FERSERVIZI
GRUPPO FERROVIE DELLO STATO ITALIANE

Area Acquisti di Gruppo
Il Responsabile

CHIARIMENTI

eGPA AGA n. 1/2022 Servizi professionali volti ad analizzare la sicurezza informatica dei sistemi informativi delle Società del Gruppo Ferrovie dello Stato Italiane - CIG 9068715C5A.

Allegati:
- *All. 1: Accordo di Data Protection*
- *All. 2: Accordo di Data Protection_altre società*

Con riferimento alla procedura in oggetto si riscontrano le seguenti richieste di chiarimenti ritenute di interesse generale.

1. Domanda:
"in merito al documento di offerte tecnico economica citato nei punto C.1.1 e C.1.3 dell'All. 5 "Capitolato Tecnico", l'effort economico farà riferimento esclusivamente alle tariffe giornaliere di cui al punto 4.2 del Disciplinare di gara"

Risposta
Si conferma. L'effort economico, definito nel *"documento di offerta tecnico economica"* di cui ai punti C.1.1 e C.1.3 del Capitolato Tecnico, dovrà fare riferimento alle tariffe giornaliere previste nel disciplinare di gara, così come da offerta migliorativa presentata in gara dall'operatore economico aggiudicatario.
Si precisa che la tariffa giornaliera è identificabile come una tariffa a corpo, comprensiva di tutti gli oneri che il fornitore deve sostenere per portare a termine l'attività.

2. Domanda:
"in merito al documento di offerte tecnico economica citato nei punto C.1.1 e C.1.3 dell'All. 5 "Capitolato Tecnico", il piano temporale e l'effort economico possono essere oggetto di revisione da parte del refente FS e in che misura"

Risposta
Il piano temporale e l'effort economico riportati nel *"documento di offerta tecnico economica"* di cui ai punti C.1.1 e C.1.3 del Capitolato Tecnico dovranno essere condivisi e negoziati con il referente FS ed, infine, accettati da quest'ultimo.

3. Domanda:
"sarebbe possibile avere lo schema di offerta tecnico/economica (All.ti 4 e 5) citata al punto h dell'art. 1 dell'All. 6 "Schema di accordo quadro""

Risposta
Non sono previsti degli schemi di offerta tecnica ed economica, in quanto la presentazione dell'offerta dovrà avvenire, in modalità telematica, tramite Portale Acquisti di Ferservizi secondo le modalità indicate rispettivamente nel paragrafo 7.B e 7.C, nonché nel paragrafo 8 del Disciplinare di gara.
Pertanto, gli All.ti 4 e 5 allo Schema di Accordo Quadro, denominati "Offerta Tecnica" ed "Offerta Economica", saranno materialmente allegati in fase di stipula, in quanto costituiti dall'Offerta tecnica ed economica prodotte in gara dal soggetto aggiudicatario/contraente.
Si chiarisce che tali documenti differiscono dal documento di offerta tecnico economica citato nel Capitolato Tecnico, punti C.1.1 e C.1.3, di cui ai precedenti quesiti nn. 1 e 2.

4. Domanda:
"sarebbe possibile avere una stima della quota parte di attività che verranno svolte presso le sedi del gruppo FS piuttosto che presso le sedi dell'affidataria"

Risposta
Il luogo di esecuzione delle attività di security assessment sarà definito di volta in volta in base alla tipologia del perimetro di analisi. Inoltre, si chiarisce che le sedi del Gruppo FS Italiane, che potrebbero rientrare nel perimetro di analisi, sono tutte le sedi del Gruppo FS Italiane sia nazionali che internazionali.
A titolo esemplificativo e non esaustivo si riporta che nell'ultimo triennio su 100 attività condotte il 90% sono state fatte presso sedi del Gruppo FS Italiane; il restante 10% presso le sedi del fornitore. Del 90% condotte presso le sedi del Gruppo FS Italiane, il 70% sono state condotte a Roma e il 30% presso altre sedi del Gruppo FS Italiane sul territorio nazionale.

5. Domanda:

"sarebbe possibile avere una stima della quota parte di attività che verranno svolte in orari notturni o nei giorni festivi"

Risposta

Non è possibile fornire tale indicazione, in quanto gli orari di esecuzione delle attività di security assessment saranno definite di volta in volta in base alla tipologia del perimetro di analisi e al contesto di business che viene impattato.

A titolo esemplificativo e non esaustivo si riporta che nell'ultimo triennio il 30% delle attività è stato condotto fuori dall'orario d'ufficio.

6. Domanda:

"L'applicazione delle penali di cui ai punti 4.b e 5.b fanno riferimento ad un ritardo di inizio delle attività oltre ai 7 giorni della approvazione del GANTT. Per il calcolo di tali giorni di riferimento si escludono i ritardi dovuti a causa di forza maggiore o causati dal gruppo FS?"

Risposta

In coerenza con l'art.55 delle Condizioni Generali di Contratto, si conferma che

"…La disapplicazione totale o parziale della penale da parte del Committente è consentita qualora ricorra una delle circostanze di seguito indicate:

i) il ritardo nell'esecuzione del contratto sia determinato da circostanze obiettive in nessun modo imputabili al Fornitore

ii) …"

7. Domanda:

7.1 *"In merito al punto 3 del paragrafo C.2.1 si chiede se l'esecuzione delle attività del remediation plan siano escluse dall'Accordo quadro. A titolo di esempio, nel caso in cui si riscontrassero delle vulnerabilità relative ad un server windows applicativo, le quali necessitano di remediation con relativa pianificazione delle attività di patching, l'oggetto dell'accordo quadro esclude l'esecuzione dell'attività di patching limitandosi solo alla pianificazione della stessa?*

7.2 *"Nel caso in cui siano comprese invece attività di remediation, è possibile avere un elenco degli applicativi, prodotti, soluzioni, apparati che sarebbero oggetto di tali remediation? Rispetto a tali applicativi, prodotti, soluzioni, apparati sono richieste certificazioni tecniche?"*

Risposta

7.1 e 7.2 Si conferma che le attività di applicazione delle remediation sono escluse dal presente Accordo Quadro. Al fornitore è richiesto solo la redazione dei piani di rientro (remediation plan) e la verifica continuativa, durante l'implementazione delle remediation da parte dei soggetti tecnici incaricati, che le soluzioni indicate nel piano siano applicabili al contesto anche, ove necessario, attraverso l'indicazione di ulteriori azioni di rientro emerse in corso d'opera.

8. Domanda:

"Rif.: Disciplinare - 4.1. B.1) Certificazioni Professionali (CP) = max 36 punti

Con riferimento al criterio di attribuzione dei punteggi tecnici relativi al possesso delle Certificazioni Professionali, chiediamo cortesemente quanto segue:

Quesito 1:

per concorrere all'attribuzione del punteggio previsto per il possesso delle certificazioni suddivise nelle tre macro-tipologie (T1,T2,T3) in capo a ciascuna figura professionale Senior e Junior

8.1• *è possibile presentare certificazioni anche di livello superiore a quelle richieste? Es. certificazione OSCE (superiore * alla OSCP, PEN-200, PEN-210, PEN-300, Exp-301, WEB-200)*

8.2• *per le risorse T1, è possibile presentare la certificazione eWPT (analoga alla WEB-200)?*

8.3• *possono considerarsi cumulabili i punti (3+3) qualora ci fossero più certificazioni possedute nella fascia T1? Es.: stessa risorsa in possesso di OSCP + WEB-300?"*

Risposta

8.1 e 8.2 No, le certificazioni che saranno prese in considerazione sono quelle elencate nel Disciplinare di gara. Potranno quindi essere prese in considerazione altre certificazioni, oltre a quelle elencate, esclusivamente se queste hanno come propedeuticità, certificata e riscontrata dall'ente certificatore, una di quelle elencate nel Disciplinare. In questo caso il valore del punteggio assegnato sarà relativo alla certificazione elencata propedeutica. L'onere della attestazione di propedeuticità, pena la non presa in considerazione della certificazione stessa, sarà a carico dell'Operatore economico aggiudicatario in fase di comprova;

8.3 No, come indicato nel paragrafo 4.1 B.1) del Disciplinare di gara il possesso da parte della singola persona di almeno una delle certificazioni professionali elencate per ciascuna macro-tipologia (T1, T2, T3) determina l'attribuzione del punteggio corrispondente (T1= 3 punti; T2= 2 punti; T3= 1 punto). Il punteggio tecnico massimo attribuibile ad ogni persona è di 6 punti, ottenibile per il possesso di almeno una certificazione per ciascuna delle tre le macro-tipologie di certificazioni.

In ogni caso, qualora una singola persona sia in possesso di più certificazioni appartenenti alla medesima macro-Tipologia, il punteggio attribuibile sarà comunque pari al massimo previsto per la macro-Tipologia medesima (T1 = 3, T2 = 2, T3 = 1).

9. Domanda:

"Partecipazione in costituendo RTI:

• in caso di partecipazione in costituendo RTI, sarà la solo Mandataria incaricata ad operare sul portale per il caricamento della documentazione anche a nome delle Mandanti?"

Risposta

Sì, si conferma.

Restano ferme tutte le indicazioni contenute nel Disciplinare di gara sulle modalità di presentazione della documentazione richiesta, nonché sulla relativa sottoscrizione.

10. Domanda:

"con riferimento al paragrafo 3.7 pagina 5 del disciplinare della Gara eGPA AGA 15/2021 Gara 5 CIG 8818357268 che recita: "l'aggiudicatario della presente gara (o suo subappaltatore) non potra' partecipare alla procedura di gara successiva per l'erogazione dei servizi di sicurezza informatica specialistici, ne potra' assumere il ruolo di subappaltatore", confermate che la partecipazione/aggiudicazione alla Gara in oggetto eGPA AGA n. 1/2022 Servizi professionali volti ad analizzare le sicurezza informatica dei sistemi informativi delle Societa' del Gruppo Ferrovie dello Stato Italiane – CIG 9068715C5A, non pregiudicherà la partecipazione/aggiudicazione alla procedura della gara dei servizi di sicurezza informatica specialistici citata nel disciplinare della Gara eGPA AGA 15/2021 di prossima futura emissione?"

Risposta

Allo stato non sono previste preclusioni nei confronti del concorrente/aggiudicatario della gara in oggetto eGPA AGA n. 1/2022 con riferimento alla partecipazione/aggiudicazione alla successiva gara per l'erogazione dei servizi di sicurezza informatica specialistici. Restano ferme eventuali diverse determinazioni che potranno essere assunte dalla Stazione appaltante in fase di indizione della suddetta gara.

11. Domanda:

"Disciplinare di gara

• Par. 4.1 B.1) Certificazioni Professionali – pag. 10

Si chiede di confermare che presentando come offerta migliorativa una figura professionale che possieda: 1 delle certificazioni T1 e 1 delle certificazioni T2 e 1 delle certificazioni T3, sono attribuiti rispettivamente 3-2-1 punti, per un totale di 6 punti. In caso contrario, si chiede di meglio specificare."

Risposta
Sì, si conferma.

12. Domanda:
"Disciplinare di gara
• Par. 7.A.8) Garanzia Provvisoria – pag. 28
Si chiede di sapere, in caso di partecipazione in costituendo RTI, se la garanzia provvisoria dovrà essere firmata da tutti i componenti del costituendo RTI."

Risposta
Come indicato nel Disciplinare di gara, paragrafo 7.8.A), e nello Schema di Garanzia provvisoria allegato allo stesso (All. 11), la garanzia provvisoria dovrà essere sottoscritta dal Garante e corredata di autentica notarile attestante poteri e qualità del firmatario.
Qualora l'offerta sia presentata da un raggruppamento temporaneo di imprese, la garanzia provvisoria dovrà, a pena di esclusione, essere presentata con riferimento al raggruppamento medesimo, facendone espressa menzione e specificando singolarmente la denominazione di tutti i suoi componenti.

13. Domanda:
"Disciplinare di gara
• Par. 7.A.10) Attestazione del versamento di € 140,00 – pag. 30
Si chiede di sapere, in caso di partecipazione in costituendo RTI, se l'attestazione di avvenuto versamento all'ANAC debba essere firmata da tutti i componenti del RTI."

Risposta
Sì. L'attestazione del versamento deve essere scansionata, sottoscritta digitalmente da tutti i componenti del raggruppamento costituendo e caricata sul Portale dall'Operatore economico Capogruppo/Mandataria.

14. Domanda:
"Capitolato Tecnico
• Par. D. Perimetro e caratteristiche di erogazione - pag. 13

14.1 *o Si chiede conferma che la singola attività che verrà commissionata prevede assessment su almeno 1000 IP oppure almeno 10 applicazioni. In caso contrario, si chiede di meglio specificare.*
14.2 *o Si chiede se è possibile specificare il numero massimo di IP o di applicazioni che saranno oggetto di ciascuna attività.*
14.3 *o Si chiede conferma che con la frase "Numero di attività contemporanee almeno pari a 3;" si intende che al massimo potranno essere assegnate contemporaneamente tre attività di assessment, su IP o su applicazioni. In caso contrario, si chiede di meglio specificare."*

Risposta
14.1 Non si conferma. Il valore indicato nel Capitolato Tecnico serve a definire criteri quantitativi di capacità dell'affidatario a poter eseguire attività così dimensionate. Il dimensionamento effettivo dei target (numero IP, numero applicazioni, etc.) variano a seconda del perimetro di interesse.
14.2 Non è possibile definire preventivamente un numero massimo di IP o di applicazioni che potrebbero essere oggetto di assessment. Questo dipenderà dal perimetro di analisi di volta in volta indicato. Come indicato nel paragrafo 13 del Capitolato Tecnico è in ogni caso richiesto che l'affidatario sia in grado di operare su attività di Security Assessment che possano impattare contemporaneamente:
- Un numero di IP almeno pari a 1000;
- Numero di applicazioni almeno pari a 10;
- Numero di attività contemporanee almeno pari a 3;

14.3 Non si conferma. Il valore indicato serve a determinare quantitativamente la capacità di operare da parte dell'affidatario, che in ogni caso deve essere in grado di operare almeno, non al massimo, sul perimetro dimensionale indicato e contemporaneamente su IP e applicazioni.

15. Domanda:
"Certificazione ISO 27001: è obbligatorio presentare un certificato ISO 27001 o è sufficiente attenersi allo standard?"

Risposta
Si conferma che l'affidatario dovrà attenersi agli standard indicati nel Capitolato Tecnico par. D, tra cui la ISO 27001 e possederne la relativa certificazione.

16. Domanda:

"Fatturato: è possibile la partecipazione alla gara per le società che, pur avendo un fatturato, non hanno ancora presentato un bilancio in quanto costituite all'inizio del 2021?"

Risposta

Quanto alle modalità di dimostrazione del requisito in esame si rimanda a quanto previsto dal d.lgs. 50/2016, con particolare riferimento all'art. 86, comma 4.

17. Domanda:

"Documento All. 6_Schema di Accordo Quadro
Pagina 53
Paragrafo ARTICOLO 37
In riferimento all'articolo 37 dello Schema di Accordo Quadro, si chiede di avere visibilità "dell'Allegato 9 Accordo di Data Protection" citato al suddetto articolo ma non presente all'interno della lista di documenti pubblicati sul portale dedicato al presente bando gara."

Risposta

Si allegano al presente documento i seguenti Accordi di Data Protection:

- *All. 1: Accordo di Data Protection*, che verrà sottoscritto al momento della formalizzazione dell'Accordo Quadro per le società Ferservizi SpA, Ferrovie dello Stato Italiane SpA, FS Sistemi Urbani Srl, Busitalia Sita Nord Srl, Busitalia Veneto SpA;
- *All. 2: Accordo di Data Protection_altre società*, che verrà sottoscritto dalle società diverse da quelle di cui sopra al momento dell'eventuale emissione degli ordini applicativi.

Entrambi i suddetti documenti sono da riferirsi allo schema menzionato all'interno dello Schema di Accordo Quadro, art. 37.

18. Domanda:

"Documento ALL.5 Capitolato Tecnico
Pagina 13
Paragrafo C.3
In riferimento al paragrafo C.3 del Capitolato Tecnico dei Servizi, si chiede di confermare che le certificazioni professionali inerenti il penetration test ed ethical hacking, possedute dal Senior Penetration Tester e dal Junior Penetration Tester, debbano essere una tra quelle indicate per le figure T1, T2, T3 riportare a pag. 13 della tabella "Certificazioni Professionali (CP)" del Disciplinare di gara. Es. se la figura professionale sarà un Senior Penetration tester di tipo T3, dovrà possesere esclusivamente una delle seguenti certificazioni: CISM, OWSE, CSSLP (e non tutte quelle elencate nel suddetto paragrafo C.3)."

Risposta

Si precisa che le macro-tipologie (T1, T2 e T3) afferiscono alle certificazioni che possono essere possedute dalle figure professionali, quali elementi migliorativi (e quindi attributivi di punteggio) indicati nel Disciplinare di gara, E NON afferiscono invece a diverse tipologie di figure professionali.

Per concorrere all'attribuzione del punteggio migliorativo, l'operatore economico potrà offrire figure di Senior Penetration Tester e di Junior Penetration Tester in possesso di almeno una delle certificazioni indicate nel paragrafo 4.1 B.1) del Disciplinare di gara per ciascuna macro-tipologia. Il possesso di almeno una certificazione garantirà l'assegnazione del punteggio previsto per la macro-tipologia nella quale la certificazione è ricompresa.

19. Domanda:

"Documento eGPA_01.2022_DISCIPLINARE

Pagina 46

Paragrafo 13. SUBAPPALTO

Si chiede di confermare che, per lo svolgimento delle attività oggetto dell'Accordo Quadro, sia possibile ricorrere ai contratti continuativi di cooperazione, servizio e fornitura previsti dall'art. 105 comma 3 c-bis) e che lo svoglimento di servizi direttamente a favore della Stazione Appaltante da parte di fornitori con i quali sussistono i citati contratti di servizio non configuri una fattispecie di subappalto."

Risposta

No, non si conferma. Il ricorso a contratti continuativi di cooperazione, servizio e fornitura di cui all'art. 105 3 c-bis) è possibile (e non configura subappalto) solo se la prestazione viene resa a favore dell'operatore economico affidatario del contratto d'appalto. Lo svolgimento dei servizi direttamente a favore della Stazione Appaltante, al contrario, fuoriesce dal suddetto ambito e configura, pertanto, subappalto.

20. Domanda:

"Documento eGPA_01.2022_DISCIPLINARE

Pagina 46

Paragrafo 13. SUBAPPALTO

Si chiede di confermare che, in caso di RTI, sia possibile per ciascuna Mandante procedere autonomamente alla stipula degli eventuali contratti di subappalto."

Risposta
Ciascuna mandante potrà provvedere a stipulare autonomamente il contratto di subappalto con l'impresa subappaltatrice a condizione che le prestazioni sub-affidate, nel rispetto delle previsioni dell'art. 105 D.Lgs. n. 50/2016 e della disciplina di gara, rientrino fra le attività di competenza della mandante.

21. Domanda:
"Documento eGPA_01.2022_DI SCIPLINARE
Pagina 46
Paragrafo 13. SUBAPPALTO
Si chiede di confermare che, in caso di ricorso al subappalto, alla luce dell'art. 49 comma 2 L. 108/2021 di conversione del DL 77/2021 sia possibile per l'affidatario subappaltare le prestazioni oggetto dell'Accordo Quadro in misura superiore al 75%."

Risposta
Sì, in quanto alla luce dell'attuale formulazione dell'art. 105 del d.lgs. n. 50/2016, non sussiste alcun limite percentuale massimo alle prestazioni subappaltabili, fermo restando quanto previsto al comma 1 del suddetto articolo ovvero "…*A pena di nullità, fatto salvo quanto previsto dall'articolo 106, comma 1, lettera d), il contratto non può essere ceduto, non può essere affidata a terzi l'integrale esecuzione delle prestazioni o lavorazioni oggetto del contratto di appalto, nonché la prevalente esecuzione delle lavorazioni relative al complesso delle categorie prevalenti e dei contratti ad alta intensità di manodopera….".*

22. Domanda:
"Si chiede se le seguenti certificazioni:
• *eLearnSecurity Certified Professional Penetration Tester (eCPPT)*
• *eLearnSecurity Certified Professional Penetration Tester (eCPTX)*
• *eLearnSecurity Web application Penetration Tester eXtreme (eWPTX)*
• *eLearnSecurity Junior Penetration Tester (eJPT)*
• *eLearnSecurity Certified eXploit Developer (eCXD)*
• *eLearnSecurity Mobile Application Penetration Tester (eMAPT)*
• *eLearnSecurity Web application Penetration Tester (eWPT)*
• *EC-Council Certified Application Security Engineer (CASE)*
• *ISACA Certified Information System Auditor (CISA)*
possono essere considerate equiparabili a quelle elencate a pag. 11 del Disciplinare di Gara e, in caso positivo ai fini del punteggio, in quali categorie rientrerebbero (T1, T2 o T3)."

Risposta
Le certificazioni che saranno prese in considerazione sono quelle elencate nel Disciplinare di Gara. Potranno essere prese in considerazione altre certificazioni, oltre a quelle elencate, esclusivamente se queste hanno come propedeuticità, certificata e riscontrata dall'ente certificatore, una di quelle elencate nel Disciplinare. In questo caso il valore del punteggio assegnato sarà relativo alla certificazione elencata propedeutica, si veda risposta ai quesiti 8.1 e 8.2.

23. Domanda:
"La certificazione OWSE citata nelle categorie T2 e T3 del Disciplinare di Gara (Tabella pag. 11) ha doppia valenza e quindi fornisce un punteggio di 3 punti o può essere spesa in una sola delle due categorie?"

Risposta
Si tratta di un refuso. Si precisa che la certificazione OWSE è da considerare valida per la sola categoria T2. A tal riguardo si è provveduto ad allineare in tal senso la Busta tecnica prevista sul Portale, eliminando la certificazione OWSE dalla categoria T3.

24. Domanda:
"In relazione al requisito di capacità economica e finanziaria, riferimento punto III.1.2 del Bando di Gara, si chiede di confermare che i livelli minimi di capacità richiesti si riferiscano a "servizi professionali volti ad analizzare la sicurezza informatica dei sistemi informativi", da considerarsi non limitatamente alle Società del Gruppo Ferrovie dello Stato Italiane."

Risposta
Sì, si conferma.

25. Domanda:
"In riferimento all'elenco delle certificazioni indicato nel Disciplinare di Gara, considerando che l'elenco PEN-200, PEN-210, PEN-300, WEB-200, WEB-300, EXP-301, EXP-401 identifica dei corsi e non delle certificazioni, si chiede la modalità di dimostrazione alla relativa partecipazione. In alternativa se tali requisiti devono essere esclusi e considerate le sole effettive certificazioni presenti nella Tabella di pag. 11 del Disciplinare di Gara."

Risposta
Ai fini della comprova in capo all'aggiudicatario di quanto dichiarato ai fini dell'attribuzione del punteggio verrà richiesta la certificazione degli esami previsti a valle dei corsi (non è sufficiente presentare l'attestato di partecipazione al singolo corso).

26. Domanda:
"Si chiede di specificare cosa si intende per "Piano di evoluzione del servizio e delle tecnologie" indicato al paragrafo 4.1. A) Progetto Tecnico del Disciplinare di Gara (pag. 7)."

Risposta
Con *"Piano di evoluzione del servizio e delle tecnologie"* l'affidatario deve illustrare come intende evolvere il servizio e le tecnologie impiegate, al fine di seguire le evoluzioni delle tecniche di assessment, delle vulnerabilità, delle minacce e tutto ciò che possa variare nel tempo ed impattare il modello di erogazione del servizio definito in fase di aggiudicazione.

27. Domanda:
"Documento eGPA_01.2022_DISCIPLINARE
Pagina 21
Paragrafo 7.a
Nel disciplinare è riportato che per inserire la propria documentazione amministrativa è richiesta la compilazione dei campi a video nella area "Risposta Amministrativa". In tale sezione è però presente in alto a sinistra un questionario on line su file excell (come da word allegato). Oltre alla suddetta compilazione nell'area richiesta è necessario anche provvedere alla compilazione di questo questionario excell? Tale questionario deve essere firmato digitalmente?"

Risposta
La modalità di presentazione dell'offerta, ivi inclusa la Busta Amministrativa, è quella indicata nel Disciplinare di gara, paragrafi 7 e 8, ovvero il concorrente dovrà compilare i campi a video presenti all'interno delle buste on-line (Amministrativa, Economica e Tecnica) e ad allegare i documenti richiesti.
Una volta espletate tali attività il Concorrente, per trasmettere la propria offerta telematica, dovrà:

- cliccare su "Trasmetti risposta";
- scaricare i file pdf autogenerati dal sistema e contenenti:
    - la dichiarazione formulata a video nella Busta Amministrativa;
    - la dichiarazione formulata a video di Offerta Tecnica;

- la dichiarazione formulata a video di Offerta Economica.

Firmare digitalmente tali file pdf e allegarli sul Portale secondo le istruzioni visualizzate a video.

- cliccare su "OK" per confermare la trasmissione.

Pertanto non è necessario scaricare e compilare il menzionato questionario in excel.

28. Domanda:

"Che tipo di inquadramento possono avere le figure professionali richieste? E' consentito proporre figure professionali con collaborazione coordinata e continuativa?"

Risposta

Non è richiesto alcuno specifico inquadramento/tipologia contrattuale per le figure professionali richieste rientrando tali aspetti nell'organizzazione del concorrente, purchè lo stesso ne possa disporre, a qualsiasi titolo, per tutta la durata dell'appalto.

29. Domanda:

"Documento Disciplinare eGPA_01.2022_DISCIPLINARE pag. 46 par.13 Subappalto: si prega di chiarire quali sono i limiti ammessi per il subappalto"

Risposta

Si rinvia alla disciplina del subappalto, regolata dall'art. 105 del d.lgs. n. 50/2016, attualmente vigente, precisando che, fermo restando quanto previsto al comma 1 del predetto articolo, non sono previsti limiti percentuali massimi.

30. Domanda:

"Disciplinare eGPA_01.2022_DISCIPLINARE par. 7.A.7) Documentazione necessaria per effettuare gli accertamenti ai fini ANTIMAFIA (All.ti 12.1, 12.2 e 12.3)- si prega di confermare se è possibile utilizzare un proprio formato per l'allegato 12.2."

Risposta

Sì, purché tale formato sia completo di tutte le informazioni richieste negli atti di gara e reso in conformità all'All. 12.2 del Disciplinare.

31. Domanda:

"Documento: Disciplinare di Gara – Paragrafo 13. Subappalto

Domanda: Si chiede di confermare se un Operatore Economico possa utilizzare, per la esecuzione di tutte o parte delle prestazioni contrattuali, una società dalla stessa controllata, soggetta all'esercizio dell'attività di direzione e coordinamento da parte del predetto Operatore Economico (attività che si estrinseca nell'impartire direttive e nell'applicare apposite procedure di Gruppo dirette a indirizzarne la gestione e a garantirne il controllo), fermi restando il possesso in capo alla suddetta società dei requisiti di ordine generale e la permanenza in capo al predetto Operatore Economico della titolarità del rapporto contrattuale nonché della integrale responsabilità per la regolare esecuzione delle prestazioni subaffidate. Si chiede, quindi, di confermare che, al ricorrere delle anzidette condizioni, non essendo configurabile nessuna alterità sostanziale tra il del predetto Operatore Economico e la società controllata, l'affidamento a quest'ultima delle prestazioni non è configurabile come subappalto di cui all'art. 105 del D.lvo n. 50/2016 e s.m.i.."

Risposta

No, non si conferma. L'affidamento delle prestazioni ad una società soggetta al controllo dell'Appaltatore principale, così come ipotizzato nella domanda, è configurabile come subappalto e pertanto soggetto alla relativa disciplina.

32. Domanda:

"Documento: Disciplinare di Gara – Paragrafo 13. Subappalto
Domanda: Atteso che la Corte di Giustizia UE nella pronuncia del 26/09/2019, in causa C-63/18, ha ritenuto incompatibili con il diritto comunitario i limiti al subappalto stabilito al comma 2 dell'art. 105 del D.Lgs. n. 50/2016 e s.m.i., si chiede conferma a codesta spettabile Amministrazione della non applicabilità di un limite percentuale quantitativo al subappalto, vista anche la modifica in merito introdotta nel Codice dei Contratti Pubblici con la nuova disciplina prevista dalla Legge n. 108 del 29 Luglio 2021 (che ha convertito il precedente Decreto-Legge 31 maggio 2021, n. 77 (cosiddetto "Semplificazioni-bis") recante "Governance del Piano nazionale di rilancio e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure"."

Risposta

Si conferma che alla luce dell'attuale formulazione dell'art. 105 del d.lgs. n. 50/2016, fermo restando quanto previsto al comma 1 del predetto articolo, non sono previsti limiti percentuali massimi.

33. Domanda:

33.1 *"I report devono essere prodotti esclusivamente in lingua italiana o possono essere alternativamente prodotti anche in lingua inglese?*
33.2 *È possibile avvalersi di personale non madrelingua italiana?"*

Risposta

33.1 Si fa presente che l'operatore economico dovrà garantire la disponibilità a produrre report sia in italiano che in inglese, a seconda della specifica esigenza di volta in volta manifestata dalla società richiedente.

33.2 Sì, purché il personale sia in grado di interloquire in lingua italiana sia in forma scritta che in forma orale.

34. Domanda:

"Documento All. 5_Capitolato Tecnico.pdf

§§ C. Modalità di erogazione del servizio.

***34.1** È possibile disporre di una stima percentuale, anche indicativa, delle attività che si ritiene dovranno essere effettuate: a) onsite, nonché b) "in orari notturni e/o extra lavorativi, oppure nei giorni festivi"?*

***34.2** È lecito ritenere che, anche in virtù della: a) possibilità tecnica di condurre attività su perimetri interni operando da remoto previa predisposizione di opportuna connettività, e b) organizzazione delle attività in modo da non causare disservizi, le attività che ricadranno in a) e/o b) avranno carattere minoritario?"*

Risposta

34.1 Si vedano le risposte ai quesiti nn. 4 e 5.

34.2 Non è possibile stabilire ad oggi quante potranno essere le attività che potranno essere condotte da remoto. A titolo esemplificativo e non esaustivo si riporta che nell'ultimo triennio la prevalenza delle attività è stata condotta on site.

35. Domanda:

"Il Documento All. 5_Capitolato Tecnico.pdf specifica, per i profili Senior e Junior Penetration Tester, rispettivamente "almeno 4 anni di esperienza" e "almeno 2 anni di esperienza".

Il Doc. eGPA_01.2022_DISCIPLINARE.pdf riporta invece, nella Tabella Seniority, esperienze rispettivamente superiori a 6 anni (Senior) e 4 anni (Junior), ed esperienze superiori a 6 anni riportate sia per Senior che per Junior.

Come sono da interpretare queste difformità?"

Risposta

Non si ravvisano difformità.

Nel Capitolato Tecnico sono disciplinati i requisiti minimi espressi in termini di Seniority, ovvero gli anni di esperienza minima richiesti in capo a ciascuna figura professionale.

Nel Disciplinare, al paragrafo 4.1 B.2), sono invece indicati gli anni di Seniority che concorrono all'attribuzione del punteggio tecnico per elementi dell'offerta migliorativi rispetto al requisito minimo richiesto per ciascuna figura professionale.

36. Domanda:

"Documento All. 5_Capitolato Tecnico.pdf
§ D. Perimetro e Caratteristiche di erogazione
Si conferma che il senso del paragrafo seguente è che possono essere ordinate contemporaneamente fino a tre attività di complessità simile a 1000 indirizzi IP, 10 applicazioni?
L'Affidatario deve essere in grado di operare su attività di Security Assessment che impattano contemporaneamente:
o Un numero di IP almeno pari a 1000;
o Numero di applicazioni almeno pari a 10;
o Numero di attività contemporanee almeno pari a 3;"

Risposta

Si specifica che il senso del paragrafo è che il cliente deve essere dimensionato in modo tale da poter effettuare almeno 3 attività di assessment contemporanee su un numero di indirizzi IP pari almeno a 1000 e numero di applicazioni pari almeno a 10 per ogni attività.

37. Domanda:

"la pagina "https://www.ariba.com/suppliers/ariba-networkfulfillment/pricing" da come risultato "page not found".
Potreste fornirci qualche indicazione in merito al flusso / utilizzo / costi?
Nello specifico cosa verrà veicolato su questo sistema di e-Procurement? A cosa serve il catalogo elettronico?"

Risposta

Si rappresenta che è possibile accedere alla Piattaforma di e-Requisitioning di Ariba Network (AN) tramite l'indirizzo corretto di seguito indicato: http://www.ariba.com/suppliers/ariba-network-fulfillment/pricing.
All'interno della pagina raggiungibile con il suddetto link è possibile reperire le informazioni richieste, ivi compresi i relativi costi e condizioni di utilizzo.
Ulteriori informazioni non sono nella disponibilità di questa Stazione appaltante, in quanto la sottoscrizione da parte dell'aggiudicatario dell'abbonamento per l'utilizzo della suddetta Piattaforma avviene direttamente con il fornitore della stessa.

Come indicato nel Disciplinare di gara e nello Schema di Accordo Quadro ad esso allegato, questa Stazione appaltante si avvale della Piattaforma per la gestione delle transazioni con i clienti, dei cataloghi on line, dei prodotti, degli ordini di acquisto.

38. Domanda:

"In riferimento al paragrafo - 15.2 Trattamento dei dati personali per le attività previste dal Contratto del Disciplinare si richiede copia dell'accordo di data protection che sarà allegato al contratto e che costituisce parte integrante dello stesso"

Risposta

Si allegano al presente documento i due Accordi di Data Protection, in merito ai quali si veda la risposta alla domanda n. 17.

39. Domanda:

"Si chiede di specificare quale sia la tipologia di sistemi che saranno oggetto di valutazione di sicurezza (VA/PT), al fine di determinare in maniera più accurata le professionalità richieste allo svolgimento delle attività."

Risposta

L'aggiudicatario dovrà essere in grado di erogare in proprio servizi su tutto il perimetro tecnologico del Gruppo FS Italiane che prevede sia soluzioni e infrastrutture proprie IT di mercato che custom, che sistemi industriali ICS/SCADA propri del settore ferroviario.

40. Domanda:

"In riferimento al par. C.1. "Vulnerability Assessment, Penetration Test" del capitolato di gara si chiede di confermare che la produzione di log prodotti da proxy applicativi e/o strumenti di scan siano sufficienti a soddisfare la richiesta di tracciamento di tutte le attività svolte per ogni VA/PT."

Risposta

In generale è richiesto che l'aggiudicatario sia sempre in grado di dare evidenza delle attività svolte durante gli assessment con un livello di verbosità adeguato ad attestare la corretta effettuazione e riconducibilità delle attività per consentire una ricostruzione della sequenza e/o modifica di eventi che possono aiutare a distinguere eventuali violazioni della sicurezza.

41. Domanda:

"In riferimento al par. C.2.1. "Fasi delle attività di Remediation Plan (Piano di Rientro)" si chiede di confermare che l'attività in carico all'Affidatario sia unicamente la gestione, a supporto del Gruppo FS Italiane, del piano di rientro proposto dal fornitore dell'applicazione/sistema vulnerabile."

Risposta

Al fornitore è richiesta la redazione e la gestione dei piani di rientro (remediation plan) e la verifica continuativa, durante l'implementazione delle remediation da parte dei soggetti tecnici incaricati, che le soluzioni indicate nel piano siano applicabili al contesto anche, ove necessario, attraverso l'indicazione di ulteriori azioni di rientro emerse in corso d'opera.

42. Domanda:

"In merito alle sedi di erogazione è possibile avere indicazioni sulle sedi principali in cui si prevede l'erogazione di attività in loco?"

Risposta

Si veda la risposta al quesito n. 4.

43. Domanda:

"In caso di erogazione dei servizi in loco presso sedi del gruppo FSI che comportano delle spese di trasferta, queste come saranno gestite? Preventivate contestualmente alla proposta di progetto e rimborsate previa approvazione?"

Risposta

I costi delle trasferte sono a carico dell'aggiudicatario e non saranno riconosciute a parte rispetto all'Ordine applicativo che viene emesso per l'esecuzione delle attività

Le tariffe giornaliere offerte dall'operatore economico si intendono comprensive e compensative di ogni eventuale onere, diretto ed indiretto, nessuno eccettuato, che l'operatore economico dovrà sostenere per eseguire tutte le attività, per osservare tutte le prescrizioni esecutive dell'affidamento, nonché per assolvere a tutti gli adempimenti ed obblighi assunti dallo stesso, ivi compresi eventuali oneri dovuti a trasferte.

44. Domanda:

"si chiede conferma che la risposta di offerta economica consiste nello specificare unicamente due tariffe giornaliere per Senior e Junior consultant, rispettivamente, come sconto applicato alla tariffa base d'asta"

Risposta
Sì, si conferma.
L'operatore economico deve offrire due sconti percentuali, rispettivamente: uno sconto percentuale sulla tariffa giornaliera a base di gara per la figura Senior Penetration Tester; uno sconto percentuale sulla tariffa giornaliera a base di gara per la figura Junior Penetration Tester.

45. Domanda:
"nell'allegato 5 (capitolato tecnico) si fa riferimento al paragrafo C.4 che però non fa parte del documento. Si chiede se si tratta di un refuso e conferma che il paragrafo corretto sia C.3, o se invece manca un paragrafo."

Risposta
Si conferma che trattasi di un refuso. Il riferimento corretto è al paragrafo C.3 del Capitolato Tecnico.

46. Domanda:
"Al paragrafo D del capitolato tecnico (allegato 5) si menziona la presenza di applicazioni in perimetro. Si tratta di applicazioni web, mobile, o native? Applicazioni commerciali o custom?"

Risposta
Si veda risposta al quesito n. 39.

47. Domanda:
47.1*"Si richiede avere una stima del volume complessivo di giornate per figura professionale, effettivamente erogate nell'ultimo anno di servizio.*
47.2 *Si richiede di specificare la percentuale di tempo in cui le risorse saranno impiegate on-site su sedi diverse da Roma e provincia"*

Risposta
47.1 Si evidenzia che nell'ultimo anno di servizio sono state erogate circa 3600 gg/u complessivi di cui mediamente circa il 55% Senior e 45% Junior.
47.2 Si rinvia alla risposta fornita al quesito n. 4.

48. Domanda:

"Si chiede di confermare che la comprova del possesso del requisito relativo alla capacità economico-finanziaria di cui al punto III 1.2 lett. a) del Bando di gara possa essere fornita attraverso la copia conforme all'originale dei Certificati rilasciati da committenti pubblici-privati e contratti e/o fatture;"

Risposta

Ai fini della comprova del requisito di capacità economico-finanziaria, trova applicazione l'art. 86 comma 4 del d.l.gs n.50/2016 e ss. mm. e ii. e il richiamato All. XVII: pertanto l'operatore potrà assolvere all'onere di comprova del requisito del fatturato specifico, mediante presentazione dei bilanci o di estratti di bilancio, qualora la pubblicazione del bilancio sia obbligatoria in base alla legislazione del paese di stabilimento dell'operatore economico; una dichiarazione concernente il fatturato globale e, se del caso, il fatturato del settore di attività oggetto dell'appalto, al massimo per gli ultimi tre esercizi disponibili in base alla data di costituzione o all'avvio delle attività dell'operatore economico, nella misura in cui le informazioni su tali fatturati siano disponibili.

Si rammenta che ai sensi del secondo periodo dell'art. 86 comma 4 del CCP *"L'operatore economico, che per fondati motivi non è in grado di presentare le referenze chieste dall'amministrazione aggiudicatrice, può provare la propria capacità economica e finanziaria mediante un qualsiasi altro documento considerato idoneo dalla stazione appaltante"*.

Alla luce di quanto sopra è possibile produrre copia conforme all'originale dei Certificati rilasciati da committenti pubblici-privati e contratti (da cui sia possibile evincere l'oggetto, l'importo e periodo di esecuzione) e/o fatture quietanzate, da cui sia possibile evincere il fatturato specifico richiesto nel bando di gara.

49. Domanda:

"Si chiede di confermare che il valore del fatturato specifico annuo almeno pari ad un milione, sia da ritenersi come il fatturato complessivo da considerare negli ultimi 3 esercizi finanziari approvati e non il valore medio annuo dei singoli esercizi;"

Risposta

No, non si conferma. Come esplicitato nel punto III.1.2) del Bando di gara, ai fini della partecipazione è richiesto che l'operatore economico abbia realizzato negli ultimi 3 esercizi finanziari (da bilancio approvato alla data di pubblicazione del bando di gara), un fatturato specifico **medio annuo** relativo ai servizi oggetto dell'appalto per un valore almeno pari a 1.000.000,00 EUR (euro unmilione/00), IVA esclusa.

50. Domanda:

"Per le Risorse professionali che contribuiscono all'assegnazione del punteggio tecnico e per le quali si dovranno descrivere le esperienze pregresse ovvero possesso delle certificazioni, si chiede di voler chiarire e/o precisare se possano essere anche esterni al concorrente: possibilità quindi di proporre nella Offerta Tecnica risorse appartenenti a società subappaltatrici;"

Risposta

Sì, si conferma.

51. Domanda:

"Chiediamo di prendere visione del Data Processing Agreement, essendo espressamente previsto dalle previsioni contrattuali che la società appaltatrice tratterà dati personali di titolarità della committente;"

Risposta

Si allegano al presente documento i due Accordi di Data Protection indicati negli atti di gara, in merito ai quali si veda la risposta alla domanda n. 17.

52. Domanda:

"Con riferimento alle condizioni generali di contratto, chiediamo la possibilità di limitare la responsabilità della società appaltatrice, per eventuali danni cagionati nel corso dello svolgimento dei servizi, salvo il caso di dolo o colpa grave;"

Risposta

No, non è possibile derogare alle previsioni contenute nelle Condizioni Generali di Contratto per gli appalti di forniture delle Società del Gruppo Ferrovie dello Stato Italiane, applicabili, in quanto compatibili, agli appalti di servizi limitatamente alle disposizioni indicate negli atti di gara.

53. Domanda:

"Con riferimento alle condizioni generali di contratto, chiediamo la possibilità di inserire per tutelare le nostre informazioni riservate, la reciprocità dell'obbligo di riservatezza con durata predefinita;"

Risposta

No, si veda risposta alla domanda n. 52.

54. Domanda:

"Chiediamo, limitatamente alle previsioni di cui all'art. 61.1 delle condizioni generali di contratto, che sia prevista la possibilità per la stazione appaltante di risolvere il rapporto contrattuale in caso di mancata esecuzione, da parte del Fornitore, di tutto o di parte della prestazione affidata entro il termine o i termini (anche parziali o intermedi) previsti in contratto, salvo il caso in cui tale ritardo sia dipeso da cause non imputabili all'appaltatore;"

Risposta

No, si veda risposta alla domanda n. 52.

55. Domanda:

"Sempre in relazione all'art. 61.1 delle condizioni generali di contratto, chiediamo che sia prevista la possibilità per la stazione appaltante di risolvere il rapporto contrattuale in caso di ritardo nell'avvio delle prestazioni rispetto al termine stabilito dal contratto, salvo il caso in cui tale ritardo sia dipeso da cause non imputabili all'appaltatore."

Risposta

No, si veda risposta alla domanda n. 52.

****

RETTIFICA AL BANDO DI GARA

Contestualmente alla pubblicazione delle risposte alle richieste di chiarimento di cui sopra, viene disposta la seguente rettifica al bando di gara relativa alla sezione III.1.8):

"Numero della sezione: III.1.8
Punto in cui si trova il testo da modificare: Forma giuridica che dovrà assumere il raggruppamento di operatori economici aggiudicatario dell'appalto:
anziché:
È consentita la partecipazione alla gara ai soggetti di cui agli artt. 45 e ss. D.Lgs. n. 50/2016 in forma singola o associata.
leggi:
È consentita la partecipazione alla gara ai soggetti di cui agli artt. 45 e ss. D.Lgs. n. 50/2016 in forma singola o associata.
Non potranno invece partecipare alla presente procedura - né individualmente né in forma associata -, pena l'esclusione dalla gara, l'aggiudicatario o un suo subappaltatore della procedura di gara eGPA AGA 15/2021 – Gara 5 "Affidamento dei servizi ICT di gestione sistemistica e delle infrastrutture hardware,

hosting, housing, IaaS erogati tramite Data Center che svolgono funzione di Data Center Primario con certificazione ANSI TIA-942 Rating IV da parte di enti certificatori autorizzati o Tier IV Constructed da parte di Uptime Institute e Data Center Secondari con certificazione ANSI TIA-942 Rating III o successivo o Uptime Institute Tier III Constructed o successivo e fornitura di servizi di connettività e apparati di rete TLC", nonché, le società che si trovino in una situazione di controllo o collegamento con i predetti operatori economici. Tali soggetti non potranno nemmeno assumere il ruolo di subappaltatore."

***

PROROGA DEI TERMINI e COMUNICAZIONE VARIAZIONE NUMERO DI ASSISTENZA DEL PORTALE ACQUISTI

Si precisa che in data 02.03.2022 è stata disposta la proroga dei termini fissati negli atti di gara. Gli stessi sono stati rideterminati come di seguito riportati:

- Scadenza presentazione delle offerte: 17 marzo 2022, ore 13:00.
- Data per la ricognizione delle offerte: 18 marzo 2022, ore 10:00.

Pertanto le richieste di accredito per la partecipazione alla seduta pubblica dovranno pervenire con le modalità indicate nel disciplinare di gara entro le ore 15:00 del 17 marzo 2022.

Contestualmente a quanto sopra si è provveduto a modificare il termine per la presentazione delle offerte indicato sul Portale Acquisti di Ferservizi SpA.

Si comunica, inoltre, che il Servizio Assistenza del Portale Acquisti ha modificato il numero dedicato, rispetto a quello indicato sugli atti di gara (par. 6 del Disciplinare di gara e sez. VI.3 n. 1) del Bando di gara). Il nuovo numero dedicato è il seguente: +39 02 00 70 42 52.

Claudia Gasbarri

CLAUDIA GASBARRI

Firmato digitalmente da CLAUDIA GASBARRI
Data: 2022.03.04 13:36:01 +01'00'

Allegato n. 1

Servizi professionali volti ad analizzare la sicurezza informatica dei sistemi informativi delle Società del Gruppo Ferrovie dello Stato Italiane

Accordo di Data Protection

Titolare – Responsabile

INDICE

Articolo 1: Premesse e Allegati 5
Articolo 2: Oggetto dell'Accordo 5
Articolo 3: Definizioni 5
Articolo 4: Ambito di competenza 6
Articolo 5: Ambito del trattamento 6
Articolo 6: Obblighi del Titolare 6
Articolo 7: Obblighi Responsabile 6
7.1 RISPETTO DELLE ISTRUZIONI DEL TITOLARE 6
7.2 CONFORMITÀ ALLA NORMATIVA DP 7
7.3 AMMINISTRATORI DI SISTEMA 7
7.4 MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE 7
7.5 PRONTA NOTIFICA 8
7.6 RISPOSTA AI QUESITI 8
7.7 INFORMAZIONI PER DIMOSTRAZIONE CONFORMITÀ 8
7.8 COOPERAZIONE CON TITOLARE PER AUTORITÀ DI SUPERVISIONE 8
7.9 CONSENSO PREVENTIVO SUB-RESPONSABILE 8
7.10 ACCORDO DATA PROTECTION (ADP) 8
Articolo 8: Riservatezza 8
Articolo 9: Sicurezza trattamento 8
Articolo 10: Nomina sub-Responsabile 9
Articolo 11: Diritti degli Interessati 9
Articolo 12: Richieste degli Interessati 9
Articolo 13: Supporto al Titolare 10
Articolo 14: Persone autorizzate al trattamento 10
Articolo 15: Comunicazione di dati 10
Articolo 16: Trasferimenti a paesi terzi 10
Articolo 17: Trattamento economico-esclusione 11
Articolo 18: Responsabilità 11
Articolo 19: Cessazione 11
Articolo 20: Obblighi dopo cessazione 11
Articolo 21: Legge applicabile 11
Articolo 22: Tribunale competente 11
Articolo 23: Intero accordo 12

Articolo 24: Annullamento **12**

Articolo 25: Variazioni del presente ADP **12**

Allegato A – Istruzioni sulle attività di Trattamento oggetto del presente ADP **14**

Allegato B – Misure tecniche e organizzative di sicurezza specificate **17**

Allegato B.1 – Misure di sicurezza specificate per le Postazioni di Lavoro mediante le quali è effettuato il trattamento di dati personali 17

Allegato B.2 – Misure di sicurezza specificate per eventuali strumenti mobile mediante le quali è effettuato il trattamento di dati personali 20

Allegato B.3 – Misure di sicurezza specificate sui dati personali trattati 20

Allegato C – [da mantenere se ci sono sub-responsabili individuati] Elenco sub-responsabili **21**

Accordo di Data Protection

TRA

Ferservizi S.p.A., Società con Socio Unico, soggetta alla direzione e coordinamento di Ferrovie dello Stato Italiane S.p.A., con sede legale in Roma, Piazza della Croce Rossa n° 1, Codice Fiscale e Partita IVA n. 04207001001, **in proprio e in nome e per conto delle Società del Gruppo Ferrovie dello Stato Italiane**[1], in persona di [x], in qualità di [x], munito dei necessari poteri per la sottoscrizione del presente Accordo di Data Protection (di seguito "Titolare" e "Titolari")

E

[FORNITORE], con sede in ..., iscritta al registro delle imprese di ..., codice fiscale e partita IVA ..., in persona di ..., in qualità di ...munito dei necessari poteri per la sottoscrizione del presente Accordo di Data Protection, (di seguito "Responsabile").

Titolare e Responsabile verranno in seguito entrambi indicati come "la Parte" o congiuntamente "le Parti".

PREMESSE

Normativa Data Protection (Normativa DP)

L' art. 28 del Regolamento (UE) 2016/679 ("GDPR" o "Normativa DP") stabilisce che quando il trattamento deve essere effettuato per conto di un titolare, il trattamento da parte del soggetto terzo nominato responsabile del trattamento è disciplinato da un contratto che è vincolante per il responsabile nei confronti del titolare e che definisce l'oggetto e la durata del trattamento, la natura e lo scopo, il tipo di dati personali e le categorie di interessati trattati, gli obblighi e i diritti del titolare.

Contratto

Il Responsabile fornirà servizi al Titolare in relazione all'analisi di sicurezza informatica dei sistemi informativi delle Società del Gruppo Ferrovie dello Stato Italiane ("Servizi"), come specificato nel contratto sottoscritto dalle parti ("Contratto").

Servizi

Nel contesto dei Servizi, i Titolari trasferiranno al Responsabile alcuni dati personali e il Responsabile elaborerà e utilizzerà tali dati personali per conto dei Titolari nel rispetto della Normativa DP e in conformità al presente accordo sul trattamento dei dati (di seguito "ADP").

Competenza del Responsabile

Il Responsabile fornisce garanzie sufficienti, in particolare in termini di conoscenze specialistiche, affidabilità e risorse, per attuare misure tecniche e organizzative che soddisfino i requisiti della Normativa DP, compresa la sicurezza del trattamento per garantire la riservatezza e la protezione dei diritti degli interessati.

Affidamento dati

[1] Ferrovie dello Stato Italiane SpA, FS Sistemi Urbani Srl, Busitalia Sita Nord Srl, Busitalia Veneto SpA

I Titolari affidano al Responsabile le attività di trattamento di dati personali come dettagliato nell'Allegato A (Istruzioni) e Allegato B (Misure di Sicurezza tecnico-organizzative) e il Responsabile si impegna ad eseguire il trattamento per conto del Titolare.

Titolare/i

Le Società del Gruppo FS Italiane, determinando le finalità e i mezzi del trattamento dei dati personali per l'esecuzione dei Servizi sono qualificate come "Titolari", in base alla Normativa DP.

Ruolo di Ferrovie dello Stato Italiane SpA

Alcune Società del Gruppo FS Italiane, in qualità di Titolari del trattamento, hanno sottoscritto con Ferrovie dello Stato Italiane SpA (FS) un *service* avente ad oggetto la fornitura di servizi di *cybersecurity*. Tali servizi determinano un trattamento di dati personali e, in ottemperanza all'Art. 28 del Regolamento (UE) 2016/679 le Società hanno sottoscritto un Accordo di *Data Protection*, nell'ambito del quale FS si configura come Responsabile del Trattamento.

Si specifica, pertanto, che i servizi attivati da FS nell'ambito del Contratto di cui questo ADP è parte integrante, potranno essere svolti in virtù del *service* predetto. In tali casi, **FS sarà qualificata come Responsabile del trattamento e [FORNITORE] come sub-responsabile o altro responsabile**.

Resta inteso che:

- FS è autorizzata ad avvalersi di [FORNITORE] per le operazioni di trattamento, in virtù dell'Accordo di *Data Protection* sottoscritto tra le Società del Gruppo FS Italiane e FS;
- mediante il presente atto, sono imposti a [FORNITORE] gli stessi obblighi in materia di protezione dei dati contenuti nell'Accordo di Data Protection sottoscritto tra le Società del Gruppo FS Italiane e FS;
- ai sensi dell'Art. 28, Par. 4, per i servizi attivati da FS in qualità di Responsabile del trattamento, nel caso in cui [FORNITORE] ometta di adempiere ai propri obblighi in materia di protezione dei dati, FS conserva nei confronti dei Titolari la responsabilità di adempimento degli obblighi di [FORNITORE].

Contrattualizzazione

Le Parti intendono stipulare un accordo contrattuale per le operazioni di trattamento dei dati.

Sulla base degli assunti di cui sopra, le Parti convengono quanto segue.

Articolo 1: Premesse e Allegati

Le premesse e gli allegati sono parti sostanziali di questo ADP.

Articolo 2: Oggetto dell'Accordo

Le Parti con questo ADP intendono disciplinare il trattamento dei dati personali da parte del Responsabile, specificare l'oggetto, la durata, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati e gli obblighi e i diritti delle Parti.

Articolo 3: Definizioni

I termini utilizzati nel presente ADP hanno il seguente significato:

- "dati personali", "categorie speciali di dati personali", "processo/trattamento", "titolare", "responsabile" e "interessato" hanno lo stesso significato utilizzato nel GDPR;

- "sub-responsabile": qualsiasi entità impegnata dal Responsabile che accetti di ricevere dati personali esclusivamente finalizzati alla realizzazione dei Servizi in conformità con le istruzioni del Titolare, i termini dell'ADP e i termini del subappalto;
- "Normativa Data Protection" (Normativa DP): la legislazione che tutela i diritti e le libertà fondamentali delle persone fisiche e, in particolare, il loro diritto alla vita privata in relazione al trattamento dei dati personali, applicabile ad un Titolare nello Stato membro dell'UE in cui questi è stabilito;
- "misure tecniche e organizzative": misure volte a garantire un livello di sicurezza adeguato al rischio, volte a proteggere i dati personali dalla distruzione accidentale o illecita o dalla perdita accidentale, dall'alterazione, dalla divulgazione non autorizzata o dall'accesso non autorizzato ai dati personali trasmessi, archiviati o altrimenti trattati e contro tutte le altre forme illecite di trattamento;
- "violazione dei dati personali" o "data breach": violazione della sicurezza che porta alla distruzione, perdita, alterazione, divulgazione non autorizzata o illegale di dati personali trasmessi, archiviati o altrimenti elaborati.
- "autorità di controllo" è l'autorità pubblica indipendente istituita da uno Stato membro incaricata di sorvegliare l'applicazione della Normativa DP (per l'Italia, il "Garante").

Articolo 4: Ambito di competenza

Tramite questo ADP i Titolari impegnano **[FORNITORE]**, che sottoscrivendo questo accordo lo accetta, come "Responsabile" come definito dalla Normativa DP, per il trattamento dei dati.

Articolo 5: Ambito del trattamento

I dettagli del trattamento dei dati, le istruzioni operative rispetto alle attività di competenza del Responsabile ovvero le categorie di dati personali e di soggetti interessati sono specificati nell'Allegato A.

Articolo 6: Obblighi del Titolare

I Titolari del trattamento garantiscono:

A) Conformità - Che è responsabile per la valutazione dell'ammissibilità del trattamento dei dati e garantisce i diritti degli interessati coinvolti.

B) Sicurezza - Che le misure tecniche e organizzative oggetto del presente accordo assicurano un livello di sicurezza adeguato ai rischi connessi al trattamento dei dati e alla natura dei dati da proteggere;

C) Istruzioni - Che le istruzioni oggetto del presente accordo sono sufficienti a definire lo scopo e la procedura del trattamento dei dati.

Articolo 7: Obblighi Responsabile

Il Responsabile garantisce:

7.1 RISPETTO DELLE ISTRUZIONI DEL TITOLARE

Di trattare i dati personali solo per conto del Titolare, limitati alle sole attività di trattamento strettamente necessarie per l'esecuzione di questo ADP e in conformità con le sue istruzioni documentate e questo ADP; se non è in grado di fornire tale conformità per qualsiasi motivo, accetta di informare

tempestivamente i Titolari della sua impossibilità di adempiere, nel qual caso i Titolari hanno il diritto di sospendere l'elaborazione dei dati e / o risolvere il Contratto e questo ADP.

7.2 CONFORMITÀ ALLA NORMATIVA DP

Che verrà data attuazione alle istruzioni ricevute dal Titolare nel rispetto degli obblighi di cui al Contratto e nel presente ADP. Nell'ipotesi di eventuali modifiche alla normativa vigente che possano incidere sulle obbligazioni assunte, il Responsabile si impegna a darne immediata comunicazione al Titolare, il quale potrà sospendere l'elaborazione dei dati e/o risolvere il Contratto e il presente ADP.

7.3 AMMINISTRATORI DI SISTEMA

Il Responsabile si impegna ad adempiere alle seguenti prescrizioni ai fini della corretta applicazione dei provvedimenti del Garante per la protezione dei dati personali del 27/11/2008 e del 25/6/2009 relativi alla gestione degli amministratori di sistema, nonché agli eventuali successivi provvedimenti o norme in materia.

I soggetti preposti dal Responsabile a svolgere funzioni di amministratori di sistema che godono di profili di accesso superiori a quelli degli utenti ordinari per quanto attiene le banche dati o gli applicativi contenenti i dati degli interessati oggetto delle operazioni di trattamento, devono essere previamente selezionati in base alla valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

La nomina degli amministratori di sistema, deve avvenire per iscritto e con designazione individuale delle persone autorizzate al trattamento e deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Gli estremi identificativi delle persone fisiche amministratori di sistema operanti sui sistemi che ospitano i dati personali, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di richieste da parte del Titolare o accertamenti da parte del Garante.

L'operato degli amministratori di sistema è oggetto, con cadenza almeno annuale, di un'attività di verifica, in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dal Codice Privacy.

Il Responsabile deve provvedere al tracciamento dei log di accesso degli amministratori di sistema, secondo modalità definite in comune accordo con i Titolari.

Entro il 15 gennaio di ogni anno, il Responsabile comunicherà al Titolare con apposito rapporto scritto il soddisfacimento delle prescrizioni di cui ai citati provvedimenti.

7.4 MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

Il Responsabile, prima di eseguire il trattamento dei dati, tenuto conto del rischio per i diritti e le libertà degli interessati coinvolti e gli esiti di eventuali *Data Protection Impact Assessment* svolti dal Titolare, garantisce l'adozione delle misure tecniche e organizzative di sicurezza adeguate al rischio del trattamento.

In particolare, sono specificate le misure di sicurezza tecnico-organizzative di cui all'Allegato B del presente documento.

Nel valutare il livello appropriato di sicurezza, si dovrà prestare particolare attenzione ai rischi di distruzione accidentale o illecita, perdita, alterazione, divulgazione non autorizzata o accesso non autorizzato ai dati personali trasmessi, archiviati o altrimenti elaborati.

7.5 PRONTA NOTIFICA

Che informerà tempestivamente i Titolari:

- **Violazione dei dati** (*data breach*) - Qualsiasi violazione dei dati personali, della quale verrà a conoscenza entro 12 ore dal momento in cui ne avrà notizia, fornendo gli elementi utili a valutare l'entità della violazione (es. categorie di dati, categorie e numero approssimativo degli interessati coinvolti);
- **Richieste da parte degli interessati** - Qualsiasi richiesta ricevuta direttamente dagli interessati della quale verrà a conoscenza entro 3 giorni lavorativi dal momento in cui ne avrà notizia;
- **Istruzioni in violazione** - Qualsiasi istruzione scritta ricevuta dal Titolare che, secondo il parere del Responsabile, è in violazione della Normativa DP e / o in violazione dei doveri contrattuali ai sensi del presente ADP.

7.6 RISPOSTA AI QUESITI

Trattare tempestivamente e adeguatamente tutte le richieste del Titolare in relazione al trattamento dei dati e attenersi alle linee guida dell'Autorità di Controllo/Garante in merito all'elaborazione dei dati.

7.7 INFORMAZIONI PER DIMOSTRAZIONE CONFORMITÀ

Rendere disponibili al Titolare tutte le informazioni necessarie a dimostrare la conformità agli obblighi e alle istruzioni stabiliti nel presente ADP e, su richiesta del Titolare, a presentare le proprie procedure di trattamento dei dati per la revisione delle stesse. Il Responsabile deve consentire e contribuire a tali verifiche, comprese le ispezioni, che devono essere svolte dal Titolare o da persone dallo stesso autorizzate.

7.8 COOPERAZIONE CON TITOLARE PER AUTORITÀ DI SUPERVISIONE

Collaborare con i Titolari nel rispetto di eventuali ordini emessi dall'Autorità di Controllo o dalle autorità giudiziarie in relazione al trattamento dei dati;

7.9 CONSENSO PREVENTIVO SUB-RESPONSABILE

In caso di subappalto, di agire in conformità con quanto stabilito nell'articolo 10 di questo ADP;

7.10 ACCORDO DATA PROTECTION (ADP)

Che i servizi di trattamento da parte del sub-Responsabile saranno eseguiti in conformità con questo ADP.

Articolo 8: Riservatezza

Il Responsabile garantisce che le persone autorizzate all'esecuzione del trattamento dei dati si siano impegnate a rispettare la riservatezza o che siano soggette ad un obbligo legale di riservatezza, anche per un periodo ragionevole dopo la fine del rapporto di lavoro con il Responsabile.

Articolo 9: Sicurezza trattamento

Responsabili e sub-Responsabili devono rispettare le misure di sicurezza tecniche e organizzative che soddisfano almeno i requisiti della Normativa DP e qualsiasi misura particolare esistente specificata in questo ADP. Responsabili e sub-Responsabili informeranno immediatamente i Titolari di eventuali violazioni dei dati personali.

Articolo 10: Nomina sub-Responsabile

Il Responsabile dei dati non deve affidare in subappalto alcuna delle operazioni di trattamento dei dati senza la previa autorizzazione scritta del Titolare.

Laddove il Responsabile dei dati, affidi i propri obblighi ai sensi del presente ADP con il consenso del Titolare, questi lo fa solo tramite un accordo scritto con il sub-Responsabile, imponendo a quest'ultimo gli stessi obblighi stabiliti nell'ADP.

In particolare, il sub-Responsabile deve fornire garanzie sufficienti per attuare le misure tecniche e organizzative appropriate in modo tale che il trattamento soddisfi i requisiti del GDPR.

Il Responsabile dei dati rimane pienamente responsabile nei confronti del Titolare per l'adempimento degli obblighi dei sub-Responsabili.

L'elenco dei sub-responsabili è riportato in allegato al presente accordo (Allegato C) e aggiornato periodicamente.

Articolo 11: Diritti degli Interessati

Il Responsabile, in caso di richieste pervenute al Titolare che fanno riferimento a dati personali trattati dal Responsabile, dovrà garantire al Titolare di poter soddisfare i seguenti diritti degli interessati (artt. 15 e ss. del GDPR):

a) Diritto di Accesso: il Responsabile dovrà collaborare con i Titolari per confermare all'Interessato se siano o meno in corso trattamenti di dati personali che lo riguardano, unitamente ad ulteriori informazioni che potrebbero essere nell'esclusiva disponibilità del Responsabile;
b) Diritto di Cancellazione: il Responsabile, previa precisa ed esplicita conferma del Titolare, dovrà cancellare tutti i dati degli interessati richiedenti.
c) Diritto di Portabilità: il Responsabile dovrà consentire al Titolare di trasmettere i Dati Personali che riguardano l'interessato, direttamente all'interessato o ad un altro Titolare indicato dall'Interessato, attraverso un canale sicuro e utilizzando un formato strutturato, di uso comune e leggibile da dispositivo automatico, come concordato con i Titolari.
d) Diritto di Rettifica: il Responsabile dovrà garantire al Titolare la rettifica e/o integrazione dei Dati Personali degli Interessati richiedenti;
e) Diritto di Limitazione: il Responsabile dovrà garantire al Titolare la possibilità di limitare il trattamento dei dati personali dell'Interessato richiedente, per es. mediante dispositivi tecnici che indichino chiaramente che il trattamento dei dati personali è stato limitato, in modo tale che i dati personali non siano sottoposti ad ulteriori trattamenti e non possano essere modificati.
f) Diritto di Opposizione: il Responsabile dovrà garantire al Titolare che, in caso di opposizione al trattamento da parte dell'interessato, si astenga dal porre in essere qualsiasi ulteriore attività di trattamento dei dati personali.

Il Responsabile e i sub-Responsabili comunicheranno ogni informazione utile al fine di aiutare i Titolari a rispettare i diritti degli interessati entro 3 giorni lavorativi dal ricevimento dell'istanza da parte del Titolare.

Articolo 12: Richieste degli Interessati

Nel caso in cui il Responsabile riceva direttamente, o tramite un Sub-Responsabile, richieste di esercizio dei diritti, il Responsabile provvede a dare tempestiva comunicazione scritta al Titolare e comunque al

massimo entro 3 giorni lavorativi dal ricevimento dell'istanza da parte dell'interessato (all'attenzione di protezionedati@fsitaliane.it), allegando una copia della richiesta e fornendo tutte le informazioni utili.

Responsabile e sub-Responsabili non risponderanno a richieste degli interessati a meno che non siano specificamente autorizzati a farlo.

Articolo 13: Supporto al Titolare

Il Responsabile dei dati e i sub-Responsabili, se presenti, coopereranno con i Titolari - tenendo conto della natura del trattamento e delle informazioni a disposizione - nel garantire il rispetto degli obblighi relativi alla valutazione d'impatto preventiva (Data Protection Impact Assessment) dei trattamenti dei dati che possono comportare un rischio elevato per i diritti e le libertà degli interessati.

Articolo 14: Persone autorizzate al trattamento

Il Responsabile dei dati e i sub-responsabili, se presenti, garantiscono che solo il personale qualificato, debitamente autorizzato e addestrato tratterà i dati personali ai sensi del presente ADP.

Il Responsabile garantisce che chiunque agisca sotto la sua autorità, che ha accesso ai dati personali relativi al trattamento dei dati, li tratti secondo specifiche istruzioni ricevute dai Titolari o dal Responsabile stesso, in conformità con il presente ADP. Per l'attuazione dell'obbligo di cui sopra, il Responsabile deve identificare l'ambito delle operazioni di trattamento consentite e deve:

- fornire a tali persone autorizzate istruzioni dettagliate e formazione al fine di conformarsi alla normativa data protection e al presente ADP;
- assicurare che tali persone abbiano accesso solo ai dati personali, la cui conoscenza è necessaria per svolgere i compiti loro assegnati.

I nomi di tali persone autorizzate al trattamento devono essere forniti a Titolari se richiesto.

Articolo 15: Comunicazione di dati

Il Responsabile si asterrà dal comunicare dati personali del trattamento a terzi senza il preventivo consenso scritto dei Titolari.

Articolo 16: Trasferimenti a paesi terzi

Il Responsabile e gli eventuali sub-Responsabili non possono trasferire i dati personali provenienti dai Titolari al di fuori dello Spazio economico europeo (SEE) senza il previo consenso scritto di quest'ultimo (soggetto sempre a questo ADP e alle istruzioni del Titolare in relazione a tale trasferimento), sulla base dell'esistenza di adeguate garanzie per la protezione dei dati personali al fine di garantire che il livello di protezione delle persone interessate garantito dalla Normativa DP non sia compromesso.

Tuttavia, il trasferimento di dati personali all'estero può aver luogo, senza alcuna specifica autorizzazione da parte del Titolare, nel caso in cui la Commissione europea abbia deciso che il paese terzo di destinazione garantisce un livello adeguato di protezione.

Inoltre, in assenza di una decisione della Commissione ai sensi del paragrafo precedente, il Responsabile può trasferire dati personali relativi al trattamento in paesi terzi se una delle salvaguardie di cui agli articoli 46 e 47 del GDPR è soddisfatta (ossia l'utilizzo di clausole contrattuali standard approvate dalla

Commissione o da un'Autorità di Controllo, norme vincolanti d'impresa approvate da un'Autorità di Controllo o altre).

Articolo 17: Trattamento economico-esclusione

Si conviene che il Responsabile non ha diritto a nessun compenso specifico per l'esecuzione delle attività descritte in questo ADP; i servizi previsti dal presente ADP, infatti, sono conseguenti al Contratto e pertanto non è dovuta alcuna remunerazione o indennità o rimborso per le attività qui contemplate, in quanto l'intera valutazione economica del rapporto tra Responsabile e Titolare è stata debitamente definita nel Contratto.

Articolo 18: Responsabilità

Il Responsabile conserva nei confronti dei Titolari l'intera responsabilità dell'adempimento degli obblighi del sub-responsabile, qualora lo stesso ometta di adempiere ai propri obblighi in materia di protezione dei dati.

Articolo 19: Cessazione

Il presente ADP diventerà effettivo una volta firmato dalle Parti. L'esecuzione è valida fino al termine del Contratto o del trattamento dei dati per qualsivoglia motivo.

Articolo 20: Obblighi dopo cessazione

Alla cessazione del Contratto o del trattamento dei dati per qualsivoglia motivo, il Responsabile e i sub-Responsabili - se esistenti -, a scelta dei Titolari del trattamento,

- restituirà tutti i dati personali relativi al trattamento dei dati e le relative copie al Titolare

oppure

- distruggerà tutti i dati personali e certificherà al Titolare che lo ha fatto, a meno che la legislazione non gli impedisca di restituire o distruggere in tutto o in parte tali dati personali. In tal caso, per quanto riguarda i dati personali in questione, il Responsabile assicura che ne garantirà la riservatezza e non procederà più al loro trattamento.

Articolo 21: Legge applicabile

Questo ADP sarà regolato dalle leggi della giurisdizione dei Titolari, salvo quanto diversamente previsto in questo ADP, in linea con la Normativa DP.

Articolo 22: Tribunale competente

La sede esclusiva per tutte le controversie derivanti da o in connessione con questo ADP è il luogo di stabilimento dei Titolari, fatto salvo il diritto dei Titolari di presentare un'azione giudiziaria contro il Responsabile ed i sub-Responsabili, se presenti, di fronte qualsiasi altro tribunale competente.

Articolo 23: Intero accordo

Salvo quanto sopra dichiarato in relazione all'obbligo dei Titolari, in relazione alle variazioni delle sue istruzioni, questo documento contiene l'intero accordo delle Parti in relazione al suo oggetto (trattamento in appalto di dati personali).

Articolo 24: Annullamento

Se una disposizione di questo ADP è o diventa invalida o inapplicabile, la validità e l'applicabilità delle altre disposizioni di questo ADP rimangono inalterate. In questo caso, le Parti concordano di adottare una disposizione che corrisponda al meglio allo scopo previsto nella disposizione non valida o agli interessi delle Parti, come riportato nell'intera struttura di questo ADP.

Il presente accordo verrà automaticamente annullato in caso di risoluzione, per qualsiasi motivo, del Contratto.

Articolo 25: Variazioni del presente ADP

Fatti salvi gli obblighi dei Titolari, le modifiche delle clausole del presente ADP e delle annesse istruzioni che comportano una variazione di condizioni economiche superiore o pari al 5% (cinque per cento) dell'importo complessivo del contratto di riferimento, possono essere considerate valide solo se concordate tra i contraenti. L'accordo deve essere comprovato dalla firma di entrambe le Parti dell'emendamento scritto. L'emendamento deve specificare i contenuti che sostituiscono la corrispondente clausola dell'ADP, ovvero vi si aggiungono. Le Parti possono anche aggiungere clausole su questioni relative all'attività di business, laddove necessario, purché non contraddicano le clausole di questo ADP.

Allegati:
Allegato A: istruzioni per attività di trattamento, categorie di dati personali, durata del trattamento e soggetti interessati
Allegato B: misure tecniche e organizzative di sicurezza specificate
Allegato C [da mantenere se ci sono sub-responsabili individuati]: elenco sub-responsabili

Allegato A – Istruzioni sulle attività di Trattamento oggetto del presente ADP

Ruolo del Responsabile nel Trattamento

Attività di trattamento svolte dal Responsabile	Descrizione
Vulnerability Assessment	Le attività di *vulnerability assessment* dovranno essere svolte secondo le modalità, le istruzioni e sui perimetri applicativi di volta in volta esplicitati dalla S.O. Cyber Security. Si specifica che, in ogni caso, l'attività non dovrà prevedere il trattamento di dati personali se non strettamente indispensabili a certificare una vulnerabilità (ad es. è chiaramente ammessa l'identificazione di eventuali utenze con credenziali deboli) senza l'ingiustificata raccolta e conoscenza di dati non necessari. La reportistica prodotta dovrà prevedere l'anonimizzazione di eventuali dati personali, ove tale anonimizzazione non pregiudichi la certificazione della vulnerabilità. Eventuale documentazione prodotta a supporto dei report formali deve essere cancellata/distrutta in maniera sicura una volta formalizzato il Report.
Penetration Testing	Le attività di *penetration testing* dovranno essere svolte secondo le modalità, le istruzioni e sui perimetri applicativi di volta in volta esplicitati dalla S.O. Cyber Security. Si specifica che, in ogni caso, l'attività non dovrà prevedere il trattamento di dati personali se non strettamente indispensabili a certificare una vulnerabilità (ad es. è chiaramente ammessa l'identificazione di eventuali utenze con credenziali deboli) senza l'ingiustificata raccolta e conoscenza di dati non necessari. La reportistica prodotta dovrà prevedere l'anonimizzazione di eventuali dati personali, ove tale anonimizzazione non pregiudichi la certificazione della vulnerabilità. Eventuale documentazione prodotta a supporto dei report formali deve essere cancellata/distrutta in maniera sicura una volta formalizzato il Report.

Tipologie di Interessati

I Dati Personali trattati dal Responsabile per conto del Titolare riguardano le seguenti tipologie di Interessati:

X Clienti
X Prospect
X Lead/ Lead qualificati
X Candidati
X Dipendenti
X Fornitori
X Soggetti Terzi
X Famigliari (anche conviventi)
☐ Altro (specificare)
……

Tipologia di Dati Personali

I Dati Personali trattati dal Responsabile per conto del Titolare riguardano le seguenti categorie di Dati Personali:

X Comuni/Personali (es. Dati Anagrafici, CF, etc.)
X Particolari (es. Biometrico, Stato di Salute, Comportamentali/Psicologici, etc.)
X Giudiziari
X Dati relativi alla gestione del rapporto di lavoro, alla valutazione dei dipendenti e provvedimenti disciplinari
X Dati di navigazione (compresi log di accesso e indirizzi IP)
X Dati di videosorveglianza
X Dati di geolocalizzazione
X Dati di profilazione
X Sondaggi di opinione

Conservazione dei dati

I Dati Personali trattati dal Responsabile per conto del Titolare dovranno essere conservati, nel rispetto della Data Retention *Policy* della/e Società Titolare/i, per il tempo strettamente necessario alle finalità perseguite, come di seguito indicato:

Tipologie di interessato	Dettaglio sui Dati	Conservazione e Cancellazione
Vulnerability Assessment	I Report contenenti le vulnerabilità che riportano dati personali e ogni file di supporto	**Al termine dello specifico incarico**, il Responsabile è tenuto a restituire tutti i dati personali relativi al trattamento dei dati e le relative copie al Titolare e a distruggere tutti i dati personali, certificando al Titolare che lo ha fatto, a meno che la legislazione non gli impedisca di restituire o distruggere in tutto o in parte tali dati personali. In tal caso, per quanto riguarda i dati personali in questione, il Responsabile assicura che ne garantirà la riservatezza e non procederà più al loro trattamento.
Penetration Testing	I Report contenenti le vulnerabilità che riportano dati personali e ogni file di supporto	**Al termine dello specifico incarico**, il Responsabile è tenuto a restituire tutti i dati personali relativi al trattamento dei dati e le relative copie al Titolare e a distruggere tutti i dati personali, certificando al Titolare che lo ha fatto, a meno che la legislazione non gli impedisca di restituire o distruggere in tutto o in parte tali dati personali. In tal caso, per quanto riguarda i dati personali in questione, il Responsabile assicura che ne

		garantirà la riservatezza e non procederà più al loro trattamento.

Allegato B – Misure tecniche e organizzative di sicurezza specificate

Allegato B.1 – Misure di sicurezza specificate per le Postazioni di Lavoro mediante le quali è effettuato il trattamento di dati personali

#	Dominio	Controllo	Informazioni aggiuntive
1	**Meccanismi di identificazione e autenticazione**	Esistenza di meccanismi di accesso ai sistemi tramite il riconoscimento attraverso un nome utente e l'autenticazione attraverso password.	-
2	**Utilizzo utenze univoche e nominali**	Esistenza di utenze che siano associate in modo univoco a persone fisiche, identificabili con nome e cognome e/o riconducibili univocamente ad un unico soggetto responsabile	In caso di utenze Machine-To-Machine, è necessario attribuire le credenziali ad unico soggetto utilizzatore.
3	**Meccanismi di autorizzazione**	Implementazione di controlli che permettano di definire quali operazioni possa compiere uno specifico utente	L'autorizzazione è la fase successiva all'autenticazione degli utenti, dove vengono concessi (o negati) all'utente i privilegi di accesso ai sistemi informatici. I privilegi devono essere concessi in linea con i requisiti dettati nella politica di gestione degli accessi dell'organizzazione e nel rispetto dei principi di: - "Least Privilege": devono essere concessi all'utente esclusivamente i privilegi strettamente necessari a svolgere le attività per le quali è autorizzato; -"Need to Know": gli utenti devono essere autorizzati a trattare i soli dati essenziali allo svolgimento della loro mansione. La sussistenza dei requisiti di autorizzazione degli utenti deve essere verificata almeno semestralmente.
4	**Gestione utenze Privilegiate**	Implementazione di controlli specifici sulle utenze con privilegi ampi per impedire operazioni illecite	Devono essere previste procedure per l'attribuzione di privilegi di accesso "ampi" in base al ruolo e alle attività da eseguire sui sistemi
5	**Password policy conforme alle linee guida aziendali**	Insieme di regole che definiscono come dovrebbe essere costituita una password affinché possa essere ritenuta sufficientemente sicura; tale misura è associata alle utenze interne (non clienti).	I criteri di robustezza delle password includono: - lunghezza (almeno 8 caratteri) - frequenza di sostituzione adeguata (es. 90 gg) - presenza di: almeno da una lettera maiuscola, un numero e un carattere speciale - password history adeguata (es. ultime 5 password memorizzate) per evitare il riutilizzo di una stessa credenziale o, in alternativa, assicurare che le stesse credenziali non possano essere riutilizzate per un determinato lasso di tempo (e.g. sei mesi); - password differente dall'user_id associata o non "qwerty" o differente da alcune parole quali il nome della società. Per maggiori dettagli si rimanda all'allegato DdG n. 212/AD del 12 luglio 2016.
6	**Accesso logico terze parti**	L'accesso logico ai sistemi da parte di terzi (ad esempio clienti, fornitori, consulenti) deve essere soggetto a controlli rigorosi.	I requisiti per il controllo degli accessi logici ai sistemi comprendono: - autorizzare il personale prima che gli venga concesso l'accesso alle applicazioni dell'organizzazione; - assegnare specifici privilegi di accesso per accedere alle applicazioni o funzionalità di un'applicazione; - adottare opportuni meccanismi di controllo

#	Dominio	Controllo	Informazioni aggiuntive
			dell'accesso (ad esempio password, token o biometrico).
7	**Tracciamenti accessi utenti**	Registrazione e memorizzazione dei log degli accessi degli utenti (es. login, logout e principali attività utente, ad esempio download di dati, cancellazione di dati, modifiche massive dei dati)	Si specifica che si fa riferimento ai soli sistemi target (il tracciamento non riguarda le postazioni di lavoro/client)
8	**Tracciamento accessi Amministratori di Sistema**	Registrazione e memorizzazione dei log degli accessi degli Amministratori di Sistema (es. login, logout e principali attività utente, ad esempio download di dati, cancellazione di dati, modifiche massive dei dati)	Si specifica che si fa riferimento ai soli sistemi target (il tracciamento non riguarda le postazioni di lavoro/client)
9	**Protezione dei log**	Esistenza di meccanismi di protezione dei log in maniera da non poter essere cancellati da personale non autorizzato.	I log raccolti devono essere protetti da un uso improprio (ad esempio manomissione in transito, accesso/modifica/cancellazione non autorizzati). Esempi di misure di sicurezza dei log memorizzati in locale ("at rest") sono: - memorizzare o copiare i log su storage in sola lettura; - autorizzare, registrare e monitorare tutti gli accessi ai log; - implementare meccanismi di rilevamento delle manomissioni, in modo da sapere se un record del log è stato modificato o eliminato; - rivedere periodicamente i privilegi per l'accesso ai log. Esempi di misure di sicurezza dei log in transito sono: - se i log sono inviati su reti non attendibili (ad esempio Internet), utilizzare un protocollo di trasmissione sicuro/ cifrato (as esempio TLS); - Effettuare controlli di due diligence (normativi e di sicurezza) prima di inviare i log a terze parti.
10	**Retention dei log**	Esistenza di un limite temporale (almeno 6 mesi, al massimo 12 mesi) entro il quale possano essere conservati i log	- Almeno 6 mesi per gli Amministratori di Sistema (come da normativa di riferimento). - Il limite temporale è funzione di eventuali vincoli tecnologici presenti sul sistema
11	**Tracciamento degli Incident**	Registrazione e memorizzazione degli incidenti avvenuti/individuati	Esistenza di una procedura e strumenti a supporto che permettono di registrare e gestire eventuali fault occorsi, incidenti di sicurezza logica e fisica (es. accesso non autorizzato, furto/smarrimento ecc)
12	**Network Time Protocol (NTP)**	Configurazione del protocollo NTP al fine di sincronizzare il clock del sistema	Si specifica che la sincronizzazione deve avvenire con i sistemi del Cliente o con fonti attendibili pubbliche
13	**Hardening dei sistemi**	Implementazione di specifiche configurazioni su sistemi e componenti che permettono di incrementare la sicurezza di un sistema.	Linee Guida del Vendor/AGID
14	**Antivirus**	Adozione di strumenti di prevenzione e protezione da virus.	**-**

#	Dominio	Controllo	Informazioni aggiuntive
15	**Collezionamento eventi virus su piattaforma centralizzata**	Tutti gli eventi virus-related devono essere inviati ad una piattaforma centralizzata di collezionamento.	**-**
16	**Aggiornamento software anti-virus**	Il software anti-virus deve essere costantemente aggiornato.	-
17	**Patch Management**	Installazione di patch di sicurezza sui sistemi per risolvere le vulnerabilità presenti	-
18	**Patch Management tramite tool automatici**	Utilizzo di tool automatici per le attività di patch management.	-
19	**Back up periodico**	Effettuazione pianificata di copie di riserva finalizzata a duplicare, con una periodicità prestabilita, i dati, le configurazioni e le immagini di sistema su appositi supporti di memorizzazione.	- Definizione e conduzione di un processo automatico e/o operativo che garantisce l'esecuzione periodica dei backup - Le informazioni e i dati da copiare riguardano i dati memorizzati sui sistemi, i file di configurazione, ecc… - E' preferibile effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore. - Il backup deve essere effettuato almeno settimanalmente. - I dati e le informazioni presenti nelle copie di backup devono essere protetti con misure almeno pari a quelli dei dati originali
20	**Tecniche di cifratura**	Esistenza di tecniche di cifratura dei dati memorizzati (es. dati memorizzati nei database o nelle memorie di massa)	La cifratura deve essere utilizzata in tutta l'organizzazione al fine di: - proteggere la riservatezza delle informazioni sensibili o delle informazioni soggette a requisiti legali e normativi; - determinare se le informazioni critiche sono state alterate (ad esempio implementando funzioni hash o la firma digitale). Per maggiori dettagli fare riferimento alla relativa "Linea guida protezione postazioni di lavoro" emessa nel 2014 per quanto concerne le attività di cifratura del disco e delle memorie di massa.
21	**Cancellazione base (a livello software)**	Utilizzo di algoritmi e meccanismi generici per la cancellazione dei dati	Utilizzo di meccanismi quali ad esempio la sovrascrittura con una sequenza di zero, la formattazione.

Allegato B.2 – Misure di sicurezza specificate per eventuali strumenti mobile mediante le quali è effettuato il trattamento di dati personali

Non è ammesso il trattamento di dati personali mediante strumenti *mobile* (*smartphone, tablet*, etc.).

Allegato B.3 – Misure di sicurezza specificate sui dati personali trattati

Deve essere prevista la protezione del dato personale (anche se inclusa in report di VA/PT e di Digital Forensic) sia *at rest* sia in transito.

In particolare, è richiesto al Responsabile:

- cifratura dei Report e di eventuale documentazione di supporto in transito;
- cifratura di eventuali copie di back-up;
- cifratura dei supporti (hard disk, postazioni di lavoro, etc.) contenenti i Report;
- tecniche e protocolli per la protezione dei dati durante le attività di assessment (es. VPN);
- misure di sicurezza fisiche per controllare gli accessi che vengono effettuati ai locali nelle sedi del Responsabile in cui sono effettuati gli *assessment*;
- tutti i Report e l'eventuale documentazione di supporto deve essere oggetto di un processo di cancellazione e/o sovrascrittura sicuri (e.g, sovrascritture, *degausser*, DBAN *software*).

Allegato C – [da mantenere se ci sono sub-responsabili individuati] Elenco sub-responsabili

Allegato n. 2

Servizi professionali volti ad analizzare la sicurezza informatica dei sistemi informativi delle Società del Gruppo Ferrovie dello Stato Italiane

Accordo di Data Protection

Titolare – Responsabile

INDICE

Articolo 1: Premesse e Allegati 5
Articolo 2: Oggetto dell'Accordo 5
Articolo 3: Definizioni 5
Articolo 4: Ambito di competenza 6
Articolo 5: Ambito del trattamento 6
Articolo 6: Obblighi del Titolare 6
Articolo 7: Obblighi Responsabile 6
7.1 RISPETTO DELLE ISTRUZIONI DEL TITOLARE 6
7.2 CONFORMITÀ ALLA NORMATIVA DP 6
7.3 AMMINISTRATORI DI SISTEMA 7
7.4 MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE 7
7.5 PRONTA NOTIFICA 7
7.6 RISPOSTA AI QUESITI 8
7.7 INFORMAZIONI PER DIMOSTRAZIONE CONFORMITÀ 8
7.8 COOPERAZIONE CON TITOLARE PER AUTORITÀ DI SUPERVISIONE 8
7.9 CONSENSO PREVENTIVO SUB-RESPONSABILE 8
7.10 ACCORDO DATA PROTECTION (ADP) 8
Articolo 8: Riservatezza 8
Articolo 9: Sicurezza trattamento 9
Articolo 10: Nomina sub-Responsabile 9
Articolo 11: Diritti degli Interessati 9
Articolo 12: Richieste degli Interessati 10
Articolo 13: Supporto al Titolare 10
Articolo 14: Persone autorizzate al trattamento 10
Articolo 15: Comunicazione di dati 11
Articolo 16: Trasferimenti a paesi terzi 11
Articolo 17: Trattamento economico-esclusione 11
Articolo 18: Responsabilità 11
Articolo 19: Cessazione 12
Articolo 20: Obblighi dopo cessazione 12
Articolo 21: Legge applicabile 12
Articolo 22: Tribunale competente 12
Articolo 23: Intero accordo 12

Articolo 24: Annullamento **12**

Articolo 25: Variazioni del presente ADP **13**

Allegato A – Istruzioni sulle attività di Trattamento oggetto del presente ADP **16**

Allegato B – Misure tecniche e organizzative di sicurezza specificate **19**

Allegato B.1 – Misure di sicurezza specificate per le Postazioni di Lavoro mediante le quali è effettuato il trattamento di dati personali 19

Allegato B.2 – Misure di sicurezza specificate per eventuali strumenti mobile mediante le quali è effettuato il trattamento di dati personali 22

Allegato B.3 – Misure di sicurezza specificate sui dati personali trattati 22

Allegato C – [da mantenere se ci sono sub-responsabili individuati] Elenco sub-responsabili **23**

Accordo di Data Protection

TRA

…… [*specificare il nome del Titolare*], con sede legale in …….. [*specificare l'indirizzo della sede legale del Titolare*], in persona del suo legale rappresentante …….. [*specificare il nome completo del legale rappresentante del Titolare*] (di seguito "[*specificare il nome abbreviato del Titolare*]" o "Titolare")

E

…… [*specificare il nome del Responsabile*], con sede legale in …… *[specificare l'indirizzo della sede legale del Responsabile*], in persona del suo legale rappresentante …… [*specificare il nome completo del legale rappresentante del Responsabile*] (di seguito "Responsabile").

Titolare e Responsabile verranno in seguito entrambi indicati come "la Parte" o congiuntamente "le Parti".

PREMESSE

Normativa Data Protection (Normativa DP)

L' art. 28 del Regolamento (UE) 2016/679 ("GDPR" o "Normativa DP") stabilisce che quando il trattamento deve essere effettuato per conto di un titolare, il trattamento da parte del soggetto terzo nominato responsabile del trattamento è disciplinato da un contratto che è vincolante per il responsabile nei confronti del titolare e che definisce l'oggetto e la durata del trattamento, la natura e lo scopo, il tipo di dati personali e le categorie di interessati trattati, gli obblighi e i diritti del titolare.

Contratto

Il Responsabile fornirà servizi al Titolare in relazione all'analisi di sicurezza informatica dei sistemi informativi delle Società del Gruppo Ferrovie dello Stato Italiane ("Servizi"), come specificato nel contratto sottoscritto dalle parti [*specificare la data del contratto*] ("Contratto").

Servizi

Nel contesto dei Servizi, il Titolare trasferirà al Responsabile alcuni dati personali e il Responsabile elaborerà e utilizzerà tali dati personali per conto del Titolare nel rispetto della Normativa DP e in conformità al presente accordo sul trattamento dei dati (di seguito "ADP").

Competenza del Responsabile

Il Responsabile fornisce garanzie sufficienti, in particolare in termini di conoscenze specialistiche, affidabilità e risorse, per attuare misure tecniche e organizzative che soddisfino i requisiti della Normativa DP, compresa la sicurezza del trattamento per garantire la riservatezza e la protezione dei diritti degli interessati.

Affidamento dati

Il Titolare affida al Responsabile le attività di trattamento di dati personali come dettagliato nell'Allegato A (Istruzioni) e Allegato B (Misure di Sicurezza tecnico-organizzative) e il Responsabile si impegna ad eseguire il trattamento per conto del Titolare.

Titolare

[La Società del Gruppo FS], determinando le finalità e i mezzi del trattamento dei dati personali per l'esecuzione dei Servizi è qualificato come "Titolare", in base alla Normativa DP;

Contrattualizzazione

Le Parti intendono stipulare un accordo contrattuale per le operazioni di trattamento dei dati.

Sulla base degli assunti di cui sopra, le Parti convengono quanto segue.

Articolo 1: Premesse e Allegati

Le premesse e gli allegati sono parti sostanziali di questo ADP.

Articolo 2: Oggetto dell'Accordo

Le Parti con questo ADP intendono disciplinare il trattamento dei dati personali da parte del Responsabile, specificare l'oggetto, la durata, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati e gli obblighi e i diritti delle Parti.

Articolo 3: Definizioni

I termini utilizzati nel presente ADP hanno il seguente significato:

- "dati personali", "categorie speciali di dati personali", "processo/trattamento", "titolare", "responsabile" e "interessato" hanno lo stesso significato utilizzato nel GDPR;
- "sub-responsabile": qualsiasi entità impegnata dal Responsabile che accetti di ricevere dati personali esclusivamente finalizzati alla realizzazione dei Servizi in conformità con le istruzioni del Titolare e i termini dell'ADP;
- "Normativa Data Protection" (Normativa DP): la legislazione che tutela i diritti e le libertà fondamentali delle persone fisiche e, in particolare, il loro diritto alla vita privata in relazione al trattamento dei dati personali, applicabile ad un Titolare nello Stato membro dell'UE in cui questi è stabilito;
- "misure tecniche e organizzative": misure volte a garantire un livello di sicurezza adeguato al rischio, volte a proteggere i dati personali dalla distruzione accidentale o illecita o dalla perdita accidentale, dall'alterazione, dalla divulgazione non autorizzata o dall'accesso non autorizzato ai dati personali trasmessi, archiviati o altrimenti trattati e contro tutte le altre forme illecite di trattamento;
- "violazione dei dati personali" o "data breach": violazione della sicurezza che porta alla distruzione, perdita, alterazione, divulgazione non autorizzata o illegale di dati personali trasmessi, archiviati o altrimenti elaborati.

- “autorità di controllo” è l’autorità pubblica indipendente istituita da uno Stato membro incaricata di sorvegliare l’applicazione della Normativa DP (per l’Italia, il “Garante”).

Articolo 4: Ambito di competenza

Tramite questo ADP il Titolare impegna *[Fornitore]*, che sottoscrivendo questo accordo lo accetta, come "Responsabile" come definito dalla Normativa DP, per il trattamento dei dati.

Articolo 5: Ambito del trattamento

I dettagli del trattamento dei dati, le istruzioni operative rispetto alle attività di competenza del Responsabile ovvero le categorie di dati personali e di soggetti interessati sono specificati nell'Allegato A.

Articolo 6: Obblighi del Titolare

Il Titolare del trattamento garantisce:

A) Conformità - Che è responsabile per la valutazione dell'ammissibilità del trattamento dei dati e garantisce i diritti degli interessati coinvolti.

B) Sicurezza - Che le misure tecniche e organizzative oggetto del presente accordo assicurano un livello di sicurezza adeguato ai rischi connessi al trattamento dei dati e alla natura dei dati da proteggere;

C) Istruzioni - Che le istruzioni oggetto del presente accordo sono sufficienti a definire lo scopo e la procedura del trattamento dei dati.

Articolo 7: Obblighi Responsabile

Il Responsabile garantisce:

7.1 RISPETTO DELLE ISTRUZIONI DEL TITOLARE

Di trattare i dati personali solo per conto del Titolare, limitati alle sole attività di trattamento strettamente necessarie per l'esecuzione di questo ADP e in conformità con le sue istruzioni documentate e questo ADP; se non è in grado di fornire tale conformità per qualsiasi motivo, accetta di informare tempestivamente il Titolare della sua impossibilità di adempiere, nel qual caso il Titolare ha il diritto di sospendere l'elaborazione dei dati e / o risolvere il Contratto e questo ADP.

7.2 CONFORMITÀ ALLA NORMATIVA DP

Che verrà data attuazione alle istruzioni ricevute dal Titolare nel rispetto degli obblighi di cui al Contratto e nel presente ADP. Nell’ipotesi di eventuali modifiche alla normativa vigente che possano incidere sulle obbligazioni assunte, il Responsabile si impegna a darne immediata

comunicazione al Titolare, il quale potrà sospendere l'elaborazione dei dati e/o risolvere il Contratto e il presente ADP.

7.3 AMMINISTRATORI DI SISTEMA

Il Responsabile si impegna ad adempiere alle seguenti prescrizioni ai fini della corretta applicazione dei provvedimenti del Garante per la protezione dei dati personali del 27/11/2008 e del 25/6/2009 relativi alla gestione degli amministratori di sistema, nonché agli eventuali successivi provvedimenti o norme in materia.

I soggetti preposti dal Responsabile a svolgere funzioni di amministratori di sistema che godono di profili di accesso superiori a quelli degli utenti ordinari per quanto attiene le banche dati o gli applicativi contenenti i dati degli interessati oggetto delle operazioni di trattamento, devono essere previamente selezionati in base alla valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

La nomina degli amministratori di sistema, deve avvenire per iscritto e con designazione individuale delle persone autorizzate al trattamento e deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Gli estremi identificativi delle persone fisiche amministratori di sistema operanti sui sistemi che ospitano i dati personali, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di richieste da parte del Titolare o accertamenti da parte del Garante.

L'operato degli amministratori di sistema è oggetto, con cadenza almeno annuale, di un'attività di verifica, in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dal Codice Privacy.

Il Responsabile deve provvedere al tracciamento dei log di accesso degli amministratori di sistema, secondo modalità definite in comune accordo con il Titolare.

Entro il 15 gennaio di ogni anno, il Responsabile comunicherà al Titolare con apposito rapporto scritto il soddisfacimento delle prescrizioni di cui ai citati provvedimenti.

7.4 MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

Il Responsabile, prima di eseguire il trattamento dei dati, tenuto conto del rischio per i diritti e le libertà degli interessati coinvolti e gli esiti di eventuali *Data Protection Impact Assessment* svolti dal Titolare, garantisce l'adozione delle misure tecniche e organizzative di sicurezza specificate nell'Allegato B.

Nel valutare il livello appropriato di sicurezza, si dovrà prestare particolare attenzione ai rischi di distruzione accidentale o illecita, perdita, alterazione, divulgazione non autorizzata o accesso non autorizzato ai dati personali trasmessi, archiviati o altrimenti elaborati.

7.5 PRONTA NOTIFICA

Che informerà tempestivamente il Titolare:

- **Violazione dei dati** (*data breach*) - Qualsiasi violazione dei dati personali, della quale verrà a conoscenza entro 12 ore dal momento in cui ne avrà notizia, fornendo gli elementi utili a valutare l'entità della violazione (es. categorie di dati, categorie e numero approssimativo degli interessati coinvolti);
- **Richieste da parte degli interessati** - Qualsiasi richiesta ricevuta direttamente dagli interessati della quale verrà a conoscenza entro 3 giorni lavorativi dal momento in cui ne avrà notizia;
- **Istruzioni in violazione** - Qualsiasi istruzione scritta ricevuta dal Titolare che, secondo il parere del Responsabile, è in violazione della Normativa DP e / o in violazione dei doveri contrattuali ai sensi del presente ADP.

7.6 RISPOSTA AI QUESITI

Trattare tempestivamente e adeguatamente tutte le richieste del Titolare in relazione al trattamento dei dati e attenersi alle linee guida dell'Autorità di Controllo/Garante in merito all'elaborazione dei dati.

7.7 INFORMAZIONI PER DIMOSTRAZIONE CONFORMITÀ

Rendere disponibili al Titolare tutte le informazioni necessarie a dimostrare la conformità agli obblighi e alle istruzioni stabiliti nel presente ADP e, su richiesta del Titolare, a presentare le proprie procedure di trattamento dei dati per la revisione delle stesse. Il Responsabile deve consentire e contribuire a tali verifiche, comprese le ispezioni, che devono essere svolte dal Titolare o da persone dallo stesso autorizzate.

7.8 COOPERAZIONE CON TITOLARE PER AUTORITÀ DI SUPERVISIONE

Collaborare con il Titolare nel rispetto di eventuali ordini emessi dall'Autorità di Controllo o dalle autorità giudiziarie in relazione al trattamento dei dati;

7.9 CONSENSO PREVENTIVO SUB-RESPONSABILE

In caso di affidamento delle operazioni di trattamento, di agire in conformità con quanto stabilito nell'articolo 10 di questo ADP;

7.10 ACCORDO DATA PROTECTION (ADP)

Che i servizi di trattamento da parte del sub-Responsabile saranno eseguiti in conformità con questo ADP.

Articolo 8: Riservatezza

Il Responsabile garantisce che le persone autorizzate all'esecuzione del trattamento dei dati si siano impegnate a rispettare la riservatezza o che siano soggette ad un obbligo legale di riservatezza, anche per un periodo ragionevole dopo la fine del rapporto di lavoro con il Responsabile.

Articolo 9: Sicurezza trattamento

Responsabili e sub-Responsabili devono rispettare le misure di sicurezza tecniche e organizzative che soddisfano almeno i requisiti della Normativa DP e qualsiasi misura particolare esistente specificata in questo ADP. Responsabili e sub-Responsabili informeranno immediatamente il Titolare di eventuali violazioni dei dati personali.

Articolo 10: Nomina sub-Responsabile

Il Responsabile dei dati non deve affidare alcuna delle operazioni di trattamento dei dati senza la previa autorizzazione scritta del Titolare.

Laddove il Responsabile dei dati affidi i propri obblighi ai sensi del presente ADP con il consenso del Titolare, questi lo fa solo tramite un accordo scritto con il sub-Responsabile, imponendo a quest'ultimo gli stessi obblighi stabiliti nell'ADP.

In particolare, il sub-Responsabile deve fornire garanzie sufficienti per attuare le misure tecniche e organizzative appropriate in modo tale che il trattamento soddisfi i requisiti del GDPR.

Il Responsabile dei dati rimane pienamente responsabile nei confronti del Titolare per l'adempimento degli obblighi dei sub-Responsabili.

L'elenco dei sub-responsabili è riportato in allegato al presente accordo (Allegato C) e aggiornato periodicamente.

Articolo 11: Diritti degli Interessati

Il Responsabile, in caso di richieste pervenute al Titolare che fanno riferimento a dati personali trattati dal Responsabile, dovrà garantire al Titolare di poter soddisfare i seguenti diritti degli interessati (artt. 15 e ss. del GDPR):

a) Diritto di Accesso: il Responsabile dovrà collaborare con il Titolare per confermare all'Interessato se siano o meno in corso trattamenti di dati personali che lo riguardano, unitamente ad ulteriori informazioni che potrebbero essere nell'esclusiva disponibilità del Responsabile;
b) Diritto di Cancellazione: il Responsabile, previa precisa ed esplicita conferma del Titolare, dovrà cancellare tutti i dati degli interessati richiedenti.
c) Diritto di Portabilità: il Responsabile dovrà consentire al Titolare di trasmettere i Dati Personali che riguardano l'interessato, direttamente all'interessato o ad un altro Titolare indicato dall'Interessato, attraverso un canale sicuro e utilizzando un formato strutturato, di uso comune e leggibile da dispositivo automatico, come concordato con il Titolare.
d) Diritto di Rettifica: il Responsabile dovrà garantire al Titolare la rettifica e/o integrazione dei Dati Personali degli Interessati richiedenti;
e) Diritto di Limitazione: il Responsabile dovrà garantire al Titolare la possibilità di limitare il trattamento dei dati personali dell'Interessato richiedente, per es. mediante dispositivi tecnici che indichino chiaramente che il trattamento dei dati personali è stato limitato, in

modo tale che i dati personali non siano sottoposti ad ulteriori trattamenti e non possano essere modificati.

f) Diritto di Opposizione: il Responsabile dovrà garantire al Titolare che, in caso di opposizione al trattamento da parte dell'interessato, si astenga dal porre in essere qualsiasi ulteriore attività di trattamento dei dati personali.

Il Responsabile e i sub-Responsabili comunicheranno ogni informazione utile al fine di aiutare il Titolare a rispettare i diritti degli interessati entro 3 giorni lavorativi dal ricevimento dell'istanza da parte del Titolare.

Articolo 12: Richieste degli Interessati

Nel caso in cui il Responsabile riceva direttamente, o tramite un Sub-Responsabile, richieste di esercizio dei diritti, il Responsabile provvede a dare tempestiva comunicazione scritta al Titolare e comunque al massimo entro 3 giorni lavorativi dal ricevimento dell'istanza da parte dell'interessato (all'attenzione di ... [*indicare le informazioni di contatto della funzione interna del Titolare cui recapitare l'informazione*]), allegando una copia della richiesta e fornendo tutte le informazioni utili.

Responsabile e sub-Responsabili non risponderanno a richieste degli interessati a meno che non siano specificamente autorizzati a farlo.

Articolo 13: Supporto al Titolare

Il Responsabile dei dati e i sub-Responsabili, se presenti, coopereranno con il Titolare - tenendo conto della natura del trattamento e delle informazioni a disposizione - nel garantire il rispetto degli obblighi relativi alla valutazione d'impatto preventiva (Data Protection Impact Assessment) dei trattamenti dei dati che possono comportare un rischio elevato per i diritti e le libertà degli interessati.

Articolo 14: Persone autorizzate al trattamento

Il Responsabile dei dati e i sub-responsabili, se presenti, garantiscono che solo il personale qualificato, debitamente autorizzato e addestrato tratterà i dati personali ai sensi del presente ADP.

Il Responsabile garantisce che chiunque agisca sotto la sua autorità, che ha accesso ai dati personali relativi al trattamento dei dati, li tratti secondo specifiche istruzioni ricevute dal Titolare o dal Responsabile stesso, in conformità con il presente ADP. Per l'attuazione dell'obbligo di cui sopra, il Responsabile deve identificare l'ambito delle operazioni di trattamento consentite e deve:

- fornire a tali persone autorizzate istruzioni dettagliate e formazione al fine di conformarsi alla normativa data protection e al presente ADP;

- assicurare che tali persone abbiano accesso solo ai dati personali, la cui conoscenza è necessaria per svolgere i compiti loro assegnati.

I nomi di tali persone autorizzate al trattamento devono essere forniti al Titolare se richiesto.

Articolo 15: Comunicazione di dati

Il Responsabile si asterrà dal comunicare dati personali del trattamento a terzi senza il preventivo consenso scritto del Titolare.

Articolo 16: Trasferimenti a paesi terzi

Il Responsabile e gli eventuali sub-Responsabili non possono trasferire i dati personali provenienti dal Titolare al di fuori dello Spazio economico europeo (SEE) senza il previo consenso scritto di quest'ultimo (soggetto sempre a questo ADP e alle istruzioni del Titolare in relazione a tale trasferimento), sulla base dell'esistenza di adeguate garanzie per la protezione dei dati personali al fine di garantire che il livello di protezione delle persone interessate garantito dalla Normativa DP non sia compromesso.

Tuttavia, il trasferimento di dati personali all'estero può aver luogo, senza alcuna specifica autorizzazione da parte del Titolare, nel caso in cui la Commissione europea abbia deciso che il paese terzo di destinazione garantisce un livello adeguato di protezione.

Inoltre, in assenza di una decisione della Commissione ai sensi del paragrafo precedente, il Responsabile può trasferire dati personali relativi al trattamento in paesi terzi se una delle salvaguardie di cui agli articoli 46 e 47 del GDPR è soddisfatta (ossia l'utilizzo di clausole contrattuali standard approvate dalla Commissione o da un'Autorità di Controllo, norme vincolanti d'impresa approvate da un'Autorità di Controllo o altre).

Articolo 17: Trattamento economico-esclusione

Si conviene che il Responsabile non ha diritto a nessun compenso specifico per l'esecuzione delle attività descritte in questo ADP; i servizi previsti dal presente ADP, infatti, sono conseguenti al Contratto e pertanto non è dovuta alcuna remunerazione o indennità o rimborso per le attività qui contemplate, in quanto l'intera valutazione economica del rapporto tra Responsabile e Titolare è stata debitamente definita nel Contratto.

Articolo 18: Responsabilità

Il Responsabile conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi del sub-responsabile, qualora lo stesso ometta di adempiere ai propri obblighi in materia di protezione dei dati.

Articolo 19: Cessazione

Il presente ADP diventerà effettivo una volta firmato dalle Parti. L'esecuzione è valida fino al termine del Contratto o del trattamento dei dati per qualsivoglia motivo.

Articolo 20: Obblighi dopo cessazione

Alla cessazione del Contratto o del trattamento dei dati per qualsivoglia motivo, il Responsabile e i sub-Responsabili - se esistenti -, a scelta del Titolare del trattamento,

- restituirà tutti i dati personali relativi al trattamento dei dati e le relative copie al Titolare

  o

- distruggerà tutti i dati personali e certificherà al Titolare che lo ha fatto, a meno che la legislazione non gli impedisca di restituire o distruggere in tutto o in parte tali dati personali. In tal caso, per quanto riguarda i dati personali in questione, il Responsabile assicura che ne garantirà la riservatezza e non procederà più al loro trattamento.

Articolo 21: Legge applicabile

Questo ADP sarà regolato dalle leggi della giurisdizione del Titolare, salvo quanto diversamente previsto in questo ADP, in linea con la Normativa DP.

Articolo 22: Tribunale competente

La sede esclusiva per tutte le controversie derivanti da o in connessione con questo ADP è il luogo di stabilimento del Titolare, fatto salvo il diritto del Titolare di presentare un'azione giudiziaria contro il Responsabile ed i sub-Responsabili, se presenti, di fronte qualsiasi altro tribunale competente.

Articolo 23: Intero accordo

Salvo quanto sopra dichiarato in relazione all'obbligo del Titolare, in relazione alle variazioni delle sue istruzioni, questo documento contiene l'intero accordo delle Parti in relazione al suo oggetto (trattamento di dati personali).

Articolo 24: Annullamento

Se una disposizione di questo ADP è o diventa invalida o inapplicabile, la validità e l'applicabilità delle altre disposizioni di questo ADP rimangono inalterate. In questo caso, le Parti concordano di adottare una disposizione che corrisponda al meglio allo scopo previsto

nella disposizione non valida o agli interessi delle Parti, come riportato nell'intera struttura di questo ADP.

Il presente accordo verrà automaticamente annullato in caso di risoluzione, per qualsiasi motivo, del Contratto.

Articolo 25: Variazioni del presente ADP

Fatti salvi gli obblighi del Titolare, le modifiche delle clausole del presente ADP e delle annesse istruzioni che comportano una variazione di condizioni economiche superiore o pari al 5% (cinque per cento) dell'importo complessivo del contratto di riferimento, possono essere considerate valide solo se concordate tra i contraenti. L'accordo deve essere comprovato dalla firma di entrambe le Parti dell'emendamento scritto. L'emendamento deve specificare i contenuti che sostituiscono la corrispondente clausola dell'ADP, ovvero vi si aggiungono. Le Parti possono anche aggiungere clausole su questioni relative all'attività di business, laddove necessario, purché non contraddicano le clausole di questo ADP.

Allegati:
Allegato A: istruzioni per attività di trattamento, categorie di dati personali, durata del trattamento e soggetti interessati
Allegato B: misure tecniche e organizzative di sicurezza specificate
Allegato C [da mantenere se ci sono subfornitori individuati]: elenco subfornitori

[*Firme*]

Per il Titolare:

Nome (scritto in forma estesa):

Ruolo:

Indirizzo:

Firma…….

(timbro dell'azienda)

Per il Responsabile:

Nome (scritto in forma estesa):

Ruolo:

Indirizzo:

Firma…….

(timbro dell'azienda)

[*Fine documento*]

Allegato A – Istruzioni sulle attività di Trattamento oggetto del presente ADP

Ruolo del Responsabile nel Trattamento

Attività di trattamento svolte dal Responsabile	Descrizione
Vulnerability Assessment	Le attività di *vulnerability assessment* dovranno essere svolte secondo le modalità, le istruzioni e sui perimetri applicativi di volta in volta esplicitati dalla S.O. Cyber Security. Si specifica che, in ogni caso, l'attività non dovrà prevedere il trattamento di dati personali se non strettamente indispensabili a certificare una vulnerabilità (ad es. è chiaramente ammessa l'identificazione di eventuali utenze con credenziali deboli) senza l'ingiustificata raccolta e conoscenza di dati non necessari. La reportistica prodotta dovrà prevedere l'anonimizzazione di eventuali dati personali, ove tale anonimizzazione non pregiudichi la certificazione della vulnerabilità. Eventuale documentazione prodotta a supporto dei report formali deve essere cancellata/distrutta in maniera sicura una volta formalizzato il Report.
Penetration Testing	Le attività di *penetration testing* dovranno essere svolte secondo le modalità, le istruzioni e sui perimetri applicativi di volta in volta esplicitati dalla S.O. Cyber Security. Si specifica che, in ogni caso, l'attività non dovrà prevedere il trattamento di dati personali se non strettamente indispensabili a certificare una vulnerabilità (ad es. è chiaramente ammessa l'identificazione di eventuali utenze con credenziali deboli) senza l'ingiustificata raccolta e conoscenza di dati non necessari. La reportistica prodotta dovrà prevedere l'anonimizzazione di eventuali dati personali, ove tale anonimizzazione non pregiudichi la certificazione della vulnerabilità. Eventuale documentazione prodotta a supporto dei report formali deve essere cancellata/distrutta in maniera sicura una volta formalizzato il Report.

Tipologie di Interessati

I Dati Personali trattati dal Responsabile per conto del Titolare riguardano le seguenti tipologie di Interessati:

X Clienti
X Prospect
X Lead/ Lead qualificati
X Candidati
X Dipendenti
X Fornitori
X Soggetti Terzi
X Famigliari (anche conviventi)
☐ Altro (specificare)
……

Tipologia di Dati Personali

I Dati Personali trattati dal Responsabile per conto del Titolare riguardano le seguenti categorie di Dati Personali:

X Comuni/Personali (es. Dati Anagrafici, CF, etc.)
X Particolari (es. Biometrico, Stato di Salute, Comportamentali/Psicologici, etc.)
X Giudiziari
X Dati relativi alla gestione del rapporto di lavoro, alla valutazione dei dipendenti e provvedimenti disciplinari
X Dati di navigazione (compresi log di accesso e indirizzi IP)
X Dati di videosorveglianza
X Dati di geolocalizzazione
X Dati di profilazione
X Sondaggi di opinione

Conservazione dei dati

I Dati Personali trattati dal Responsabile per conto del Titolare dovranno essere conservati, nel rispetto della Data Retention *Policy* di [Società], per il tempo strettamente necessario alle finalità perseguite, come di seguito indicato:

Tipologie di interessato	Dettaglio sui Dati	Conservazione e Cancellazione
Vulnerability Assessment	I Report contenenti le vulnerabilità che riportano dati personali e ogni file di supporto	**Al termine dello specifico incarico**, il Responsabile è tenuto a restituire tutti i dati personali relativi al trattamento dei dati e le relative copie al Titolare e a distruggere tutti i dati personali, certificando al Titolare che lo ha fatto, a meno che la legislazione non gli impedisca di restituire o distruggere in tutto o in parte tali dati personali. In tal caso, per quanto riguarda i dati personali in questione, il Responsabile assicura che ne garantirà la riservatezza e non procederà più al loro trattamento.
Penetration Testing	I Report contenenti le vulnerabilità che riportano dati personali e ogni file di supporto	**Al termine dello specifico incarico**, il Responsabile è tenuto a restituire tutti i dati personali relativi al trattamento dei dati e le relative copie al Titolare e a distruggere tutti i dati personali, certificando al Titolare che lo ha fatto, a meno che la legislazione non gli impedisca di restituire o distruggere in tutto o in parte tali dati personali. In tal caso, per quanto riguarda i dati personali in questione, il Responsabile assicura che ne

		garantirà la riservatezza e non procederà più al loro trattamento.

Allegato B – Misure tecniche e organizzative di sicurezza specificate

Allegato B.1 – Misure di sicurezza specificate per le Postazioni di Lavoro mediante le quali è effettuato il trattamento di dati personali

#	Dominio	Controllo	Informazioni aggiuntive
1	**Meccanismi di identificazione e autenticazione**	Esistenza di meccanismi di accesso ai sistemi tramite il riconoscimento attraverso un nome utente e l'autenticazione attraverso password.	-
2	**Utilizzo utenze univoche e nominali**	Esistenza di utenze che siano associate in modo univoco a persone fisiche, identificabili con nome e cognome e/o riconducibili univocamente ad un unico soggetto responsabile	In caso di utenze Machine-To-Machine, è necessario attribuire le credenziali ad unico soggetto utilizzatore.
3	**Meccanismi di autorizzazione**	Implementazione di controlli che permettano di definire quali operazioni possa compiere uno specifico utente	L'autorizzazione è la fase successiva all'autenticazione degli utenti, dove vengono concessi (o negati) all'utente i privilegi di accesso ai sistemi informatici. I privilegi devono essere concessi in linea con i requisiti dettati nella politica di gestione degli accessi dell'organizzazione e nel rispetto dei principi di: - "Least Privilege": devono essere concessi all'utente esclusivamente i privilegi strettamente necessari a svolgere le attività per le quali è autorizzato; -"Need to Know": gli utenti devono essere autorizzati a trattare i soli dati essenziali allo svolgimento della loro mansione. La sussistenza dei requisiti di autorizzazione degli utenti deve essere verificata almeno semestralmente.
4	**Gestione utenze Privilegiate**	Implementazione di controlli specifici sulle utenze con privilegi ampi per impedire operazioni illecite	Devono essere previste procedure per l'attribuzione di privilegi di accesso "ampi" in base al ruolo e alle attività da eseguire sui sistemi
5	**Password policy conforme alle linee guida aziendali**	Insieme di regole che definiscono come dovrebbe essere costituita una password affinché possa essere ritenuta sufficientemente sicura; tale misura è associata alle utenze interne (non clienti).	I criteri di robustezza delle password includono: - lunghezza (almeno 8 caratteri) - frequenza di sostituzione adeguata (es. 90 gg) - presenza di: almeno da una lettera maiuscola, un numero e un carattere speciale - password history adeguata (es. ultime 5 password memorizzate) per evitare il riutilizzo di una stessa credenziale o, in alternativa, assicurare che le stesse credenziali non possano essere riutilizzate per un determinato lasso di tempo (e.g. sei mesi); - password differente dall'user_id associata o non "qwerty" o differente da alcune parole quali il nome della società. Per maggiori dettagli si rimanda all'allegato DdG n. 212/AD del 12 luglio 2016.
6	**Accesso logico terze parti**	L'accesso logico ai sistemi da parte di terzi (ad esempio clienti, fornitori, consulenti) deve essere soggetto a controlli rigorosi.	I requisiti per il controllo degli accessi logici ai sistemi comprendono: - autorizzare il personale prima che gli venga concesso l'accesso alle applicazioni dell'organizzazione; - assegnare specifici privilegi di accesso per accedere alle applicazioni o funzionalità di un'applicazione; - adottare opportuni meccanismi di controllo

#	Dominio	Controllo	Informazioni aggiuntive
			dell'accesso (ad esempio password, token o biometrico).
7	**Tracciamenti accessi utenti**	Registrazione e memorizzazione dei log degli accessi degli utenti (es. login, logout e principali attività utente, ad esempio download di dati, cancellazione di dati, modifiche massive dei dati)	Si specifica che si fa riferimento ai soli sistemi target (il tracciamento non riguarda le postazioni di lavoro/client)
8	**Tracciamento accessi Amministratori di Sistema**	Registrazione e memorizzazione dei log degli accessi degli Amministratori di Sistema (es. login, logout e principali attività utente, ad esempio download di dati, cancellazione di dati, modifiche massive dei dati)	Si specifica che si fa riferimento ai soli sistemi target (il tracciamento non riguarda le postazioni di lavoro/client)
9	**Protezione dei log**	Esistenza di meccanismi di protezione dei log in maniera da non poter essere cancellati da personale non autorizzato.	I log raccolti devono essere protetti da un uso improprio (ad esempio manomissione in transito, accesso/modifica/cancellazione non autorizzati). Esempi di misure di sicurezza dei log memorizzati in locale ("at rest") sono: - memorizzare o copiare i log su storage in sola lettura; - autorizzare, registrare e monitorare tutti gli accessi ai log; - implementare meccanismi di rilevamento delle manomissioni, in modo da sapere se un record del log è stato modificato o eliminato; - rivedere periodicamente i privilegi per l'accesso ai log. Esempi di misure di sicurezza dei log in transito sono: - se i log sono inviati su reti non attendibili (ad esempio Internet), utilizzare un protocollo di trasmissione sicuro/ cifrato (as esempio TLS); - Effettuare controlli di due diligence (normativi e di sicurezza) prima di inviare i log a terze parti.
10	**Retention dei log**	Esistenza di un limite temporale (almeno 6 mesi, al massimo 12 mesi) entro il quale possano essere conservati i log	- Almeno 6 mesi per gli Amministratori di Sistema (come da normativa di riferimento). - Il limite temporale è funzione di eventuali vincoli tecnologici presenti sul sistema
11	**Tracciamento degli Incident**	Registrazione e memorizzazione degli incidenti avvenuti/individuati	Esistenza di una procedura e strumenti a supporto che permettono di registrare e gestire eventuali fault occorsi, incidenti di sicurezza logica e fisica (es. accesso non autorizzato, furto/smarrimento ecc)
12	**Network Time Protocol (NTP)**	Configurazione del protocollo NTP al fine di sincronizzare il clock del sistema	Si specifica che la sincronizzazione deve avvenire con i sistemi del Cliente o con fonti attendibili pubbliche
13	**Hardening dei sistemi**	Implementazione di specifiche configurazioni su sistemi e componenti che permettono di incrementare la sicurezza di un sistema.	Linee Guida del Vendor/AGID
14	**Antivirus**	Adozione di strumenti di prevenzione e protezione da virus.	**-**

#	Dominio	Controllo	Informazioni aggiuntive
15	**Collezionamento eventi virus su piattaforma centralizzata**	Tutti gli eventi virus-related devono essere inviati ad una piattaforma centralizzata di collezionamento.	**-**
16	**Aggiornamento software anti-virus**	Il software anti-virus deve essere costantemente aggiornato.	-
17	**Patch Management**	Installazione di patch di sicurezza sui sistemi per risolvere le vulnerabilità presenti	-
18	**Patch Management tramite tool automatici**	Utilizzo di tool automatici per le attività di patch management.	-
19	**Back up periodico**	Effettuazione pianificata di copie di riserva finalizzata a duplicare, con una periodicità prestabilita, i dati, le configurazioni e le immagini di sistema su appositi supporti di memorizzazione.	- Definizione e conduzione di un processo automatico e/o operativo che garantisce l'esecuzione periodica dei backup - Le informazioni e i dati da copiare riguardano i dati memorizzati sui sistemi, i file di configurazione, ecc… - E' preferibile effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore. - Il backup deve essere effettuato almeno settimanalmente. - I dati e le informazioni presenti nelle copie di backup devono essere protetti con misure almeno pari a quelli dei dati originali
20	**Tecniche di cifratura**	Esistenza di tecniche di cifratura dei dati memorizzati (es. dati memorizzati nei database o nelle memorie di massa)	La cifratura deve essere utilizzata in tutta l'organizzazione al fine di: - proteggere la riservatezza delle informazioni sensibili o delle informazioni soggette a requisiti legali e normativi; - determinare se le informazioni critiche sono state alterate (ad esempio implementando funzioni hash o la firma digitale). Per maggiori dettagli fare riferimento alla relativa "Linea guida protezione postazioni di lavoro" emessa nel 2014 per quanto concerne le attività di cifratura del disco e delle memorie di massa.
21	**Cancellazione base (a livello software)**	Utilizzo di algoritmi e meccanismi generici per la cancellazione dei dati	Utilizzo di meccanismi quali ad esempio la sovrascrittura con una sequenza di zero, la formattazione.

Allegato B.2 – Misure di sicurezza specificate per eventuali strumenti mobile mediante le quali è effettuato il trattamento di dati personali

Non è ammesso il trattamento di dati personali mediante strumenti *mobile* (*smartphone, tablet*, etc.).

Allegato B.3 – Misure di sicurezza specificate sui dati personali trattati

Deve essere prevista la protezione del dato personale (anche se inclusa in report di VA/PT e di Digital Forensic) sia *at rest* sia in transito.

In particolare, è richiesto al Responsabile:

- cifratura dei Report e di eventuale documentazione di supporto in transito;
- cifratura di eventuali copie di back-up;
- cifratura dei supporti (hard disk, postazioni di lavoro, etc.) contenenti i Report;
- tecniche e protocolli per la protezione dei dati durante le attività di assessment (es. VPN);
- misure di sicurezza fisiche per controllare gli accessi che vengono effettuati ai locali nelle sedi del Responsabile in cui sono effettuati gli *assessment*;
- tutti i Report e l'eventuale documentazione di supporto deve essere oggetto di un processo di cancellazione e/o sovrascrittura sicuri (e.g, sovrascritture, *degausser*, DBAN *software*).

Allegato C – [da mantenere se ci sono sub-responsabili individuati] Elenco sub-responsabili