Trattamento*, dando così a *Sogei* la possibilità di opporsi a tale modifica e, conformemente alle istruzioni ricevute dalla stessa, a comunicarle al *Titolare del trattamento* affinché possa opporsi a tali modifiche fornendo specifiche motivazioni entro 15 giorni lavorativi a mezzo PEC o lettera raccomandata A/R. In assenza di opposizione, le modifiche/sostituzioni proposte si intenderanno approvate.

6.3 Fatto salvo quanto previsto dall'*Allegato Privacy*, qualora il *Sub-Responsabile* omettesse di adempiere ai propri obblighi in materia di protezione dei dati, il *Sub-Responsabile* iniziale conserva l'intera responsabilità nei confronti *di Sogei*.

***7.* DIRITTI DEGLI INTERESSATI**

7.1 Ove richiesto, il *Sub-Responsabile*, senza ingiustificato ritardo, dovrà assistere il *Titolare* nel dare riscontro scritto, anche se di mero diniego, alle istanze trasmesse dagli interessati ai fini dell'esercizio dei diritti previsti dagli artt. da 15 a 23 del *Regolamento*, vale a dire alle istanze relative 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 a un processo decisionale automatizzato, compresa la profilazione.

7.2 Qualora gli interessati trasmettessero le predette istanze al *Sub-Responsabile*, quest'ultimo deve inoltrarle tempestivamente a *Sogei*, affinché questa, a sua volta, possa tempestivamente inoltrarle al *Titolare*. Resta inteso che il *Sub-Responsabile* presterà ogni assistenza necessaria per soddisfare l'obbligo di dare seguito alle richieste per l'esercizio dei diritti degli interessati nei termini di legge.

8. MISURE DI SICUREZZA

8.1 Per ridurre e mantenere per quanto più possibile al minimo i rischi e i pericoli derivanti dal *Trattamento* dei *Dati Personali*, il *Sub-Responsabile* si impegna ad individuare le misure tecniche e organizzative più adeguate da mettere in atto sulla base delle indicazioni ricevute, in modo tale che il *Trattamento* soddisfi i requisiti del *Regolamento* e garantisca la tutela dei diritti degli interessati. Il *Sub-Responsabile*, sulla base di quanto previsto nella presente Appendice e delle ulteriori istruzioni e metodologie con lo stesso condivise, adotta tutte le *Misure di Sicurezza* richieste dall'art. 32 del *Regolamento*, assicurando altresì l'adozione di tutte le *Misure di Sicurezza* previste dal *Contratto*, dall'*Allegato Privacy* e dalle ulteriori *Norme in materia di Protezione dei Dati Personali*, tenendo altresì in considerazione le *best practice* applicabili in materia e i provvedimenti dell'Autorità di controllo nazionale ed europea.

8.2 Il *Sub-Responsabile* si obbliga ad aggiornare i sistemi di protezione della rete informatica e di interconnessione dei sistemi, anche individuando quelli più idonei all'esigenza di evitare accessi non consentiti, trattamenti illeciti e scongiurare l'eventuale perdita dei *Dati Personali*.

8.3 Il *Sub-Responsabile*, nel valutare l'adeguato livello di sicurezza, si impegna a tenere conto in special modo dei rischi presentati dal *Trattamento* che derivano, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso accidentale o illegale ai dati personali trasmessi, conservati o comunque trattati. Il *Sub-Responsabile* si impegna altresì a definire un piano di sicurezza informatico atto a presidiare i dati e i sistemi, il quale terrà conto delle misure organizzative e tecniche necessarie a seconda delle tipologie di dati oggetto di *Trattamento*.

8.4 Qualora il *Contratto* prevedesse attività di sviluppo ed evoluzione dei servizi ICT da realizzarsi per conto del *Titolare*, il *Sub-Responsabile*, in occasione della consegna della documentazione contrattualmente prevista al termine della fase di analisi dei requisiti, consegnerà a *Sogei* uno specifico documento contenente la valutazione dei rischi per la relativa approvazione da parte del *Titolare*, con particolare riguardo ai diritti e le libertà dell'interessato e le conseguenti "misure di sicurezza per la tutela del servizio", comprendenti anche le *Misure di Sicurezza* conseguenti alla valutazione d'impatto, ove necessaria, oggetto di valutazione e approvazione.

8.5 Il *Sub-Responsabile* dovrà prevedere attività di monitoraggio e di auditing con il fine di perfezionare o comunque migliorare le contromisure adottate, onde misurarne l'efficacia sul medio e lungo periodo.

9. VIOLAZIONE DEI DATI PERSONALI ("DATA BREACH")

9.1 Il *Sub-Responsabile del trattamento* è consapevole degli obblighi che incombono sul *Titolare del trattamento*, ai sensi degli artt. 33 e 34 del *Regolamento*.

9.2 Il *Sub-Responsabile* si impegna a comunicare a *Sogei* e al *Titolare* ogni violazione, conosciuta o anche solo sospettata, di *Dati Personali* ai sensi e nei termini previsti dagli artt. 33 e 34 del *Regolamento*. A tal fine, il *Sub-Responsabile* deve attenersi ai flussi di notifica del data breach contenuti nelle istruzioni specifiche riportate in calce alla presente Appendice, rendendo disponibile - senza ingiustificato ritardo e, ove possibile, entro 36 ore dalla scoperta dell'evento - ogni tempestiva e utile informazione per il corretto adempimento degli obblighi derivanti dalle norme da ultimo richiamate. Una volta definite le ragioni della *Violazione*, il *Sub-Responsabile*, di concerto con il *Titolare*, *Sogei* e/o altro soggetto da questi indicato, si attiveranno per implementare nel minor tempo possibile tutte le *Misure di Sicurezza* atte ad arginare il verificarsi di una nuova violazione della stessa specie con ogni mezzo e risorse ritenuti allo scopo necessari.

9.3 Il *Sub-Responsabile* assicura la massima collaborazione per approfondire tutti gli aspetti necessari e utili per identificare la violazione e si obbliga a mettere in atto tutte le eventuali azioni e misure aggiuntive indicate dal *Titolare*, anche tramite la *Sogei*, per far fronte alla *Violazione di dati personali*.

9.4 Il *Sub-Responsabile* mantiene un'accurata documentazione di tutte le *Violazioni di dati personali* registrate, comprese le circostanze ad esse relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione è integrata con le eventuali azioni intraprese dallo stesso e opportunamente comunicate al *Titolare* e a *Sogei*.

9.5 È fatto obbligo di mantenere l'assoluto riserbo sulle *Violazioni di dati personali* intercorse. Tali notizie non dovranno essere in alcun modo diffuse in qualunque forma, anche mediante la loro messa a disposizione o consultazione. La comunicazione della violazione è ammessa solo tra il *Titolare*, *Sogei* e altro soggetto da questi indicati e il *Sub-Responsabile*, fatte comunque salve quelle comunicazioni richieste dalla legge o da Autorità pubbliche.

10. VALUTAZIONE DI IMPATTO ("DPIA")

10.1 Il *Sub-Responsabile del trattamento* si impegna ad assistere il *Titolare*, a livello tecnico e organizzativo, nello svolgimento della DPIA, così come disciplinata dall'art. 35 del *Regolamento*, in tutte le ipotesi in cui il *Trattamento* preveda o necessiti di una preliminare valutazione di impatto sulla protezione dei dati personali o del suo aggiornamento.

10.2 Il *Sub-Responsabile* dovrà eventualmente operare attenendosi alle ulteriori istruzioni e/o metodologie eventualmente approvate dal *Titolare* o condivise da questo con *Sogei*, fornendo comunque a questi ultimi ogni informazione utile per il corretto adempimento degli obblighi di cui all'art. 35 del *Regolamento*. Il *Sub-Responsabile del trattamento* si impegna

altresì ad assistere il *Titolare* nell'attività di consultazione preventiva dell'Autorità di controllo prevista dall'art. 36 del *Regolamento*.

11. AUDIT

11.1 Il *Sub-Responsabile* si obbliga a rispettare gli stessi obblighi assunti da *Sogei* nei confronti del *Titolare*. A tal fine, il *Sub-Responsabile* accetta e riconosce che il *Titolare* ha il diritto di analizzare, verificare o valutare il rispetto da parte sua degli obblighi normativamente e contrattualmente al *Sub-Responsabile* nell'esecuzione del *Contratto*, ove ritenuto opportuno o necessario. Tali attività potranno essere effettuate previo accordo sui tempi e sulle modalità e comunque con un preavviso minimo di 3 (tre) giorni lavorativi, tenendo anche in considerazione gli impatti che tali attività potranno avere sulla corretta erogazione dei servizi oggetto del *Contratto*.

11.2 Tali attività potranno essere effettuate dal *Titolare* direttamente avvalendosi di proprie strutture interne, anche con l'eventuale supporto di risorse esterne ovvero da società/soggetti terzi di propria fiducia appositamente incaricati e vincolati ad accordi di riservatezza. Per dare esecuzione a quanto sopra, il *Sub-Responsabile* si obbliga ad offrire la massima collaborazione in modo da permettere a questi (ovvero alla società/soggetto terzo designato e preventivamente comunicato al Sub-*Responsabile*) di svolgere efficacemente la propria attività di audit sul *Trattamento*, la quale dovrà avvenire sempre alla presenza di personale del *Sub-Responsabile* e con la redazione di un verbale sottoscritto dalle parti.

11.3 Nel corso delle attività di audit, il *Titolare* avrà diritto di accedere ai locali del *Sub-Responsabile*, direttamente o tramite soggetti appositamente incaricati, i cui nominativi verranno preventivamente comunicati a quest'ultimo e avere copia di ogni dato, documento, informazione, elemento, contenuto di ogni genere e natura che possa risultare necessario alla esecuzione dell'audit sul Trattamento dei *Dati Personali*.

11.4 Qualunque non conformità addebitabile esclusivamente al *Sub-Responsabile* relativa (i) agli obblighi previsti nel presente documento, (ii) alla legge applicabile, (iii) alle policy o procedure previste e previamente comunicate al *Sub-Responsabile* , che dovesse emergere nel corso dell'attività di audit, fermo restando ogni diritto, ivi compreso il risarcimento del danno e le ipotesi di corresponsabilità indicate dalla normativa, dalla presente nomina e dai provvedimenti dell'Autorità di controllo, dovrà essere risolta dal *Sub-Responsabile* sopportandone i relativi costi e oneri e comunque in un congruo termine concordato di volta in volta con il *Titolare* tenuto conto dei necessari tempi tecnici di attuazione. Successivamente alla soluzione delle non conformità eventualmente rilevate, le attività di *Trattamento* dovranno essere perfettamente aderenti agli obblighi assunti dal *Sub-Responsabile* e alla legge applicabile.

11.5 Ove all'esito dei predetti controlli venisse riscontrato che il *Sub-Responsabile* non abbia rispettato gli obblighi assunti in materia di protezione dei dati, le istruzioni ricevute, ovvero non avesse messo in atto, in tutto o in parte, le misure poste a presidio dei *Trattamenti* e delle attività demandategli, il *Sub-Responsabile*, su indicazione di *Sogei* e/o del *Titolare*, si obbliga ad adottare tutte le misure necessarie e a tenere una condotta conforme alle istruzioni ricevute entro un congruo termine all'occorrenza congiuntamente fissato. In caso di perdurante non adeguamento e/o conformità alle istruzioni ricevute, il *Sub-Responsabile* accetta che *Sogei* potrà sostituirlo in ragione della gravità dell'inadempimento e degli obblighi contrattuali da essa assunti nei confronti del *Titolare*.

12. CONSERVAZIONE, CANCELLAZIONE E DISTRUZIONE DEI DATI

12.1 I *Dati Personali* oggetto di *Trattamento* da parte del *Sub-Responsabile* saranno conservati per tutto il periodo di esecuzione del *Contratto*.

12.2 Terminata la prestazione dei servizi oggetto del *Contratto*, il *Titolare*, anche per il tramite di *Sogei*, potrà richiedere in qualunque momento al *Sub-Responsabile* la cancellazione e/o la restituzione di tutti i *Dati Personali* oggetto di *Trattamento*, ovvero la cancellazione di tutte le copie esistenti, salvo che il diritto dell'Unione o l'ordinamento nazionale prevedano la conservazione dei dati ai sensi dell'art. 28 par. 3, lett. g) del *Regolamento*.

12.3 La sostituzione o la dismissione di strutture, sistemi e apparecchiature che comportino o possano comportare la cancellazione di *Dati Personali* deve avvenire sulla base di un'apposita procedura concordata con il *Titolare*, fatte salve le *Norme in materia di protezione di dati personali* e i provvedimenti vigenti, in quanto compatibili con il *Regolamento*. L'eventuale cancellazione di *Dati Personali* per i quali non siano fissati i termini e/o criteri di cancellazione può avvenire su esplicita autorizzazione del *Titolare*, anche per il tramite di *Sogei*.

12.4 Eventuali operazioni di restituzione dei *Dati Personali* dovranno essere concordate con *Sogei*, secondo le modalità operative e di sicurezza concordate da quest'ultima con il *Titolare*. La restituzione deve essere comunque accompagnata dalla distruzione di tutte le copie esistenti nei sistemi di informazione del *Sub-Responsabile*.

12.5 Ad ogni modo, una volta che i dati di titolarità dell'*Amministrazione Cliente* siano distrutti o cancellati, il *Sub-Responsabile* deve documentare per iscritto detta distruzione o cancellazione.

13. RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI

13.1 Il *Sub-Responsabile* comunica al *Titolare* e a *Sogei* il nome e i dati del proprio RPD designato conformemente all'art. 37 del *Regolamento*.

14. CODICI DI CONDOTTA

14.1 Nel caso in cui il *Sub-Responsabile* aderisse a un codice di condotta approvato ai sensi dell'art. 40 del *Regolamento* o a un meccanismo di certificazione approvato ai sensi dell'art. 42, tale adesione può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai parr. 1 e 4 dell'art. 28 del *Regolamento*.

15. RESPONSABILITÀ

15.1 Il mancato rispetto delle istruzioni generali e specifiche contenute nella presente Appendice, ivi comprese quelle relative alla nomina dei *Sub-Responsabili*, anche successivamente allo scioglimento o cessazione dell'efficacia del *Contratto* a qualsiasi causa dovuta e/o successivamente alla revoca della presente nomina, può comportare per il *Sub-Responsabile* le conseguenze di cui agli artt. da 82 a 84, nonché quelle previste dall'art. 28 par. 10 del *Regolamento*.

16. MODIFICHE E INTEGRAZIONI NORMATIVE

16.1 In caso di modifica delle *Norme in materia di protezione di dati personali* che comporti nuovi requisiti – incluse nuove misure di natura fisica, logica, tecnica ed organizzativa in materia di sicurezza del *Trattamento* di *Dati Personali* - il *Sub-Responsabile* supporta *Sogei* e il *Titolare* nell'individuazione della necessità di adeguamenti e di sviluppo, adozione e/o implementazione di misure correttive e nell'adottare, con eventuale revisione degli accordi contrattuali e dei derivanti oneri, le conseguenti misure necessarie.

16.2 Il *Sub-Responsabile* si impegna, altresì, a concordare la revisione del presente atto in conseguenza di modificazioni normative e/o convenzionali.

ISTRUZIONI SPECIFICHE

A. FLUSSO DI COMUNICAZIONE DEL DATA BREACH AL GARANTE DELLA PRIVACY

Il flusso inizia con l'identificazione di una possibile compromissione di dati personali nell'ambito della gestione di un incidente di sicurezza e si conclude con l'invio al Garante, da parte del *Titolare*, del modulo compilato previsto dal Regolamento UE 2016/679.

Tale flusso prevede, pertanto, l'interazione e lo scambio di informazioni specifiche con il *Titolare* impattato dall'evento, al fine di consentirgli di adempiere a quanto previsto dagli artt. 33 e 34 del *Regolamento*.

Ai sensi dell'articolo 4 del *Regolamento* per "violazione dei dati personali" (data breach) si intende 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.

DESCRIZIONE DEL FLUSSO

Il flusso di comunicazione al *Garante* da parte del *Titolare* prevede i seguenti passi:

1 Nel caso sia il *Sub-Responsabile* o *Sogei* a rilevare una possibile "violazione dei dati personali", queste ultime notificheranno tempestivamente al *Titolar*e (competente struttura di sicurezza informatica o struttura equivalente della stessa) che è in corso la gestione di un data breach, comunicando una descrizione dell'incidente sulla base delle informazioni disponibili e assegnando ad esso un identificativo univoco. Il *Sub-Responsabile* è sempre tenuto a dare preventivamente conoscenza a *Sogei* delle comunicazioni che lo stesso intende inviare al *Titolare*.

2 Nel caso in cui sia il *Titolare* a rilevare la possibilità di un data breach, comunica a *Sogei* una descrizione dell'incidente sulla base delle informazioni disponibili, assegnandogli un identificativo univoco. *Sogei*, ove lo ritenga necessario, provvederà a darne comunicazione al *Sub-Responsabile*.

3 Il *Sub-Responsabile* e/o *Sogei*, coordinando le strutture operative coinvolte, raccolgono tutte le evidenze necessarie al *Titolare* per verificare l'effettiva perdita o diffusione di *Dati Personali* e valutare l'entità della eventuale violazione, fornendo i dettagli tecnici e le eventuali informazioni aggiuntive in merito all'incidente e l'avanzamento dell'attività;

4 Nel caso in cui non siano stati riscontrati elementi che indichino la compromissione di *Dati Personali*, il *Sub-Responsabile* e/o *Sogei* terminano il flusso di comunicazione di data breach, notificando al *Titolare* coinvolto l'identificativo dell'incidente chiuso e le relative motivazioni.

5 In caso di riscontro positivo (accertamento di evidenze relative alla compromissione di *Dati Personali*), il *Sub-Responsabile* o *Sogei* trasmettono formalmente al *Titolare* coinvolto, senza ingiustificato ritardo, tutte le evidenze raccolte e le informazioni previste all'art. 33, par. 3 del *Regolamento* per quanto di propria competenza, conformemente al modulo reso disponibile dal Garante Privacy.

6 Il *Titolare*, ricevuta la comunicazione e il relativo modulo compilato, valuta il livello di gravità della violazione, in funzione della significatività dell'impatto sui *Dati Personali* di propria titolarità, e provvede a completare il modulo per la notifica con le informazioni di propria competenza. Il modulo compilato deve essere inviato al Garante Privacy secondo le modalità rese dallo stesso disponibili entro 72 ore dalla conoscenza dell'avvenuta compromissione dei *Dati Personali*, dandone contestualmente conoscenza a *Sogei* e al *Sub-Responsabile*.

7 Eventuali richieste di ulteriori informazioni o modifiche alla predetta comunicazione necessarie durante le attività di risoluzione dell'evento saranno concordate tra *Sogei*, il *Sub-Responsabile* e il *Titolare*.

8 Tutte le comunicazioni tra il *Titolare*, *Sogei* e il *Sub-Responsabile* riguardanti gli incidenti di sicurezza informatica sono trasmesse per conoscenza, ove presente, al CERT di *Sogei* e del *Titolare*.

9 Il *Sub-Responsabile* dovrà mantenere un'accurata documentazione di tutte le "violazioni di dati personali" registrate, comprese le circostanze ad esse relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione sarà integrata con le eventuali azioni intraprese dal *Titolare* e opportunamente comunicate allo stesso.

RACCOLTA DELLE INFORMAZIONI

Le informazioni previste dal *Regolamento* saranno raccolte e riportate nel modulo di notifica di data breach messo a disposizione del Garante Privacy.

Il *Sub-Responsabile* inserirà nel modulo le seguenti informazioni, le quali saranno comunicate al *Titolare*:

- ✓ descrizione della *Violazione dei dati personali*;
- ✓ intervallo temporale dell'incidente;
- ✓ luogo dell'incidente;
- ✓ modalità di esposizione al rischio (tipo di violazione, dispositivo oggetto della violazione);
- ✓ descrizione dei sistemi di elaborazione o di memorizzazione coinvolti;
- ✓ categorie di interessati;
- ✓ numero di persone colpite dalla *Violazione dei dati*;
- ✓ tipologia di dati coinvolti nella violazione;
- ✓ misure tecniche e organizzative applicate ai dati colpiti dalla violazione;
- ✓ misure attivate per il contenimento e la prevenzione;
- ✓ possibile conseguenza della violazione;
- ✓ proposta di contenuto della comunicazione ai contraenti o alle persone interessate.

Il *Titolare* oltre a procedere alla validazione e alla eventuale integrazione delle informazioni fornite dal *Sub-Responsabile*, inserirà nel modulo le seguenti informazioni:

- ✓ i dati organizzativi di riferimento e i relativi recapiti dell'ufficio del *Titolare* colpito dal data breach, il quale mantiene i rapporti con il Garante Privacy;
- ✓ il livello di gravità della violazione;
- ✓ l'eventuale comunicazione agli utenti interessati e le relative modalità;
- ✓ qualora la notifica al Garante Privacy non sia effettuata entro 72 ore, le motivazioni del ritardo.

B. FLUSSO DI NOTIFICA DI DATA BREACH AL TITOLARE DA PARTE DEL GESTORE DEI SISTEMI INFORMATIVI

DESCRIZIONE DEL FLUSSO

Il flusso di notifica al *Titolare* prevede i seguenti passi:

1 In qualità di *Sub-Responsabile*, il RPD del Gestore dei sistemi informativi, nel corso della gestione di un incidente di sicurezza, rileva una possibile "violazione di dati personali" (Data Breach).

2 Il RPD del Gestore dei sistemi informativi notifica al CERT della *Sogei* e al RPD della stessa che è in corso la valutazione di un incidente di sicurezza, comunicando una prima sommaria descrizione dell'incidente e assegnando ad esso un identificativo univoco.

3 Il RPD del Gestore dei sistemi informativi verifica l'eventuale ed effettiva "violazione di dati personali".

4 In caso di esito negativo della valutazione, il RPD del Gestore dei sistemi informativi termina il processo, notificando al CERT della *Sogei* e al RPD della stessa l'identificativo dell'incidente chiuso e le relative motivazioni.

5 In caso di esito positivo della verifica (ossia è stata accertata la "violazione dei dati personali", è stata svolta la relativa valutazione di impatto e stabilita la gravità del rischio per i diritti e le libertà delle persone fisiche secondo il modello eventualmente condiviso), il RPD del Gestore dei sistemi informativi lo comunica immediatamente e senza ingiustificato ritardo al DDE del Contratto e al RPD Sogei. La Sogei provvede a comunicare il Data Breach al *Titolare*..

Eventuali richieste di ulteriori informazioni o modifiche alla predetta notifica all'Autorità di controllo e necessarie durante le attività di risoluzione dell'evento saranno concordate con il Gestore dei sistemi informativi.

Il RPD del Gestore dei sistemi informativi manterrà un'accurata documentazione di tutte le "violazioni di dati personali" registrate, comprese le circostanze ad esse relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione sarà integrata con le eventuali azioni intraprese da *Sogei* e dal *Titolare*, se opportunamente comunicate anche al Gestore dei sistemi informativi.

RACCOLTA DELLE INFORMAZIONI

Le informazioni previste dal *Regolamento* saranno raccolte e inserite nella notifica di avvenuto Data Breach secondo lo schema seguente.

Il RPD del Gestore dei sistemi informativi inserirà nella notifica le seguenti informazioni, che saranno comunicate da *Sogei* al *Titolare*:

- tipologia di incidente;
- descrizione del servizio impattato e/o della banca/banche dati oggetto di *Violazione di dati personali*;
- intervallo temporale dell'incidente;
- luogo dell'incidente;
- misure tecniche di sicurezza applicate ai dati violati;
- misure attivate per il contenimento e la prevenzione;
- descrizione della natura della violazione dei *Dati Personali* compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- descrizione della probabile conseguenza della *Violazione dei dati personali*;
- descrizione delle *Misure di Sicurezza* adottate o di cui si propone l'adozione per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi;
- proposta di comunicazione di violazione di dati personali all'/agli interessato/i in base ad un'analisi dei dati oggetto di violazione (qualora la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche) e non ricorrendo alcuna delle condizioni di cui all'articolo 34, par. 3, del *Regolamento*, che escludono la necessità di comunicazione della violazione all'interessato.