

ALLEGATO 26

SCHEMA ACCORDO DI RISERVATEZZA

GARA A PROCEDURA APERTA AI SENSI DEL D.LGS. 50/2016 E S.M.I., PER L’AFFIDAMENTO DEI SERVIZI INTEGRATI DI CONDUZIONE, MANUTENZIONE E PRESIDIO TECNICO DEGLI IMPIANTI INDUSTRIALI A SUPPORTO DEL CENTRO ELABORAZIONI DATI E DEI DISASTER RECOVERY SITUATI PRESSO LE SEDI DI SOGEI S.P.A. - ID 2578



ACCORDO DI RISERVATEZZA

TRA

la SOGEI – Società generale d’Informatica S.p.A., con sede legale in Roma, Via Mario Carucci n. 99 - 00143, iscritta al registro delle imprese di Roma al n. 02327910580, coincidente con il numero di codice fiscale, partita IVA n. 01043931003, per la quale interviene il Dott. _____ in qualità di _____, che agisce per la stipula del presente atto in virtù dei poteri conferitigli dalla _____ elettivamente domiciliato ai fini del presente contratto in Via M. Carucci 99, 00143 – Roma;

E

La società _____ con sede legale in _____, Via _____, iscritta al Registro delle Imprese di _____ al n. _____, C.F. _____ e P.IVA _____, in persona del legale rappresentante dott. _____, domiciliato per la carica presso la sede sociale;

CONCORDATO CHE

salvo diversa esplicita indicazione, ai termini di cui in appresso, riportati in carattere corsivo e con iniziale maiuscola, viene attribuito, ai fini del presente atto, il significato indicato a fianco di ciascuno di essi:

- *Atto*: indica il presente Accordo di Riservatezza tra le *Parti*;
- *Contratto*: indica il Contratto rep. n. _____, stipulato in data _____, con la società in epigrafe avente ad oggetto “_____”;
- *Informazioni*: s’intendono per Informazioni tutti i documenti, le specifiche, i disegni, i progetti e le informazioni personali, nonché tecniche, amministrative e di mercato sulle attività rivelate in qualunque forma (cartacea o elettronica) e modalità (acquisite anche con la partecipazione a riunioni) dalla *SOGEI* alla *Società* nel corso dello svolgimento delle attività di cui al Contratto;
- *Parte*: indica a seconda dei casi la *SOGEI* o la *Società* _____;
- *Società* _____: indica la società come in epigrafe;
- *Parti*: indica congiuntamente la *SOGEI* e la *Società* _____.
- *SOGEI*: indica la *SOGEI – Società Generale d’Informatica S.p.A.*, come in epigrafe;

PREMESSO CHE

- la *SOGEI* per lo svolgimento della propria attività nonché per quella dei propri Clienti ha la

Classificazione del documento: Consip Public

Gara a procedura aperta ai sensi del D.Lgs. 50/2016 e s.m.i., per l’affidamento dei servizi integrati di conduzione, manutenzione e presidio tecnico degli impianti industriali a supporto del Centro Elaborazioni Dati e dei Disaster Recovery situati presso le sedi di Sogei S.p.A.

Allegato 26 – Schema Accordo di riservatezza e relativi allegati

pag. 2 di 10



necessità di:

✓;

✓ **[dettaglio attività di cui al Contratto espletate dalla Società]**

- in considerazione e sulla base di quanto precede, la *SOGEI* metterà a disposizione della *Società* in qualunque forma (cartacea e/o elettronica) documenti, specifiche, disegni, dati, informazioni tecniche, amministrative e di mercato sulle attività proprie e dei suoi Clienti (di seguito, in breve, “*Informazioni*”);
- la *SOGEI* intende rendere tali *Informazioni* soggette a specifici obblighi di riservatezza secondo i termini e le condizioni contenute nel presente *Atto*;

premesso quanto sopra, e costituendo le premesse parte integrante e sostanziale del presente *Atto* tra le *Parti*, come in epigrafe domiciliate e rappresentate,

SI CONVIENE E SI STIPULA QUANTO SEGUE

1. Ai fini del presente *Atto* s’intendono per *Informazioni* tutti i documenti, le specifiche, i disegni, le informazioni tecniche, amministrative e di mercato sulle attività rivelate in qualunque forma (cartacea o elettronica o con la partecipazione a riunioni) dalla *SOGEI* alla *Società* che siano:
 - a) relative ad attività passate, presenti o future riguardanti la *SOGEI* o i suoi Clienti ed in particolare dati ed informazioni relative alla ricerca, lo sviluppo, attività commerciali, i prodotti, i servizi e le conoscenze tecniche della *SOGEI* o dei suoi Clienti ivi incluse, a titolo meramente esemplificativo, informazioni riguardanti prodotti e servizi log di sistema, di rete, di prodotti o applicativi, informazioni su Clienti, progetti, piani, organizzazione degli stessi, progetti commerciali, e così via;
 - b) considerate da *SOGEI* come riservate, ovvero di proprietà della stessa e dei Suoi Clienti e/o protette da diritto d’autore e/o in parte oggetto di segreto industriale, privative, brevetti ecc.;
2. Con il presente *Atto*, la *Società*, in proprio anche per il fatto dei Suoi dipendenti e collaboratori, si impegna a mantenere strettamente riservate e a non divulgare a terzi, eccezion fatta per le specifiche e tassative ipotesi di cui in appresso, le *Informazioni*, e quant’altro di qualsiasi natura e forma abbia ricevuto sin dall’inizio delle attività, in qualsiasi forma diretta o indiretta da *SOGEI* per l’espletamento delle attività di cui alle Premesse, o di cui fosse venuta, comunque, a conoscenza in occasione delle medesime per tale esclusivo scopo e finalità. A tal fine si precisa che per:

- dirette: sono tutte le *Informazioni* che direttamente vengono rivelate alla *Società* in

Classificazione del documento: Consip Public

Gara a procedura aperta ai sensi del D.Lgs. 50/2016 e s.m.i., per l’affidamento dei servizi integrati di conduzione, manutenzione e presidio tecnico degli impianti industriali a supporto del Centro Elaborazioni Dati e dei Disaster Recovery situati presso le sedi di Sogei S.p.A.

Allegato 26 – Schema Accordo di riservatezza e relativi allegati

pag. 3 di 10



qualsiasi forma (cartacea o elettronica) dalla *SOGEI*;

- indirette: sono tutte quelle informazioni delle quali la *Società* ne è venuta a conoscenza da parte di altri soggetti e che riguardano la *SOGEI* stessa.

3. In relazione alla delicatezza dell'attività svolta ed alla necessità di esser venuto in possesso di notizie e/o documentazione della *SOGEI* estremamente riservate la *Società* si impegna, in proprio e anche per il fatto dei suoi dipendenti e collaboratori, ad osservare rigorosamente la massima riservatezza in ordine all'attività svolta ed ai risultati conseguiti, nonché in merito ad ogni dato o informazione di cui dovessero venire a conoscenza, anche dopo la conclusione delle attività di cui alle Premesse.
4. Per quanto riportato ai precedenti punti 2 e 3 la *Società* s'impegna a far apporre la firma autografa sul presente *Atto* ad ogni dipendente e/o collaboratore che sarà coinvolto nell'attività di cui all'*Atto* stesso; pertanto ogni volta che un dipendente e/o collaboratore della *Società* sarà coinvolto nelle attività di cui al presente *Atto*, nel corso della durata dello stesso, dovrà sottoscrivere il presente *Atto*. Della sottoscrizione dello stesso la *Società* dovrà darne immediata notizia alla *SOGEI* trasmettendo copia dell'atto controfirmato alla *SOGEI* stessa e, comunque, tale comunicazione dovrà pervenire alla *SOGEI* prima dell'avvio delle attività.
5. Ogni documento, specifica, disegno, informazione tecnica, amministrativa e di mercato sulle attività della *SOGEI* e dei suoi Clienti, e simili, di cui la *Società* possa esserne venuta in possesso nell'esercizio delle attività contrattuali resta di esclusiva proprietà di *SOGEI*.
6. Pertanto, tali dati o informazioni non potranno, in alcun modo ed in qualsiasi forma, essere comunicati o divulgati a terzi, né potranno essere utilizzati per fini diversi da quelli di stretta attinenza al presente incarico.
7. Tali dati, informazioni o documenti potranno essere comunicati o divulgati a terzi solo previa autorizzazione scritta da parte di *SOGEI*.
8. Resta inteso che, in caso di inosservanza degli obblighi di riservatezza di cui sopra, la *Società* precedentemente definita, responsabile di tale inosservanza sarà tenuta a risarcire tutti i danni diretti alla stessa imputabili che dovessero derivarne alla *SOGEI*.
9. La *Società* dichiara di conoscere ed accettare quanto previsto dal codice etico della *SOGEI* e, più' in particolare, dall'articolo "Riservatezza", 5° capoverso, dello stesso (presente sul sito www.sogei.it) e dall'articolo 326 del codice penale, il quale prevede specifici obblighi relativamente al segreto d'ufficio.
10. Gli impegni di cui al presente atto sono accettati senza riserve od eccezioni di sorta, nel caso in cui sia stata espressamente indicata la natura riservata delle Informazioni.

Classificazione del documento: Consip Public

Gara a procedura aperta ai sensi del D.Lgs. 50/2016 e s.m.i., per l'affidamento dei servizi integrati di conduzione, manutenzione e presidio tecnico degli impianti industriali a supporto del Centro Elaborazioni Dati e dei Disaster Recovery situati presso le sedi di Sogei S.p.A.

Allegato 26 – Schema Accordo di riservatezza e relativi allegati

pag. 4 di 10



11. La *Società* si impegna a non divulgare le *Informazioni* né a terzi né a propri collaboratori o persone comunque facenti parte della propria organizzazione non coinvolte nello svolgimento delle attività di cui al presente *Atto* ed a garantire che analogo grado di riservatezza sia rispettato dalle persone, anche giuridiche, alle quali le *Informazioni*, previa autorizzazione di *SOGEI*, dovessero essere divulgate per indifferibili ed indispensabili motivi di esecuzione delle attività di cui in Premessa; in tal caso sempre previa autorizzazione scritta della *SOGEI*, la quale conserva il diritto di vietarne la diffusione in qualsiasi momento mediante semplice comunicazione scritta.
12. L'obbligo di riservatezza permarrà sulle *Informazioni* per un periodo di 5 (cinque) anni dalla data di cessazione del Contratto di cui in Premessa ovvero, nel caso di sua anticipata risoluzione, in qualsiasi momento o per qualsiasi causa verificatasi, per i 5 (cinque) anni immediatamente successivi a tale data.
13. L'obbligo di riservatezza non si applica alle *Informazioni* che sono:
 - di pubblico dominio;
 - state autorizzate e legittimamente divulgate dalla *Parte* da cui le stesse provengono;
 - state divulgate in forza di norme di legge o di regolamento emanate da qualsiasi Autorità competente, ovvero divulgate a fronte di ordine di una Pubblica Autorità.
14. La messa a disposizione delle *Informazioni* non crea rapporti di natura privilegiata, siano essi di carattere tecnico, commerciale, industriale o societario tra le *Parti*, né implica obbligazioni a carico di *SOGEI* in ordine all'acquisto, alla vendita od alla cessione sotto qualsiasi altra forma, di prodotti o servizi che utilizzano le *Informazioni* né, infine, crea, presuppone od impegna al raggiungimento di accordi di licenza od altri diritti di privativa industriale.
15. Tutte le *Informazioni* dovranno essere restituite alla *SOGEI* senza possibilità, per la *Società* che le ha ricevute, di trattenerne copia e distruggendo, entro 30 (trenta) giorni dal termine del presente *Atto*, ogni supporto cartaceo, informatico, audiovisivo ecc. sul quale le medesime siano contenute, dovendosi fornire prova della avvenuta eliminazione.
16. Resta inteso che tutte le *Informazioni*, in qualsiasi forma esse siano, sono e rimangono di esclusiva proprietà della *SOGEI* e nessuno potrà per nessun motivo copiare le *Informazioni* senza averne ricevuto il preventivo consenso scritto dalla *SOGEI* stessa e, qualora tale consenso venga prestato, sulle copie dovranno essere riportate le informazioni sulla riservatezza e sulla proprietà che dovessero apparire sugli originali.
17. Il presente *Atto* e le obbligazioni dal medesimo derivanti non possono essere cedute, in tutto od in parte, a terze parti senza il consenso scritto di tutte le *Parti*.

Classificazione del documento: Consip Public

Gara a procedura aperta ai sensi del D.Lgs. 50/2016 e s.m.i., per l'affidamento dei servizi integrati di conduzione, manutenzione e presidio tecnico degli impianti industriali a supporto del Centro Elaborazioni Dati e dei Disaster Recovery situati presso le sedi di Sogei S.p.A.

Allegato 26 – Schema Accordo di riservatezza e relativi allegati

pag. 5 di 10



18. In caso di violazione degli obblighi di riservatezza derivanti dal presente *Atto*, oltre all'adozione di tutte le azioni o misure ritenute opportune o necessarie per la salvaguardia dei propri diritti ed interessi, la *SOGEI* avrà diritto al risarcimento dei danni diretti subiti.
19. Nel caso di controversia relativa alla interpretazione, esecuzione, risoluzione e/o validità del presente *Atto*, la medesima sarà devoluta alla competenza esclusiva del Foro di Roma.
20. Il presente *Atto* è entrato in vigore dall'inizio delle attività e rimarrà in vigore per il periodo di 5 (cinque) anni successivi alla data di completamento delle attività.
21. Nessuna modifica al presente *Atto* sarà considerata valida ed efficace a meno che non sia fatta per iscritto e sottoscritta da persone munite degli opportuni poteri.
22. Tale *Atto* rappresenta l'unico vincolo attualmente esistente tra le *Parti* in merito al medesimo oggetto. Il presente *Atto*, firmato digitalmente dalle *Parti*, nonché sottoscritto da ciascun dipendente e/o collaboratore, coinvolto nello svolgimento delle attività, si compone di n. 22 punti che costituiscono parte integrante e sostanziale dell'*Atto* stesso.

Società SOGEI–

Dott. _____

Legale rappresentante/altro

Società Generale d'Informatica SPA

Dott. . _____

Quale soggetto beneficiario

**Per presa visione ed accettazione
(firme dei dipendenti/collaboratori)**



ALLEGATO A

Trattazione di informazioni a carattere "controllate e/o sensibili"

1. Il responsabile della gestione delle informazioni a carattere "controllate e/o sensibili" assicura che l'accesso a tali informazioni sia consentito esclusivamente al personale che abbia necessità di conoscerle e sia stato istruito sulle responsabilità e sulle conseguenze penali di una divulgazione non autorizzata delle informazioni stesse.
1. Per la gestione e la custodia delle informazioni a carattere "controllate e/o sensibile" dette informazioni sono conservate in un contenitore chiuso a chiave che non consenta l'accesso non autorizzato.
2. I documenti, gli estratti e le traduzioni che contengono informazioni a carattere "controllate e/o sensibile" non possono essere riprodotti.
3. La documentazione a carattere "controllate e/o sensibile" deve essere iscritta in un apposito registro in cui devono essere annotati gli estremi della documentazione in arrivo e in partenza.
4. Per la distruzione dei documenti a carattere "controllate e/o sensibile" è necessario usare sistemi che assicurino la completa cancellazione dell'informazione - tritacarte o inceneritori per i documenti cartacei e frantumatori per i supporti informatici - ove non sia prevista la restituzione dei documenti alla SOGEI al termine dei lavori coperti dal contratto.
5. La trasmissione di informazioni a carattere "controllate e/o sensibile" non è consentita con sistemi elettrici o elettronici, quali fax commerciali, posta elettronica o altro sistema commerciale. È consentita la trasmissione mediante posta ordinaria, vettori commerciali o trasporto a mano, purché i documenti
6. siano chiusi in busta singola opaca che non riporti all'esterno indicazioni riferite al contenuto. Nel caso di trasmissione internazionale, il vettore dovrà consentire il tracciamento del plico.
7. In caso di smarrimento o divulgazione non autorizzata, accertata o presunta, delle informazioni a carattere "controllate e/o sensibile", il responsabile deve provvedere a segnalare l'evento alla SOGEI.



ALLEGATO B

Trattazione informatica di informazioni a carattere "controllate e/o sensibili"

Per trattare informazioni e dati a carattere "controllate e/o sensibili" tramite un sistema informatico:

- Il legale rappresentante - o altro soggetto, socio o dipendente opportunamente designato dal legale rappresentante - assume la veste di amministratore di sistema ed esercita tale funzione secondo la normativa in materia di seguito riportata.
- L'amministratore di sistema è responsabile degli aspetti tecnici e di sicurezza del sistema destinato a trattare informazioni a carattere "controllate e/o sensibili".
- Quando le informazioni a carattere "controllate e/o sensibili" sono trattate mediante sistemi informatici, l'amministratore di sistema deve assicurare che siano applicate le seguenti misure di sicurezza:
 - 1) Il sistema informatico deve essere isolato. A tal fine si deve:
 - rimuovere, dove possibile, la scheda hardware per il collegamento in rete o provvedere alla rimozione dei driver relativi, premessa l'assenza di alcun cavo collegato alla medesima;
 - rimuovere, dove possibile, la scheda hardware per il collegamento in rete a mezzo wireless (Wi-Fi, 3G, Bluetooth, ecc.) o provvedere alla rimozione dei driver relativi;
 - disabilitare l'utilizzo delle porte USB o comunque limitarne l'utilizzo alla sola utenza di amministratore di sistema;
 - 2) dotare il BIOS di password al fine di evitare la possibilità di avvio da CD/DVD o memorie rimovibili USB;
 - 3) installare un sistema operativo in possesso di certificazione Common Criteria di livello EAL3 o superiore, seguendo le indicazioni riportate nel documento di Security Target della specifica versione e delle guide di installazione e configurazione cui esso faccia riferimento;
 - 4) installare un sistema Antivirus, possibilmente in versione certificata Common Criteria per il sistema operativo prescelto;
 - 5) abilitare le funzioni di controllo accessi e configurare utenze nominative (non sono ammesse utenze di gruppo) con password non banali, di lunghezza non inferiore agli 11 caratteri e contenenti almeno tre dei seguenti criteri di sicurezza:
 - almeno un carattere maiuscolo;
 - almeno un carattere minuscolo;



- almeno un carattere speciale consentito dal sistema operativo (es. £,\$);
 - almeno un carattere numerico;
- 6) le password dovranno essere modificate dagli utenti dopo il primo accesso;
 - 7) deve essere presente una sola utenza con il possesso dei diritti di amministrazione;
 - 8) abilitare lo screen saver dopo massimo 5 minuti di inattività della postazione, con il ritorno alla schermata di ingresso al ripristino;
 - 9) abilitare il sistema di log del sistema operativo;
 - 10) abilitare il log delle stampe;
 - 11) abilitare l'audit degli eventi sia per il caso di successo che per il caso di fallimento:
 - controllo eventi accesso account;
 - controllo eventi di accesso;
 - controllo gestione degli account;
 - controllo degli usi dei privilegi;
 - controllo della modifica del criterio di controllo;
 - 12) disabilitare il controllo tramite remote desktop;
 - 13) non installare sistemi di remote desktop o ambienti di virtualizzazione;
 - 14) nei casi in cui si renda necessario l'impiego di software come Application Server, provvedere a installare prodotti in possesso di certificazione Common Criteria di livello EAL3 o superiore, seguendo le indicazioni riportate nel documento di Security Target della specifica versione e delle guide di installazione e configurazione cui esso faccia riferimento;
 - 15) nei casi di sviluppo di prototipi di applicazioni web che prevedano la presenza di un controllo accessi, questo deve essere connesso con l'archivio utenti del sistema operativo (Active Directory, ecc.) e comunque non può determinare una grana più fine rispetto alle utenze configurate su sistema operativo;
 - provvedere a effettuare gli aggiornamenti periodici del sistema antivirus e del sistema operativo in modalità off-line, solo dopo aver verificato la correttezza delle misure applicate e la corrispondenza della firma degli aggiornamenti scaricati da repository ufficiali del brand fornitore del sistema stesso;
 - 16) tutti i media a carattere "controllate e/o sensibili" in uso al sistema devono avere un numero identificativo;
 - 17) non si possono produrre stampe. Eventuali bozze devono essere distrutte al termine dell'esigenza;



- 18) il sistema deve essere installato in un ambiente ad accesso controllato, o comunque custodito in apposito contenitore di sicurezza. Deve essere anche valutata la possibilità di dotare l'ambiente di sistemi anti-intrusione in grado di monitorare l'eventuale accesso non autorizzato al sistema;
- 19) tutti gli utenti devono essere opportunamente istruiti a cura dell'amministratore di sistema in merito alle procedure di sicurezza implementate;
- 20) a cessata esigenza è necessario assicurare l'attuazione delle più accurate procedure per la completa cancellazione delle informazioni a carattere "controllate e/o sensibili" memorizzate o elaborate. In particolare l'amministratore deve curare che:
 - tutti i dischi rigidi presenti nel sistema siano sottoposti a una formattazione a basso livello e a quattro cicli completi di scrittura e cancellazione;
 - il sistema operativo sia re-installato, assicurando che le nuove utenze non utilizzino username e password in uso alla precedente installazione;
 - analoga procedura sia effettuata per i supporti di memorizzazione eventualmente presenti all'interno delle stampanti o di altre periferiche autorizzate.