AVVISO

CONSULTAZIONE PRELIMINARE DI MERCATO

Oggetto

Consultazione preliminare di mercato indetta ai sensi degli artt. 77 e 78 del D. Lgs. n. 36/2023 per l'eventuale affidamento dei Servizi IaaS e PaaS in ambito Cloud e dei Servizi Specialistici di supporto tecnico-funzionale per la gestione, il monitoraggio e l'evoluzione delle infrastrutture digitali, gestita con sistemi telematici

I. PREMESSA

In applicazione dei principi di buona amministrazione, non discriminazione e trasparenza, **Ferservizi S.p.A.**, con sede in Piazza della Croce Rossa 1, 00161 Roma – capitale sociale Euro 8.170.000,00 partita IVA, Codice Fiscale e numero di iscrizione al Registro delle Imprese 04207001001, in nome e per conto di FSTechnology S.p.A. (di seguito anche "Stazione Appaltante" e/o "Ferservizi"), ha l'obiettivo di:

- garantire la massima pubblicità alle iniziative per assicurare la più ampia diffusione delle informazioni ed un celere svolgimento delle eventuali successive procedure di acquisto;
- ottenere la più proficua partecipazione da parte dei Cloud Service Provider (CSP) interessati a partecipare alla presente consultazione preliminare di mercato (di seguito anche "Consultazione");
- pubblicizzare al meglio le caratteristiche qualitative e tecniche dei servizi oggetto di Consultazione;
- ricevere, da parte dei soggetti interessati, osservazioni e suggerimenti per una più compiuta conoscenza del mercato;
- individuare le migliori soluzioni di mercato, con alto contenuto innovativo e forte impatto in termini di efficacia ed efficienza della soluzione proposta, di vantaggio o riduzione di impatti ambientali o sociali rivolti ai propri dipendenti, ai clienti o alla collettività.

Oggetto della presente Consultazione è l'affidamento dei Servizi IaaS e PaaS in ambito Cloud e dei Servizi Specialistici di supporto tecnico-funzionale per la gestione, il monitoraggio e l'evoluzione delle infrastrutture digitali, gestita con sistemi telematici (di seguito "Appalto"), rispetto al quale - previa presa visione dell'informativa sul trattamento dei dati personali pubblicata secondo le modalità di cui al successivo Paragrafo VII (Riserve e Precisazioni) - Vi chiediamo di fornire il Vostro contributo compilando il questionario allegato al presente Avviso di cui all'Allegato 1 e 1.1; il questionario dovrà essere inviato secondo i termini e le modalità indicate al successivo Paragrafo V.

Il Responsabile del presente procedimento è Denis Fusacchia.

II. SCOPO DELLA CONSULTAZIONE

La presente consultazione preliminare di mercato indetta ai sensi degli artt. 77 e 78 del D. Lgs. n. 36/2023 (di seguito "Codice"), ha la specifica finalità di raccogliere informazioni utili per la preparazione dell'Appalto ai fini del perfezionamento delle specifiche tecniche propedeutiche all'eventuale indizione di una successiva procedura di selezione da espletarsi ai sensi del D. Lgs. n. 36/2023 e s.m.i..

Pertanto, la presente Consultazione, è volta a:

- Rendere noti i requisiti minimi tecnico – funzionali richiesti per l'eventuale successivo futuro affidamento dell'Appalto di cui si ritiene necessario il possesso da parte dei CSP esperti dello specifico settore di mercato.

- agevolare la preparazione dell'Appalto, mediante la ricezione, da parte dei CSP che manifestino interesse a partecipare alla presente Consultazione, di contributi utili per il perfezionamento delle specifiche tecniche propedeutiche all'eventuale successiva indizione di una procedura di selezione da espletarsi ai sensi del D. Lgs. n. 36/2023 e s.m.i.;

- avviare un dialogo informale con i CSP partecipanti alla Consultazione, onde ricevere dai medesimi osservazioni, suggerimenti e informazioni circa ulteriori specifiche tecniche dell'Appalto.

III. DESCRIZIONE DELL'OGGETTO DELL'INIZIATIVA E REQUISITI MINIMI TECNICO – FUNZIONALI

La società FSTechnology S.p.A. del Gruppo FS ha avviato un progetto per l'affidamento dei Servizi IaaS e PaaS in ambito Cloud e dei Servizi Specialistici di supporto tecnico-funzionale per la gestione, il monitoraggio e l'evoluzione delle infrastrutture digitali, gestita con sistemi telematici.

Si rimanda agli Allegati 1, 1.1 e 2 al presente Avviso per la descrizione di dettaglio dei servizi oggetto della presente Consultazione e dei relativi requisiti tecnico-funzionali minimi richiesti che l'oggetto dell'Appalto dovrà soddisfare.

In particolare, sarà cura del CSP compilare il questionario riportato nel succitato Allegato 1 e 1.1.

IV. REQUISITI DI PARTECIPAZIONE

Si precisa che, ai fini della successiva eventuale procedura di selezione che potrà essere indetta per l'affidamento dei servizi oggetto della presente Consultazione, nonché per la stipula del relativo eventuale Accordo Quadro gli Operatori economici dovranno essere in possesso dei requisiti di ordine generale di cui agli artt. 94 e 95 del Codice.

Si evidenzia, inoltre, che la Stazione appaltante si riserva di non affidare appalti a quegli operatori economici che incorrano nell'ipotesi di cui all'art. 69 del Codice e di escludere i Concorrenti per i quali ritenga non sussistente adeguata affidabilità professionale, in presenza delle fattispecie di cui all'atto adottato e pubblicato ai sensi dell'art. 169 del Codice[1].

V. MODALITÀ DI PARTECIPAZIONE ALLA CONSULTAZIONE E TIPOLOGIA DI CONTRIBUTI AMMESSI

L'iniziativa è rivolta a tutti i CSP che siano in possesso di informazioni rilevanti per le finalità descritte nel presente Avviso e, pertanto, tutti i soggetti interessati a partecipare alla presente Consultazione

[1] L'atto di cui all'art. 169 del d.lgs. n. 36/2023 è pubblicato all'indirizzo internet: https://eprocurement.gruppofs.it/esop/tlk-host/public/fs/attach_it/regole_del_gruppo/atto_articolo_169_comma_1.pdf

potranno fornire contributi di carattere tecnico mediante la compilazione del questionario di cui al succitato Allegato 1 e 1.1.

Per partecipare alla Consultazione i CSP dovranno compilare il Modulo denominato "Manifestazione di Interesse alla Consultazione" di cui all'Allegato 1, e trasmetterla nelle modalità descritte al presente Paragrafo.

Ciascun CSP interessato dovrà - **preventivamente ed obbligatoriamente** - richiedere la registrazione al Portale Acquisti di Gruppo (di seguito, per brevità, "Portale" accessibile all'indirizzo **eprocurement.gruppofs.it**), ove non già in possesso di apposita utenza di accesso al Portale.

A tal fine dovranno seguire le istruzioni per la registrazione e l'abilitazione al Portale disponibili sulla *home page* del Portale medesimo (sezione "Istruzioni").

N.B. Si precisa che la firma digitale utilizzata dal Concorrente in detta fase di registrazione non ha alcuna valenza ai fini della sottoscrizione dei successivi documenti inerenti alla consultazione.

La registrazione al Portale è a titolo gratuito.

Tutte le comunicazioni e gli scambi di informazioni sono eseguiti tramite il Portale e, per quanto non previsto dal predetto Portale, mediante l'utilizzo del domicilio digitale o strumento analogo per gli operatori con sede legale fuori dall'Italia. In caso di necessità di supporto ai fini della registrazione al Portale, nonché nello svolgimento delle operazioni all'interno del Portale stesso, gli operatori interessati hanno facoltà di contattare il Servizio Assistenza ai riferimenti indicati nella Home Page del Portale. La partecipazione alla presente consultazione svolta in modalità telematica è aperta, previa identificazione, a tutti gli operatori interessati in possesso della dotazione informatica indicata nella sezione "Requisiti minimi HW e SW", accessibile dalla Home page del Portale, nonché di un indirizzo di Posta Elettronica Certificata (PEC) o strumento analogo per gli operatori con sede legale fuori dall'Italia.

È onere dell'operatore aggiornare tempestivamente nella propria cartella personale sul sito eprocurement.gruppofs.it qualsiasi variazione di indirizzo di posta elettronica certificata.

Eventuali modifiche dell'indirizzo PEC o problemi temporanei nell'utilizzo di tali forme di comunicazione, dovranno essere tempestivamente segnalate alla Stazione appaltante; diversamente la medesima declina ogni responsabilità per il tardivo o mancato recapito delle comunicazioni.

È obbligatorio il possesso da parte del legale rappresentante di un certificato di firma digitale, in corso di validità generato mediante un dispositivo per la creazione di una firma sicura, ai sensi di quanto previsto dall'art 38, comma 2, del D.P.R. n. 445/2000 e dall'art. 65 del D.lgs. n. 82/2005.

Sono ammessi certificati di firma digitale rilasciati da:

a) un organismo incluso nell'elenco pubblico dei certificatori tenuto dall'Agenzia per l'Italia Digitale previsto dall'art. 29 del D.lgs. 82/2005);

b) un certificatore operante in base ad una licenza od autorizzazione rilasciata da uno Stato membro dell'Unione Europea nel rispetto di quanto previsto dal Regolamento UE n. 910/2014[2].

Sono altresì ammessi, in conformità a quanto stabilito dall'art. 24 comma 4-ter del D.lgs. 82/2005, certificati di firma digitale rilasciati da un certificatore stabilito in uno Stato non facente parte dell'Unione europea, quando ricorre una delle seguenti condizioni:

a. il certificatore possiede i requisiti previsti dal Regolamento UE n. 910/2014 ed è qualificato in uno stato membro;

b. il certificato qualificato è garantito da un certificatore stabilito nella Unione Europea, in possesso dei requisiti di cui al medesimo Regolamento;

c. il certificato qualificato, o il certificatore, è riconosciuto in forza di un accordo bilaterale o multilaterale tra l'Unione europea e Paesi terzi o organizzazioni internazionali.

Sarà onere dell'Impresa indicare quale delle ipotesi sopra indicate sia applicabile all'autorità che le ha rilasciato la firma, allegandone documentazione a comprova, e indicare altresì lo strumento per mezzo del quale sarà possibile effettuare la verifica (software, link, ecc.).

La Stazione appaltante effettuerà la verifica della validità delle firme digitali utilizzando lo strumento automatico di verifica presente sul portale, e nel caso di verifica negativa una volta scaricato/i in locale il/i file, utilizzerà i software gratuiti messi a disposizione delle Certification Authority Italiane (come previsto dalle disposizioni normative in materia).
Pertanto, si suggerisce alle Imprese di effettuare, per i file firmati digitalmente, verifiche preventive con tali strumenti.
Per ciascun documento sottoscritto digitalmente il certificato di firma digitale dovrà essere valido alla data di inserimento del documento stesso a portale.

[2] La verifica della validità della firma digitale potrà essere effettuata direttamente sul sito web dell'Agenzia per l'Italia Digitale (http://www.agid.gov.it/) scaricando uno dei software elencati nella sezione Software di verifica delle Firme elettroniche (in particolar modo il DSS - Digital Signature Service disponibile anche in modalità WebApp) http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/firme-elettroniche/software-verifica.

È opportuno ricordare che un documento con firma digitale scaduta o revocata è valido solamente se al documento è associato un riferimento temporale opponibile ai terzi (marca temporale rilasciata da un certificatore iscritto nell'elenco pubblico dei certificatori) apposto durante il periodo di validità del certificato della firma.
Si precisa che i soli formati di firme digitali accettati saranno quelli di CADES e PADES (si veda nota 2).

***

MODALITÀ DI PRESENTAZIONE DELLA MANIFESTAZIONE DI INTERESSE

Al completamento delle operazioni di registrazione i CSP interessati per rispondere alla presente Consultazione dovranno:

- accedere al Portale (previa attivazione di apposita user ID, inserita in fase di registrazione, e password, ricevuta tramite comunicazione e-mail di sistema e modificabile in fase di accesso), nella sezione fasi di prequalifica (FDP) e poi cliccare su eventi ad evidenza pubblica;
- accedere all'Avviso telematico *de quo*;
- selezionare il tasto partecipa;
- (solo al primo accesso) cliccare su mia risposta, posto sulla sinistra della pagina web;
- (solo al primo accesso) cliccare sul link "Rispondi" (posizionato al centro dello schermo) per avviare il processo di risposta.

Ultimate tali operazioni i CSP potranno scaricare l'ulteriore documentazione relativa al presente avviso, porre chiarimenti, ricevere le risposte e presentare quanto necessario in risposta alla presente Consultazione.

Per redigere le relative dichiarazioni nonché per caricare l'eventuale documentazione a corredo il CSP dovrà, all'interno della Busta amministrativa digitale, allegare i documenti richiesti, sottoscritti con firma digitale.

Si precisa che tutti i file allegati al Portale (dichiarazioni e/o documenti scansionati) dovranno essere firmati digitalmente e non potranno essere superiori ai 10 Mb, pena il mancato controllo della firma digitale. Sul portale è presente uno strumento di verifica della firma digitale che è in grado di controllare la validità della firma se la dimensione del file è inferiore ai 10 MB.

Si ricorda che non è consentito firmare digitalmente una cartella compressa (es. zip) contenente uno o più documenti privi di firma digitale (laddove richiesta), ma è possibile allegare una cartella compressa contenente documenti digitalmente firmati.

Al termine dell'inserimento della documentazione richiesta, il CSP dovrà cliccare su "Salva ed Esci" per salvare quanto inserito e tornare alla propria pagina riepilogativa della fase di prequalifica.

Una volta espletate tali attività il CSP concorrente dovrà cliccare su *Trasmetti risposta*.

Il CSP potrà visualizzare nella sua cartella personale, alla colonna Stato della risposta, l'avvenuta trasmissione (Stato della risposta: *trasmessa*).

Il CSP potrà modificare i dati precedentemente trasmessi ovvero ritirare la propria risposta entro e non oltre la data e l'ora di scadenza di cui in seguito.

DOCUMENTI DA ALLEGARE

Gli Operatori economici interessati a partecipare alla presente Consultazione possono manifestare il proprio interesse inviando, sul Portale, **entro e non oltre il giorno 06/03/2026 ore 13:00** quanto segue:

a) Modulo denominato "Manifestazione di Interesse alla Consultazione", da rendere compilando il *facsimile* Allegato 1, firmato dal legale rappresentante del CSP che la rende;

b) Il questionario relativo al possesso dei requisiti di cui all'allegato 1.1 e al Capitolato Tecnico, specificando:

   a. Compilare il foglio "Requisito Minimo Fatturato" dell'allegato 1.1 e caricare la tabella risultante in un file formato PDF nel Portale Acquisti.
   b. In riferimento al paragrafo II. 1.1 "Requisiti Minimi o Distintivi Tecnici" e al paragrafo II 1.2 "Requisiti Minimi o Distintivi di Sicurezza" del Capitolato Tecnico, nella colonna F dell'allegato 1.1 – Foglio "Requisiti Minimi Obbligatori" e foglio "Requisiti Minimi Migliorativi" indicare il possesso o meno del requisito (Si/No), alla colonna G "note" inserire link a documentazione pubblica consultabile a conferma di quanto indicato ed ulteriori informazioni qualora ritenuto necessario. La tabella risultante dalla compilazione dell'Excel di cui sopra, costituirà l'allegato alla relazione tecnica di cui al par. "II. 1.5 Modalità Di Risposta" del Capitolato Tecnico e dovrà essere allegata nel Portale Acquisti in un unico PDF comprendente il punto "c".

c. In riferimento al paragrafo II. 1.3 "Requisiti Valutativi Tecnici A Carattere Qualitativo" e al paragrafo II 1.4 "Requisiti Valutativi Di Sicurezza A Carattere Qualitativo", seguire le linee guida di cui al par. "II. 1.5 Modalità Di Risposta", presentando un file word di 40 pagine così ripartite: 25 pagine (A4) per i requisiti valutativi tecnici a carattere qualitativo e ulteriori 15 pagine (A4) per i requisiti valutativi di sicurezza a carattere qualitativo – Copertina, indice e allegati esclusi;
d. In riferimento ai "Use Case e Scenari Di Migrazione Cloud", di cui al paragrafo II. 2 del Capitolato tecnico, seguire le linee guida disposte nella sezione "II. 2.5 Modalità di Risposta", disponendo un file word in italiano con lunghezza massima pari a 4 pagine (A4) per Use Case (Copertina e indice esclusi), per un totale di massimo 20 pagine;
e. In riferimento alle figure professionali di cui al paragrafo II. 3 "Profili Professionali", seguire le linee guida disposte nella sezione "II. 3.7 Modalità di Risposta", condividendo per ciascuna figura professionale n.1 pagina di copertina, riportante il numero delle figure professionali richieste operanti su Territorio e condividendo per ciascuna figura professionale richiesta i Curriculum Vitae dei professionisti in formato Europass o equivalente. Il CV per essere preso in considerazione e conteggiato dovrà rispondere a tutti i requisiti richiesti (Certificazione IT - Certificazione Lingua Inglese - Anzianità lavorativa - Comprovata esperienza nella specifica funzione - Istruzione). Per ogni figura dovrà essere presentato – a comprova – un archivio zip al cui interno dovranno essere riportate le certificazioni previste nel Capitolato Tecnico. Tutti gli zip di tutti i profili professionali dovranno essere compressi in un unico file zip per figura professionale e dovrà essere allegato nel Portale Acquisti alla sezione "allegati generici". Dovranno inoltre essere compilate le colonne E, F e G dell'allegato 1.1 – foglio "Figure Professionali"; la tabella risultante dalla compilazione dell'Excel dovrà essere allegata nel Portale Acquisti come file PDF digitalmente firmato.
f. In riferimento al paragrafo II. 4 "Catalogo Servizi Cloud" del Capitolato Tecnico, seguendo le linee guida disposte al paragrafo "II 4.1 Modalità di Risposta", compilare la colonna E dell'allegato 1.1 - Foglio "Catalogo" indicando la Metrica di Consuntivazione (es. €/mese o €/TB/mese) e nella colonna F le informazioni relative ad eventuali tool a supporto dell'operatività. È possibile fornire ulteriori eventuali informazioni a riguardo dei Tool, in un file word, la cui lunghezza massima è di 5 pagine. È inoltre possibile ampliare il catalogo con ulteriori items a cura del CSP. La

tabella risultante dalla compilazione dell'Excel di cui sopra dovrà essere allegata nel Portale Acquisti come file PDF digitalmente firmato. L'eventuale allegato word riguardante i Tool andrà allegato separatamente anch'esso nel Portale Acquisti. **Non sono ammesse offerte economiche**;

g. In riferimento ai "criteri di sostenibilità" di cui al paragrafo II. 5 "Criteri Di Sostenibilità", seguire le linee guide disposte nella sezione "II. 5.1 Modalità Di Risposta", predisponendo un file word, in cui il CSP dovrà fornire apposita dichiarazione resa ai sensi del D.P.R. 445/2000 e s.m.i. e sottoscritta digitalmente dal proprio legale rappresentante o procuratore, includendo l'elenco totale o parziale delle certificazioni richieste possedute.

N.B. Tutta la documentazione deve essere redatta in **lingua italiana**. In caso contrario, tutta la documentazione deve essere accompagnata da traduzione in lingua italiana certificata "conforme al testo straniero" dalla competente rappresentanza diplomatica o consolare ovvero da un traduttore ufficiale.

N.B. Saranno valutati esclusivamente i CSP che dimostrino di avere un'offerta public cloud (IaaS+PaaS) disponibile da almeno tre anni. Tale offerta deve aver generato almeno 500 milioni di usd di fatturato nell'anno solare 2024 (fatturato proveniente direttamente dalle vendite dell'offerta, esclusi i servizi gestiti e professionali), ed almeno 125 milioni di usd di fatturato deve essere proveniente da paesi diversi da quello di origine del CSP.

Tutti i file allegati al Portale (dichiarazioni e/o documenti scansionati) dovranno essere firmati digitalmente dal rappresentante legale dell'Operatore economico partecipante o procuratore munito di appositi poteri.

N.B. Alla manifestazione di interesse alla Consultazione NON dovrà essere allegata alcuna offerta economica, né elementi di costo.

L'invio telematico della manifestazione di interesse alla Consultazione è a totale ed esclusivo rischio del mittente, restando esclusa qualsivoglia responsabilità di Ferservizi, ove, per qualsiasi malfunzionamento alla struttura tecnica, tecnologia o di connessione dell'Operatore economico, la stessa non pervenga entro il termine di scadenza e secondo le modalità previste. Si invitano pertanto i CSP interessati ad avviare le attività finalizzate alla trasmissione di quanto richiesto con largo anticipo rispetto alla scadenza prevista onde evitare la non completa e quindi mancata trasmissione della risposta decorso tale termine.

N.B.: Qualora sia accertata la mancanza, l'incompletezza o l'irregolarità essenziale della documentazione presentata, si procederà alla richiesta di integrazione o di regolarizzazione di detta documentazione.

VI. MODALITÀ DI SVOLGIMENTO DELLA CONSULTAZIONE PRELIMINARE DI MERCATO

La Consultazione potrà svolgersi in fasi successive. I CSP sono invitati a prendere visione della documentazione allegata al presente avviso.

Le manifestazioni di interesse ricevute saranno raccolte e analizzate dalla Stazione Appaltante, ivi inclusa tutta la documentazione prodotta dai CSP in riscontro alla presente Consultazione.

In base alle risultanze delle attività di analisi condotte ed al fine di acquisire tutte le informazioni e documentazioni utili per la migliore preparazione dell'Appalto ai fini della successiva eventuale indizione della relativa procedura di selezione, Ferservizi potrà eventualmente procedere ad invitare i CSP che hanno presentato manifestazione di interesse ad uno o più incontri di approfondimento tecnico. Tali incontri saranno oggetto di apposita verbalizzazione.

Per ogni fase di svolgimento della Consultazione, i CSP partecipanti riceveranno apposita comunicazione (a mezzo di pubblicazione di avvisi sul Portale e/o sul profilo committente).

Al termine della Consultazione, Ferservizi pubblicherà sul Portale e sul Profilo committente apposito avviso di chiusura della consultazione preliminare di mercato.

VII. RISERVE E PRECISAZIONI

La partecipazione alla presente Consultazione preliminare di mercato non dà diritto ad alcun compenso e/o rimborso per le spese sostenute, deve pertanto intendersi a titolo completamente gratuito.

Il presente Avviso, in quanto costituente avvio di una mera consultazione preliminare di mercato, non è vincolante e non è finalizzato all'aggiudicazione e stipula di alcun contratto, pertanto, la presente Consultazione non comporta alcun obbligo per Ferservizi di avviare procedure di selezione del contraente per le prestazioni oggetto dell'iniziativa.

La partecipazione alla consultazione preliminare di mercato:

- è ininfluente (ossia: non assicura e non preclude) rispetto alla partecipazione alla eventuale successiva procedura di selezione per l'affidamento dell'Appalto, non costituendo condizione di accesso, né titolo preferenziale, né impegno alcuno circa il prosieguo della procedura;
- non potrà, in alcun modo, ostacolare altri CSP che non abbiano partecipato alla Consultazione avviata con il presente avviso;
- non determina alcuna aspettativa nei confronti di Ferservizi ed i CSP non possono rivendicare alcun diritto al riguardo;
- Lo schema di Accordo Quadro allegato 3 è presentato a mero titolo informativo.

Tutte le informazioni da Voi fornite in riscontro al presente documento saranno utilizzate ai soli fini dello sviluppo dell'iniziativa in oggetto e non dovranno costituire offerte tecniche o economiche; a tal fine i contributi trasmessi non dovranno fornire anticipazioni in merito alle quotazioni afferenti i servizi oggetto della presente Consultazione, al fine di non alterare il regolare sviluppo competitivo della successiva eventuale fase di selezione.

Pertanto, tutta la documentazione raccolta potrà essere utilizzata per la predisposizione della documentazione dell'eventuale successiva procedura di selezione per l'affidamento dell'Appalto, nei limiti del rispetto dei diritti di privativa e della proprietà intellettuale, di non discriminazione e di trasparenza.

Per tale motivo, in ottemperanza all'art. 78 del Codice, al fine di garantire il rispetto del principio dell'effettiva concorrenza, Ferservizi potrà comunicare agli altri candidati e offerenti nell'ambito dell'eventuale successiva procedura di selezione, le informazioni pertinenti, scambiate nel quadro della presente Consultazione.

Ciò premesso, si invita a non inviare informazioni che contengano informazioni e/o dati protetti da diritti di privativa o da diritti di proprietà intellettuale, comunque, rilevatori di segreti aziendali, commerciali, tecnici o industriali, ovvero di inviare motivata e comprovata dichiarazione per la parte delle informazioni e/o documentazioni inviate per le quali si richiede la non divulgazione.

Si precisa, in vista dell'eventuale accesso da parte di altri CSP agli esiti della presente Consultazione, che la divulgazione di quanto contenuto nei Vostri contributi avverrà in forma anonima.

Resta ferma la facoltà di Ferservizi di interrompere, modificare, prorogare, sospendere e revocare la procedura in qualsiasi momento, senza che ciò possa costituire, in alcun modo, diritto o pretesa a qualsivoglia risarcimento o indennizzo.

La consultazione sarà espletata nel rispetto dei principi e degli obblighi imposti dal Codice Etico, dalla Policy Anti-Corruption del Gruppo Ferrovie dello Stato Italiane, dagli strumenti di compliance antitrust che costituiscono parte integrante del Programma di Compliance Antitrust del Gruppo Ferrovie dello Stato Italiane, dal Modello di Organizzazione Gestione e Controllo ex D.lgs. n. 231/2001 e s.m.i. ("Modello 231") di FSTechnology S.p.A. disponibili sul sito web societario e/o di Ferrovie dello Stato Italiane, che possono essere scaricati e stampati e di cui l'Operatore potrà chiedere in ogni momento copia cartacea, nonché dalle Condizioni Generali di Contratto disponibili al seguente link https://eprocurement.gruppofs.it/esop/tlk-host/public/fs/web/regole_del_gruppo.html.

TRATTAMENTO DEI DATI PERSONALI

Le Parti (Ferservizi, FSTechnology S.p.A. e ciascun CSP) si impegnano a trattare i dati personali, acquisiti nell'ambito e per le finalità connesse alla presente Consultazione, nel rispetto della normativa vigente in materia di protezione dei dati personali (Regolamento UE 2016/679 e dal D. Lgs. n. 196/2003 e s.m.i.), in particolare con riferimento ai principi di liceità, necessità, minimizzazione e limitazione, nonché a garantirne l'integrità e la riservatezza.

Ciascuna Parte risponde delle contestazioni, azioni o pretese avanzate da parte degli interessati e/o di qualsiasi altro soggetto e/o Autorità in merito alla inosservanza alla normativa vigente in materia di protezione dei dati personali (Regolamento UE 2016/679 e dal D.Lgs. 196/2003 e s.m.i), ad essa ascrivibili.

Nell'ambito delle attività connesse alla presente Consultazione, le Parti prendono atto e concordano che tratteranno i dati personali relativi a qualsiasi persona fisica che agisca per loro conto (dipendenti e/o Terze Parti delle Società), in conformità con la relativa informativa sul trattamento dei dati personali resa e disponibile attraverso i rispettivi canali aziendali.

Il predetto obbligo di informativa verso le Terze Parti viene assolto da Ferservizi, mediante pubblicazione nella sezione "Protezione dati personali" del sito istituzionale all'indirizzo https://www.ferservizi.it/it/protezione-dati-personali.html e nel "Portale Acquisti" all'indirizzo https://eprocurement.gruppofs.it/esop/tlk-host/public/fs/web/informativa_privacy.html

L'obbligo di informativa è inoltre assolto dalle Società del Gruppo FS Italiane rispettivamente Titolari autonomi del trattamento mediante pubblicazione sui rispettivi siti istituzionali.

Dichiarano, inoltre, espressamente di aver debitamente informato i propri dipendenti e/o Terze Parti ai sensi degli artt. 13 e 14 del Regolamento EU 679/2016.

VIII. PUBBLICITÀ

Il presente avviso e i relativi allegati sono pubblicati sul Portale Acquisti raggiungibile al sito https://eprocurement.gruppofs.it/esop/tlk-host/public/fs/web/home.html nonché sul profilo del committente all'indirizzo www.gare.ferservizi.it/, nella sezione "Bandi" – FSTechnology – Forniture".

Al termine della Consultazione, Ferservizi pubblicherà sul Portale e sul Profilo committente apposito avviso di chiusura della consultazione preliminare di mercato.

Si allegano:

Allegato 1: Manifestazione di Interesse alla Consultazione;
Allegato 1.1: Questionario;
Allegato 2: Capitolato Tecnico;
Allegato 3: Schema di Accordo Quadro.

Sourcing & Procurement Services

Il Responsabile

ANTONIO CAPPIELLO

Firmato da Antonio Cappiello
Data: il 18/02/2026 alle 19:29:12 CET

Allegato 1

Manifestazione di Interesse alla consultazione

(Dichiarazione resa ai sensi e per gli effetti di cui agli artt. 46 e 47 del D.P.R. 445/2000 e s.m.i., ovvero, per gli Operatori economici stabiliti in stati diversi dall'Italia, documentazione equivalente secondo la legislazione dello stato di appartenenza e, comunque, nel rispetto di quanto previsto nell'art. 3, commi 2, 3 e 4 del D.P.R. n.445/2000 e s.m.i., e laddove applicabile, nel rispetto di quanto previsto nell'art, 33 del medesimo decreto.)

NOTE DI COMPILAZIONE: si invita a compilare le caselle in grigio. Il documento dovrà essere sottoscritto digitalmente, pertanto non è necessario apporre timbro e firma autografa.

Oggetto: Manifestazione di Interesse alla Consultazione preliminare di mercato indetta ai sensi degli artt. 77 e 78 del D.lgs. n. 36/2023 per l'eventuale affidamento dei Servizi IaaS e PaaS in ambito Cloud e dei Servizi Specialistici di supporto tecnico-funzionale per la gestione, il monitoraggio e l'evoluzione delle infrastrutture digitali, gestita con sistemi telematici.

Il/la sottoscritto/a					
Nato/a a		**Prov.**	**( )**	**il**	**/ / **
C.F.					
In qualità di:					
ovvero					
☐	**Procuratore (*in tal caso indicare gli estremi della relativa procura*)**				
della Società (indicare Ragione Sociale per esteso):					
C.F		**P.IVA**			
con sede legale in:					
Via				**n°**	
C.A.P.		**Città**		**Prov.**	**( )**
Telefono		**Fax**		**e-mail**	

MANIFESTA

il proprio interesse relativamente alla consultazione preliminare di mercato in oggetto per le finalità indicate al Paragrafo II dell'Avviso di Consultazione preliminare di mercato.

A tal fine, **consapevole, *ai sensi e per gli effetti dell'art.76 del d.P.R. 28 dicembre 2000, n. 445 e s.m.i., delle responsabilità e delle sanzioni previste in caso di dichiarazioni mendaci e/o formazione o uso di atti falsi, nonché in caso di esibizione di atti contenenti dati non più corrispondenti a verità e consapevole che qualora emerga la non veridicità del contenuto della presente dichiarazione decadrà dai benefici per i quali la stessa è rilasciata.***

AI SENSI DEGLI ARTT. 46 E 47 DEL D.P.R. 445/2000

DICHIARA SOTTO LA PROPRIA RESPONSABILITA'

Sezione I

- di aver preso piena conoscenza e di accettare integralmente il contenuto dell'Avviso di consultazione di mercato e degli eventuali chiarimenti resi;
- che l'Impresa è iscritta nel registro della Camera di Commercio, Industria, Artigianato e Agricoltura (o ad altro organismo equipollente secondo la legislazione dello Stato di appartenenza) per attività inerente all'oggetto delle prestazioni da affidare;
- di essere consapevole che, in sede di partecipazione all'eventuale procedura di selezione, all'atto di presentazione dell'offerta, l'Impresa dovrà attestare il possesso dei requisiti di ordine generale di cui agli artt. 94 e 95 del D.lgs. 36/2023 nonchè l'assenza dei motivi di esclusione di cui all'art. 69 e di cui all'atto adottato e pubblicato dalla Stazione Appaltante ai sensi dell'art. 169 del Codice[1].

Sezione II – Questionario / Generale Tecnico

- Seguire le linee guida della sezione "Documenti da allegare" del Paragrafo V. "Modalità Di Partecipazione Alla Consultazione E Tipologia Di Contributi Ammessi" dell'avviso di consultazione di mercato e compilare contestualmente l'Excel allegato 1.1 – "questionario".

Inoltre, **DICHIARA:**

[1] L'atto di cui all'art. 169 del d.lgs. n. 36/2023 è pubblicato all'indirizzo internet: https://eprocurement.gruppofs.it/esop/tlk-host/public/fs/attach_it/regole_del_gruppo/atto_articolo_169_comma_1.pdf

A. di accettare che la presente Consultazione preliminare di mercato non dà diritto ad alcun compenso e/o rimborso per le spese sostenute, e che pertanto, ogni contributo viene reso a titolo completamente gratuito;

B. di accettare integralmente, senza condizione o riserva alcuna, che l'Avviso in riferimento, in quanto costituente avvio di una mera consultazione preliminare di mercato, non è vincolante e non è finalizzato all'aggiudicazione e stipula di alcun contratto, pertanto, la Consultazione non comporta alcun obbligo per Ferservizi di avviare procedure di selezione del contraente per le prestazioni oggetto dell'iniziativa. L'operatore economico, pertanto prende atto e accetta che:

    1. la partecipazione alla consultazione preliminare di mercato è ininfluente (ossia: non assicura e non preclude) rispetto alla partecipazione alla eventuale successiva procedura di selezione per l'eventuale affidamento dell'Appalto, non costituendo condizione di accesso, né titolo preferenziale, né impegno alcuno circa il prosieguo della procedura;

    2. non potrà, in alcun modo, ostacolare altri Operatori economici che non abbiano partecipato alla Consultazione avviata con il presente avviso;

    3. non determina alcuna aspettativa nei confronti di Ferservizi e gli Operatori economici non possono rivendicare alcun diritto al riguardo.

C. di accettare integralmente, senza condizione o riserva alcuna, che i contributi dallo stesso forniti potranno essere utilizzati per la predisposizione della documentazione dell'eventuale successiva procedura di selezione per l'affidamento dell'Appalto, nei limiti del rispetto dei diritti di privativa e della proprietà intellettuale[2], di non discriminazione e di trasparenza;

D. di accettare integralmente, senza condizione o riserva alcuna, che Ferservizi ha la più ampia facoltà di interrompere, modificare, prorogare, sospendere e revocare la procedura in qualsiasi momento, senza che ciò possa costituire, in alcun modo, diritto o pretesa a qualsivoglia risarcimento o indennizzo;

E. di aver preso visione del Codice Etico, della Policy Anti-Corruption del Gruppo Ferrovie dello Stato Italiane, degli strumenti di compliance antitrust che costituiscono parte integrante del Programma di Compliance Antitrust del Gruppo Ferrovie dello Stato Italiane, il Modello di Organizzazione Gestione e Controllo ex D.lgs. n. 231/2001 e s.m.i. ("Modello 231") di FSTechnology S.p.A. disponibili sul sito web societario e/o di Ferrovie dello Stato Italiane, che possono essere scaricati e stampati e di cui l'Operatore potrà chiedere in ogni momento copia cartacea, nonché delle Condizioni Generali di

[2] Si invita l'operatore economico a non inviare informazioni che contengano informazioni e/o dati protetti da diritti di privativa o da diritti di proprietà intellettuale comunque rilevatori di segreti aziendali, commerciali, tecnici o industriali, ovvero di inviare, parallelamente alla presente dichiarazione, motivata e comprovata dichiarazione per la parte delle informazioni e/o documentazioni per le quali si richiede la non divulgazione.

Contratto disponibili al seguente link https://eprocurement.gruppofs.it/esop/tlk-host/public/fs/web/regole_del_gruppo.html;

Il sottoscritto, in vista dell'eventuale accesso da parte di altri Operatori economici agli esiti della presente Consultazione, accetta espressamente che la divulgazione di quanto contenuto nei contributi forniti avverrà in forma anonima.

Il sottoscritto rende la presente dichiarazione sotto la propria responsabilità, consapevole delle sanzioni previste dalla legge a carico di chi attesta il falso e dichiara di essere informato che i dati personali raccolti saranno trattati in conformità con il Regolamento UE 2016/679, anche con strumenti informatici, esclusivamente nell'ambito del procedimento per il quale la presente dichiarazione viene resa.

A U T O R I Z Z A

Ferservizi S.p.A. ad inviare le comunicazioni inerenti la presente procedura, ai contatti indicati al momento della registrazione sul Portale Acquisti di Gruppo, al sito https://eprocurement.gruppofs.it/esop/tlk-host/public/fs/web/home.html

Luogo		Data	
Letto, confermato e sottoscritto			

*** NB: Le dichiarazioni dovranno essere firmate digitalmente dal legale rappresentante o procuratore munito di appositi poteri.**

Allegato 1.1. - Schema di Risposta Questionario affidamento dei Servizi IaaS e PaaS in ambito Cloud e dei Servizi Specialistici di supporto tecnico-funzionale per la gestione, il monitoraggio e l'evoluzione delle infrastrutture digitali, gestita con sistemi telematici

Seguire le istruzioni di cui al V. dell'Avviso Consultazione Preliminare di Mercato

REQUISITO MINIMO FATTURATO	
REQUISITO OBBLIGATORIO	**DICHIARAZIONE DI POSSESSO**
Da quanti anni è disponibile l'offerta public cloud (IaaS+PaaS)?	
Quanti usd di fatturato nell'anno solare 2024 ha generato l'offerta? (fatturato proveniente direttamente dalle vendite dell'offerta, esclusi i servizi gestiti e professionali)	
Quanti usd di fatturato per l'offerta sono proveniente da paesi diversi da quello di origine del CSP?	

REQUISITI MINIMI O DISTINTIVI TECNICI - OBBLIGATORI - di cui par. 1.1 del Capitolato Tecnico					
ID - Capitolato Tecnico	**Ambito**	**Descrizione**	**Tipologia**	**Dichiarazione di Possesso**	**Note**
R1	Governance	Chiarisce ruoli e responsabilità tra provider e cliente nella gestione della sicurezza	Obbligatorio		
R2	Infrastruttura	Presenza di almeno due regioni all'interno dell'Unione Europea, di cui una almeno una in territorio italiano	Obbligatorio		
R3	Affidabilità	Garanzia di SLA per servizi IaaS e PaaS (calcolo, storage, database)	Obbligatorio		
R4	Prestazioni	Capacità della piattaforma di scalare orizzontalmente e verticalmente	Obbligatorio		
R5	Localizzazione	Presenza di regioni cloud fisicamente localizzate nell'UE/SEE	Obbligatorio		
R6	Localizzazione	Possibilità di vincolare l'erogazione dei servizi alla sola UE	Obbligatorio		
R7	Data Acquisition & Ingestion – Big Data	La capacità si riferisce al processo attraverso cui grandi volumi di dati, provenienti da fonti eterogenee, vengono raccolti, trasferiti e preparati per essere archiviati ed elaborati in sistemi come Data Lake o Data Warehouse.	Obbligatorio		
R9	Data Acquisition & Ingestion – Streaming	Questa capacità consente l'estrazione, l'ingestione e l'elaborazione continua dei dati come flussi di eventi in tempo reale, incluse le integrazioni di flusso, e li fornisce ai sistemi di destinazione per un consumo immediato.	Obbligatorio		
R11	Data Acquisition & Ingestion – ETL/ELT	Il principio si riferisce alle seguenti due capacity: 1. Batch capacity: capacità di elaborare grandi volumi di dati a intervalli regolari; 2. Micro–batch capacity: capacità di elaborare piccoli volumi di dati in modo frequente, con tempi di aggiornamento molto più rapidi.	Obbligatorio		
R13	Storage & Processing – Data Lakehouse	Lo storage gestisce la varietà e il volume di dati di strutture variabili attraverso un'ampia gamma di carichi di lavoro analitici che spaziano dall'analisi tradizionale alla data science. I dati possono essere fisicamente distribuiti.	Obbligatorio		
R16	Storage & Processing – Query Engine	Il Query Engine è il componente della Data Platform che gestisce e ottimizza l'esecuzione delle interrogazioni sui dati. Deve essere in grado di accedere, leggere e analizzare i dati in modo efficiente	Obbligatorio		
R19	Storage & Processing – Stream Processing	Questa capacità gestisce dati che vengono scritti ad alta frequenza e volume. Le query vengono eseguite in tempo reale sia per la valutazione dei dati rispetto ai modelli, sia per la sintesi degli eventi. I dati sono misti per struttura e dimensione.	Obbligatorio		
R21	Storage & Processing – Data Lake	Archivio centralizzato che permette di raccogliere, memorizzare e gestire grandi volumi di dati eterogenei (strutturati, semi–strutturati e non strutturati), così come sono, senza necessità di trasformarli immediatamente.	Obbligatorio		
R24	Storage & Processing – Data Transformation	Questa capacità rappresenta il processo mediante il quale i dati vengono convertiti, puliti e ristrutturati per essere resi coerenti, affidabili e utilizzabili nei sistemi di analisi o integrazione. Comprende operazioni come la normalizzazione dei formati, la conversione dei tipi di dato, la rimozione dei duplicati, l'arricchimento con informazioni aggiuntive e l'applicazione di regole di business.	Obbligatorio		
R26	Storage & Processing – Data Warehouse	Sistema centralizzato che raccoglie dati strutturati da diverse fonti, li integra e li organizza per supportare analisi, reporting e business intelligence. È ottimizzato per query complesse, conserva dati storici e permette di ottenere rapidamente insight utili per le decisioni aziendali.	Obbligatorio		
R28	Digital & Transformation – AI Tools	Capacità della piattaforma di offrire un ecosistema integrato di strumenti e servizi di AI–as–a– Service, abilitando lo sviluppo, la sperimentazione e la gestione collaborativa di soluzioni di intelligenza artificiale.	Obbligatorio		
R31	Digital & Transformation – Gen AI	Capacità della piattaforma di abilitare, integrare e rendere operativi servizi di intelligenza artificiale generativa.	Obbligatorio		
R35	Digital & Transformation – Model Training	Capacità della piattaforma di abilitare, orchestrare e ottimizzare l'intero ciclo di vita dell'addestramento dei modelli di machine learning, garantendo un'integrazione fluida tra preparazione dei dati, training, tuning, versioning e monitoraggio delle performance.	Obbligatorio		
R37	Digital & Transformation – Model Deployment	La capacità della piattaforma di gestire in modo scalabile, sicuro e governato la messa in produzione dei modelli di intelligenza artificiale, garantendo continuità operativa e osservabilità.	Obbligatorio		

R39	Data & AI Serve – AI Real Time Endpoints	La capacità di esporre modelli di AI/ML come endpoint scalabili, sicuri e a bassa latenza per l'inferenza in tempo reale.	Obbligatorio		
R41	Data & AI Serve API	La capacità API (ApplicationProgramming Interface) rappresenta un insieme di regole, protocolli e strumenti che permettono a diversi software di comunicare tra loro.	Obbligatorio		
R43	Data & AI Serve – Containerization	Supporto per la distribuzione e l'esecuzione di carichi di lavoro containerizzati.	Obbligatorio		
R45	Data & AI Serve – SQL Access	Capacità della piattaforma proposta di fornire un accesso standardizzato, affidabile ed efficiente ai dati relazionali tramite SQL (Structured Query Language), in conformità con gli standard internazionali. Questa capacità assicura che il sistema possa offrire funzionalità di interrogazione, gestione e sicurezza dei dati strutturati, nel rispetto delle esigenze di scalabilità aziendale, interoperabilità e conformità.	Obbligatorio		
R48	Visualization – Dashboarding	Supporto per dashboard altamente interattive e per l'esplorazione dei dati attraverso la manipolazione visiva dei grafici. La capacità di visualizzazioni interattive dei dati, incluse tabelle, grafici e testo in linguaggio naturale, si organizza intorno ad aree tematiche logiche per comunicare una data story.	Obbligatorio		
R51	Visualization – Geospatial Analysis	La capacità di costruire mappe, grafici, statistiche e cartogrammi a partire da dati geospaziali per rivelare pattern e relazioni.	Obbligatorio		
R53	Visualization – Self Service BI	Questa capacità consente agli utenti di connettersi ai dati, produrre e condividere analisi senza dipendere dall'IT per l'operatività delle analisi.	Obbligatorio		
R55	Integration – Data Orchestration	La gestione aumentata dei dati utilizza il machine learning e l'intelligenza artificiale per automatizzare attività come la qualità dei dati, l'integrazione, la preparazione, la catalogazione, la gestione dei carichi di lavoro, la scoperta di insight e la condivisione. Applica la significatività statistica e il contesto aziendale per migliorare le attività umane e supportare ruoli come i citizen integrator e i citizen data scientist. Nelle architetture moderne, è essenziale per gestire rapidamente grandi volumi di dati multistrutturati, spostando le pratiche da un design personalizzato verso data fabric guidati dai metadati e assistiti dall'intelligenza artificiale.	Obbligatorio		

REQUISITI MINIMI O DISTINTIVI DI SICUREZZA - OBBLIGATORI - di cui par. 1.2 del Capitolato Tecnico

ID - Capitolato Tecnico	Ambito	Descrizione	Tipologia	Dichiarazione di Possesso	Note
RCY.1	Governance e Compliance (GOV)	Il CSP deve porre in essere tutti i controlli e le misure tecnologiche ed organizzative necessarie a garantire un adeguato livello di sicurezza logica a tutto il dominio dei sistemi, servizi, dati e informazioni del Cliente.	Obbligatorio		
RCY.2	Governance e Compliance (GOV)	È fatto richiamo al CSP nell'utilizzo di un comportamento etico e riservato in tutta la filiera della gestione delle informazioni del Cliente con cui verrà in contatto e di cui dovrà salvaguardare l'integrità e la disponibilità per il proprio mandato o per autorizzazione diretta del Cliente.	Obbligatorio		
RCY.3	Governance e Compliance (GOV)	Il CSP dovrà garantire che il modello di gestione della sicurezza, le architetture e le tecnologie impiegate per l'erogazione del servizio siano soggetti a un'evoluzione continua, in linea con gli standard di sicurezza, le normative vigenti e le best practice di settore, al fine di garantire un livello adeguato di protezione nel tempo.	Obbligatorio		
RCY.4	Governance e Compliance (GOV)	I datacenter e le informazioni/servizi in Cloud devono risiedere su territorio nazionale o all'interno dello Spazio Economico Europeo.	Obbligatorio		
RCY.5	Governance e Compliance (GOV)	Il CSP dovrà garantire la possibilità a Ferrovie dello Stato di effettuare audit, ispezioni, verifiche di sicurezza e monitoraggi con proprio personale o tramite società terze, per verificare la rispondenza di quanto prescritto a quanto eseguito, garantendo il sostegno e la collaborazione adeguata e necessaria allo svolgimento delle attività di audit e verifica.	Obbligatorio		

RCY.6	Governance e Compliance (GOV)	Il CSP si impegna a garantire il rispetto di tutti gli standard normativi e le prescrizioni operative previste dalla Direttiva NIS 2, adeguando la fornitura per tutta la durata del contratto. A tal fine, dovrà assicurare la piena conformità alla normativa vigente, in particolare: - le misure di sicurezza stabilite all'allegato B del Decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81, di cui all'articolo 1, comma 2, lettera b), del Decreto-Legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla Legge 18 novembre 2019, n. 133; - le misure di sicurezza di base previste nell'Allegato 2 della Determinazione dell'Agenzia per la Cybersicurezza Nazionale n. 164179 del 14 aprile 2025, attuativa del Decreto Legislativo 4 settembre 2024, n. 138 (cd. "Decreto NIS"); - gli elementi essenziali di cybersicurezza dei beni e dei servizi informatici di cui all'Allegato 1 del Decreto del Presidente del Consiglio dei Ministri 30 aprile 2025, attuativo della Legge 28 giugno 2024, n. 90. Il CSP si impegna a garantire la piena conformità al Regolamento (UE) 2016/679 (GDPR), in tutte le attività di trattamento dei dati personali, inclusi i casi di trasferimento dei dati all'estero. Altresì, nel rispetto delle leggi, norme e direttive vigenti, tra cui il Regolamento UE 2016/679 General Data Protection Regulation (GDPR) e relativi decreti e regolamenti attuativi, i principi guida nella definizione e nell'attuazione del modello di sicurezza prendono a riferimento i principali standard e best practice internazionali, tra i quali si citano a titolo esemplificativo e non esaustivo i seguenti e successive revisioni: • COBIT5; • NIST Cybersecurity Framework for Critical Infrastructure, SP 800-145, SP 800-144, SP 500-299; • ENISA Security and Resilience in Governmental Clouds; • Cloud Control Matrix.	Obbligatorio		
RCY.7	Governance e Compliance (GOV)	Il CSP del servizio cloud deve dimostrare il possesso di seguenti certificazioni di sicurezza e conformità riconosciute, garantendo il rispetto degli standard di settore per la protezione dei dati e la gestione della sicurezza: • ISO/IEC 27001:2022 (Obbligatoria) • CSA STAR Level 1 (Obbligatoria) • ACN (Ex−AGID) (Obbligatoria per servizi PA) • PCI−DSS Level 4 (Obbligatoria per gestione transazioni su circuiti di pagamento)	Obbligatorio		
RCY.9	Governance e Compliance (GOV)	I processi di gestione del rischio riguardanti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione. Ovvero sono presenti ed aggiornate almeno su base annuale le politiche e le procedure per la definizione, l'implementazione e l'applicazione del modello di responsabilità della sicurezza condivisa rispetto a soggetti esterni e/o Amministrazioni terze (Shared Security Responsibility Model−SSRM).	Obbligatorio		
RCY.10	Governance e Compliance (GOV)	Il CSP deve adottare un programma di gestione della sicurezza della supply chain che comprenda: La verifica e il monitoraggio della sicurezza dei propri sub−fornitori; L'obbligo per i sub−fornitori di aderire a requisiti di sicurezza equivalenti.	Obbligatorio		
RCY.11	Governance e Compliance (GOV)	Il CSP deve garantire che tutto il personale, in particolare il Top Management, abbia completato un programma di formazione iniziale e aggiornamenti periodici (almeno annuali) sulla sicurezza informatica.	Obbligatorio		
RCY.12	Governance e Compliance (GOV)	Il CSP deve mantenere un inventario aggiornato di tutti gli asset, includendo hardware, software, dispositivi di rete e risorse virtuali. Tale inventario deve: − Essere integrato con un sistema di Asset Management centralizzato. − Specificare per ciascun asset informazioni critiche come proprietà, ubicazione, versione, stato e criticità rispetto alla sicurezza.	Obbligatorio		
RCY.13	Governance e Compliance (GOV)	Il CSP dovrà adottare framework e attestazioni di sicurezza conformi agli standard internazionali (es. SLSA − Supply−chain Levels for Software Artifacts o NIST Secure Software Development Framework), per garantire la sicurezza della propria catena di fornitura software e la tracciabilità del processo di sviluppo.	Obbligatorio		
RCY.14	Governance e Compliance (GOV)	Il CSP dovrà garantire la chiara identificazione e la definizione formale dei ruoli e delle responsabilità in ambito IT Security e Data Protection. Questo includerà l'identificazione delle persone coinvolte nella gestione delle informazioni, dei dati e nel trattamento dei dati personali, con una comunicazione chiara dei ruoli e delle responsabilità assegnate all'organizzazione	Obbligatorio		

RCY.15	Gestione Identità e Accessi (IAM)	Il CSP dovrà garantire l'adozione di un modello di sicurezza "Zero Trust" come approccio strategico alla sicurezza informatica che protegge l'organizzazione eliminando la fiducia implicita e convalidando continuamente ogni fase di un'interazione digitale.	Obbligatorio		
RCY.16	Gestione Identità e Accessi (IAM)	Il CSP dovrà garantire l'adeguato presidio della sicurezza logica attraverso la presenza di politiche e procedure di sicurezza delle informazioni dell'intera organizzazione che indirizzano la gestione delle utenze e degli accessi ai sistemi informatici in funzione del livello autorizzativo (es. Admin, utenti base, utenti amministratore, etc.) garantendo la revisione periodica delle utenze, password policy e adeguate misure prescrittive per amministratori di sistema e le utenze privilegiate secondo i principi di SOC 2 e CSA STAR.	Obbligatorio		
RCY.17	Gestione Identità e Accessi (IAM)	Il CSP dovrà garantire l'adeguata gestione delle utenze e degli accessi ai servizi e ai sistemi mediante meccanismi di gestione delle password per valutarne complessità, scadenza, non riutilizzabilità delle precedenti, etc.	Obbligatorio		
RCY.18	Gestione Identità e Accessi (IAM)	Il CSP dovrà garantire l'adeguata gestione degli accessi ai sistemi e ai servizi attraverso sistemi di autenticazione multi−fattore, garantendo un processo di autenticazione forte (MFA)	Obbligatorio		
RCY.19	Gestione Identità e Accessi (IAM)	Il CSP dovrà fornire strumenti che consentano di garantire che tutte le utenze siano associate univocamente a persone fisiche identificabili e, per utenze Machine−to−Machine, attribuite a un unico soggetto responsabile.	Obbligatorio		
RCY.20	Gestione Identità e Accessi (IAM)	Il CSP dovrà fornire strumenti che consentano di garantire l'adeguata gestione delle utenze e degli accessi ai servizi e ai sistemi mediante implementazione di controlli che permettano di definire quali operazioni possa compiere uno specifico utente nel rispetto dei principi di "Least Privilege" e "Need to Know".	Obbligatorio		
RCY.21	Gestione Identità e Accessi (IAM)	Il CSP dovrà fornire strumenti che consentano di garantire l'adeguata gestione delle utenze e degli accessi ai servizi e ai sistemi mediante implementazione di controlli specifici cadenzati sulle utenze con privilegi ampi per impedire operazioni illecite.	Obbligatorio		
RCY.22	Gestione Identità e Accessi (IAM)	I processo di autenticazione e autorizzazione deve essere disaccoppiato. L'autenticazione deve essere gestita dall'Identity Provider di Gruppo (AzureAD) mediante meccanismi di modern authentication (es. OAuth2) e soggetta a politiche di Multi−Factor Authentication (MFA). L'autorizzazione deve essere gestita a livello applicativo, prevedendo diversi livelli di profilazione basati sui coni di visibilità coerenti con ruoli e responsabilità degli utenti. È inoltre richiesto il riesame periodico dei diritti di accesso, con cadenza più frequente per gli utenti privilegiati (es. ogni 6 mesi) e processi di provisiong e de−provisiong.	Obbligatorio		
RCY.23	Gestione Identità e Accessi (IAM)	Il CSP dovrà implementare meccanismi di accesso temporaneo (Just−in−Time) o credenziali effimere, al fine di ridurre il rischio derivante da privilegi permanenti o non necessari, garantendo che l'accesso amministrativo avvenga solo per il tempo strettamente indispensabile all'esecuzione delle attività autorizzate.	Obbligatorio		
RCY.24	Gestione Identità e Accessi (IAM)	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 dell'accesso (ad esempio password, token o biometrico).	Obbligatorio		
RCY.25	Sicurezza delle Informazioni e dei Dati (INF)	I servizi erogati dal CSP dovranno in particolare assicurare sempre il migliore isolamento possibile dei dati e delle informazioni del Cliente anche per strumenti, sistemi o servizi condivisi e non dedicati, e garantirne la riservatezza nei confronti di accessi non autorizzati o non necessari.	Obbligatorio		
RCY.26	Sicurezza delle Informazioni e dei Dati (INF)	Il CSP dovrà garantire che le chiavi di crittografia di sua responsabilità − ad eccezione di casi specifici nei quali sarà pertinenza del Gruppo FS − siano generate in modo sicuro impedendo la diffusione delle chiavi di cifratura con soggetti non autorizzati. Su esplicita richiesta del Cliente, il CSP dovrà abilitare la modalità BYOK.	Obbligatorio		

RCY.27	Sicurezza delle Informazioni e dei Dati (INF)	Il CSP dovrà garantire la protezione dei dati, mediante cifratura, mascheramento, anonimizzazione, segregazione: esistenza di tecniche di cifratura dei dati memorizzati (es. dati memorizzati nei database o nelle memorie di massa). In particolare, Il CSP dovrà garantire la protezione dei dati, sia a riposo che in transito, attraverso le seguenti misure: Cifratura: Utilizzo di algoritmi di cifratura riconosciuti come sicuri in conformità con gli standard internazionali (es. AES−256). per proteggere la riservatezza delle informazioni sensibili, nonché delle informazioni soggette a requisiti legali e normativi. Integrità dei dati: Implementazione di tecniche per verificare se le informazioni critiche sono state alterate, ad esempio tramite funzioni hash o firme digitali. Mascheramento dei dati: Adozione di tecniche di data masking per minimizzare la visualizzazione e lettura di dati personali, applicando il principio del "need to know" per limitare l'accesso alle informazioni. Queste misure devono essere integrate nella soluzione offerta dal CSP per garantire il rispetto delle normative vigenti e la protezione delle informazioni dell'organizzazione	Obbligatorio		
RCY.28	Sicurezza delle Informazioni e dei Dati (INF)	Il CSP dovrà garantire la cancellazione dei dati e dismissione sicura dei dispositivi HW/SW utilizzati nell'ambito dell'erogazione dei servizi al Cliente, incluse le Postazioni di Lavoro del personale coinvolto dal CSP.	Obbligatorio		
RCY.29	Sicurezza delle Informazioni e dei Dati (INF)	Deve essere prevista la definizione di policy e procedure per abilitare il labeling, handling e la sicurezza sui dati.	Obbligatorio		
RCY.32	Sicurezza Applicativa (APPSEC)	Il CSP dovrà fornire strumenti che supportino l'adeguato presidio della sicurezza logica attraverso la gestione del ciclo di sviluppo sicuro del software, garantendo l'aderenza agli standard e alla normativa di settore quali OWASP e AGID e assicurando la scrittura di codice sicuro delle applicazioni nel loro specifico ambiente di sviluppo. Il CSP dovrà mettere a disposizione funzionalità e strumenti che supportino l'adozione di un approccio 'security by design' nello sviluppo e nella gestione del software, consentendo l'integrazione di misure di sicurezza fin dalle fasi iniziali del ciclo di vita applicativo, in conformità con le best practice di settore (es. OWASP, Secure SDLC).	Obbligatorio		
RCY.33	Sicurezza Applicativa (APPSEC)	Il CSP deve mettere a disposizione la possibilità di creare ambienti distinti che consentano al cliente di svolgere le attività di sviluppo separatamente dall'ambiente di Esercizio	Obbligatorio		
RCY.34	Sicurezza Applicativa (APPSEC)	In caso di applicazione di tipo web, il CSP dovrà fornire strumenti volti a garantirne la protezione mediante utilizzo di Web Application Firewall & API Protection per la protezione dei sistemi a livello di applicazione.	Obbligatorio		
RCY.35	Sicurezza Applicativa (APPSEC)	Il CSP dovrà fornire e mantenere disponibili strumenti che consentano al Cliente di monitorare e tracciare in modo trasparente i costi infrastrutturali, i costi delle componenti software, delle librerie e delle dipendenze utilizzate, al fine di permettere una visibilità completa e una gestione ottimale delle spese operative	Obbligatorio		
RCY.36	Sicurezza Applicativa (APPSEC)	L'applicazione deve assicurare, attraverso opportuni meccanismi di convalida, che tutti i parametri in input, specificati dall'utente, siano congruenti a quanto atteso. In particolare, sui dati acquisiti in ingresso, l'applicazione deve prevedere l'implementazione di meccanismi di controllo che limitino il set di caratteri o valori, inseribili dall'utente, solo a quelli congruenti ai campi richiesti e/o alle form di pertinenza, al fine di identificare ed annullare gli effetti di errori quali valori out−of−range o non pertinenti, caratteri invalidi negli stream, dati mancanti, etc. Per quanto riguarda i caratteri speciali, se presenti/richiesti in input, sono considerati pericolosi poiché la loro combinazione non può essere considerata semplice 'testo'.	Obbligatorio		
RCY.37	Sicurezza Applicativa (APPSEC)	Il CSP deve mettere a disposizione strumenti che supportino la possibilità di rendere disponibile un account di test per ogni ruolo ed un URL utilizzabili dal cliente per effettuare ogni tipo di verifica necessaria per il rilascio di nuove evolutive.	Obbligatorio		
RCY.38	Business Continuity e Disaster Recovery (BC/DR)	Il CSP dovrà essere dotato di procedure e sistemi in grado di garantire il backup e recovery dei dati e dei sistemi, garantendo la protezione delle copie di backup mediante opportune misure di sicurezza fisica e logica, che devono essere opportunamente cifrate. Il CSP dovrà così condurre dei test periodici, dandone evidenza al Cliente.	Obbligatorio		

RCY.39	Business Continuity e Disaster Recovery (BC/DR)	Il CSP dovrà garantire la continuità del servizio in caso di interruzioni o malfunzionamenti, in conformità con gli SLA e i parametri RTO/RPO concordati con il Cliente. In caso di servizi critici, il CSP dovrà assicurare la Business Continuity e Disaster Recovery attraverso: – Un piano di disaster recovery, che stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati (CED) e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. – Un piano di continuità operativa (business continuity), che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. – L'implementazione di un modello e di tecnologie di High Availability che permettano, tramite l'adozione di strumenti tecnologici ridondati, di avere un sistema altamente disponibile ai propri utenti.	Obbligatorio		
RCY.40	Business Continuity e Disaster Recovery (BC/DR)	Il CSP deve fornire strumenti che possano prevedere apposite procedure di roll back al fine di ripristinare lo stato iniziale di qualsiasi sistema o servizio, qualora dovessero presentarsi problemi imprevisti e irrisolvibili durante la procedura di aggiornamento per effetto di un cambiamento.	Obbligatorio		
RCY.41	Threat & Vulnerability Management (TVM)	Il CSP deve fornire strumenti a supporto del processo di Threat Intelligence per raccogliere, analizzare ed elaborare le informazioni relative alle potenziali minacce che potrebbero impattare il servizio e/o l'organizzazione servita	Obbligatorio		
RCY.42	Threat & Vulnerability Management (TVM)	Il CSP dovrà effettuare attività periodiche e schedulate di security assessment (a titolo esemplificativo VA, PT, SAST, IAST, DAST) per la verifica del livello di sicurezza di infrastrutture, sistemi e codice sviluppato mediante la ricerca di vulnerabilità o debolezze che, se sfruttate potrebbero compromettere il livello di sicurezza, individuando le possibili azioni di rimedio. Il CSP si impegna a condividere l'esito degli assessment e del relativo piano di rimedio concordando le priorità di intervento e i relativi tempi	Obbligatorio		
RCY.43	Threat & Vulnerability Management (TVM)	Il servizio deve supportare la costante distribuzione di release software, aggiornamenti di sicurezza e, ove necessario, workaround o misure di Virtual patching per mitigare le vulnerabilità identificate, anche quelle rilevate dagli assessment di sicurezza e dai servizi di security advisory. A tal fine, il CSP è responsabile della definizione di un piano di distribuzione per l'aggiornamento dei sistemi, la gestione del rilascio di configurazioni sicure verificate, e l'installazione tempestiva di patch raccomandate da produttori o terzi. Tutte le attività devono essere pianificate e attuate in modo da assicurare il corretto funzionamento dei sistemi, senza comprometterne i livelli di servizio. Il CSP dovrà evidenziare e documentare l'efficacia degli interventi eseguiti mediante la ripetizione delle azioni che avevano consentito di individuare le vulnerabilità, nonché di tenere traccia di ogni aggiornamento o workaround applicato, assicurando la trasparenza e la tracciabilità di tutte le modifiche apportate.	Obbligatorio		
RCY.44	Threat & Vulnerability Management (TVM)	Il CSP si impegna a condividere in modo tempestivo le azioni di adeguamento tecnologico per release hardware/software disponibili per tutti i sistemi e servizi ICT che concorrono anche indirettamente nell'erogazione del servizio al Cliente. Il CSP dovrà inoltre provvedere al supporto delle indicazioni di mitigation da seguire.	Obbligatorio		
RCY.45	Threat & Vulnerability Management (TVM)	Il CSP deve supportare la costante distribuzione del software e degli aggiornamenti di sicurezza sui sistemi/piattaforme che mitighino le vulnerabilità che insistono sulle tecnologie a supporto dei sistemi che erogano il servizio.	Obbligatorio		
RCY.46	Threat & Vulnerability Management (TVM)	Il CSP deve garantire la protezione degli endpoint e delle postazioni, nonché device mobile che accedono alle informazioni del Cliente, attraverso opportuni strumenti (es. MDM)	Obbligatorio		
RCY.47	Container Security (CS)	Il CSP dovrà fornire strumenti a supporto della implementazione di pipeline di integrazione e distribuzione continua (CI/CD) sicure, prevedendo la scansione automatica delle immagini container e dei registri per rilevare vulnerabilità, configurazioni non sicure o pacchetti obsoleti, assicurando l'uso esclusivo di immagini verificate e firmate digitalmente.	Obbligatorio		
RCY.48	Container Security (CS)	Tutti i ServiceAccount utilizzati da entità tecniche (CI/CD, operatori, tool di automazione, script, ecc.) devono disporre esclusivamente dei permessi strettamente necessari al proprio scopo, assegnati tramite Role/ClusterRole e RoleBinding/ClusterRoleBinding specifici per ambito namespace (o cluster–wide solo se indispensabile) e con token soggetti a rotazione secondo le policy aziendali.	Obbligatorio		

RCY.49	Container Security (CS)	Il CSP deve fornire strumenti che supportino la segmentazione logica e fisica della rete cluster, distinguendo tra ingressi pubblici, traffico interno al cluster, accessi amministrativi e canali di egress. L'architettura deve prevedere confini definiti tra questi domini, tramite firewall, VLAN, subnet dedicate o policy SDN.	Obbligatorio		
RCY.50	Container Security (CS)	Il CSP deve fornire strumenti che consentano la raccoltae di metriche e log dei container e dei pod in esecuzione nel cluster utilizzando componenti installati e gestiti all'interno del cluster (es. OpenShift Monitoring con Prometheus, Cluster Logging Operator con Fluentd e Loki) o soluzioni esterne integrate garantendo la visualizzazione centralizzata e un sistema di alerting continuo sui workload.	Obbligatorio		
RCY.51	Container Security (CS)	Il CSP deve fornire strumenti che assicurino che le immagini container utilizzate nei workload devono provenire solo da registry certificati, privati o con firma verificabile. È obbligatorio configurare policy di pull da registry fidati ed evitare immagini pubbliche non controllate.	Obbligatorio		
RCY.52	Container Security (CS)	Il CSP deve fornire strumenti che supportino il controllo continuo di compliance e vulnerabilità del cluster, tramite strumenti di analisi statica, runtime e policy con capacità di audit e enforcement.	Obbligatorio		
RCY.53	Container Security (CS)	Il CSP deve garantire che sia possibile che le immagini dei container siano sottoposte a controllo di sicurezza tramite opportuni servizi di vulnerability assessment.	Obbligatorio		
RCY.54	Container Security (CS)	Il CSP deve fornire funzionalità Security Context Constraints (SCC) che consentano al cliente di limitare l'esecuzione dei pod a utenti non root. Devono essere attivi i profili restricted o equivalenti, e deve essere evitata qualsiasi configurazione che consenta escalationi fino al livello di Root.	Obbligatorio		
RCY.55	Container Security (CS)	Il CSP deve mettere a disposizione strumenti che consentano diimpedire l'esecuzione di container con flag privileged: true. I profili SCC associati ai namespace applicativi devono escludere privileged e utilizzare solo profili ristretti, controllati da policy.	Obbligatorio		
RCY.56	Container Security (CS)	Il CSP deve fornire funzionalità di auditing e policy−as−code (es. OPA/Gatekeeper, Kyverno, Red Hat Advanced Cluster Security) che consentano di sottoporre il cluster a controlli continui di compliance. Le policy devono poter bloccare o segnalare configurazioni non conformi (deny/admit).	Obbligatorio		
RCY.57	Container Security (CS)	Il CSP deve fornire funzionalità che consentano al Cliente di organizzare i workload in namespace separati per team, applicazione o dominio funzionale. Devono essere definiti ruoli RBAC e risorse quota per ciascun namespace, garantendo l'isolamento logico tra i tenant e la visibilità granulare sui log.	Obbligatorio		
RCY.58	Container Security (CS)	Il CSP deve mettere a disposizione meccanismi che permettano al Cliente di definire NetworkPolicy per ciascun namespace applicativo, al fine di segmentare il traffico in ingresso, uscita e laterale tra i pod. Le funzionalità devono consentire la configurazione di policy specifiche per ogni tipo di workload applicando il principio "default deny".	Obbligatorio		
RCY.59	Container Security (CS)	Il CSP deve fornire strumenti che consentano di utilizzare immagini firmate dalla notazione per assicurarsi che le immagini provengano da origini attendibili e non vengano modificate in modo dannoso.	Obbligatorio		
RCY.60	Container Security (CS)	Il CSP deve mettere a disposizione configurazioni SCC o Admission Contraller che consentano al Cliente di impedire che i pod non siano configurati per condividere il PID namespace (hostPID: true) o lo spazio dei nomi IPC (hostIPC: true) dell'host, salvo casi eccezionali documentati.	Obbligatorio		
RCY.61	Container Security (CS)	Il CSP deve fornire meccanismi che consentano di vietare modifiche arbitrarie ai parametri sysctl. È ammesso solo l'uso di sysctl "sicuri" (es. kernel.shm_rmid_forced, net.ipv4.tcp_syncookies) definiti nei SCC o PodSecurity standards. L'uso di unsafe sysctl deve essere bloccato da policy.	Obbligatorio		
RCY.62	Container Security (CS)	Il CSP deve mettere a disposizione strumenti che supportino l'utilizzo di immagini container prive di binari potenzialmente pericolosi per l'ambiente cluster (es. wget, curl, iptables, sysctl, package manager), favorendo la minimizzazione delle immagini (distroless, scratch) e audit periodici sul contenuto delle immagini.	Obbligatorio		
RCY.63	Container Security (CS)	Il CSP deve favorire funzionalità che consentano di limitare i container all'uso di profili scc consentiti. L'accesso a profili privilegiati deve essere limitato a casi documentati e monitorati.	Obbligatorio		
RCY.64	Container Security (CS)	Il CSP deve mettere a disposizione la possibilità di configurare al Cliente la limitazione del pod all'uso di ProcMountTypes consentiti (Unmasked, Default).	Obbligatorio		

RCY.65	Container Security (CS)	Il CSP deve fornire funzionalità SCC che consentano al Cliente di impedire che un pod possa girare con allowPrivilegeEscalation abilitato.	Obbligatorio		
RCY.66	Container Security (CS)	Il CSP deve mettere a disposizione la possibilità di configurare il File system ROOT in modalità read only (readOnlyRootFilesystem) per evitare che binari malevoli possano girare sul PATH del cluster.	Obbligatorio		
RCY.67	Container Security (CS)	Il CSP deve fornire strumenti SCC che consentano di minimizzare l'ammissione di container con NET_RAW capabilities o capability addizionali.	Obbligatorio		
RCY.68	Container Security (CS)	Il CSP deve mettere a disposizione meccanismi che consentano di controllare l'assegnazione di SCC a utenti e service account affinché solo gli account che richiedono privilegi specifici possano avere accesso a profili permissivi; tutti gli altri devono essere vincolati a SCC restricted.	Obbligatorio		
RCY.69	Container Security (CS)	Il CSP deve fornire funzionalità che consentano al Cliente di garantire la presenza di NetworkPolicy attive per ogni namespace non infrastrutturale del cluster profilate in base al tipo di traffico atteso.	Obbligatorio		
RCY.70	Container Security (CS)	Il CSP deve mettere a disposizione funzionalità che supportino l'utilizzo di secrets montati come file all'interno dei pod (VolumeMount), anziché come variabili d'ambiente.	Obbligatorio		
RCY.71	Container Security (CS)	Il CSP deve fornire strumenti che consentano di filtrare l'ammissione di immagini ammettendo soltanto quelle provenienti da registry sicuri e conosciuti.	Obbligatorio		
RCY.72	Container Security (CS)	Il CSP deve mettere a disposizione funzionalità che permettano di limitare o proibire l'uso del default namespace.	Obbligatorio		
RCY.73	Container Security (CS)	Il CSP deve mettere a disposizione soluzioni di sicurezza per il monitoraggio continuo delle risorse cluster e workload, in grado di rilevare comportamenti anomali, configurazioni pericolose e vulnerabilità (come sistemi di Cloud Native Application Protection Platform (CNAPP), Cloud Security Posture Management (CSPM) e Cloud Workload Protection Platform (CWPP)).	Obbligatorio		
RCY.74	Container Security (CS)	Il CSP deve mettere a disposizione meccanismi automatici di drift detection che consentano al Cliente di rilevare gli sconstamenti tra i template Infrastructure−as−Code (es. Helm, Terraform, Ansible) e lo stato effettivo delle risorse distribuite. Gli scostamenti devono generare alert e richiedere approvazione per riconciliazione.	Obbligatorio		
RCY.75	Infrastruttura, Reti e Cloud Security (NET/INF)	Disponibilità di ambienti multi−tenant e deploy multi−region al fine di poter indirizzare segregazioni logiche e fisiche, altresì SLA relativi a Business Continuity e Disaster Recovery. Nel caso in cui siano trattati dati sensibili o critici, siano coinvolte infrastrutture o servizi strategici per la continuità operativa del Gruppo, o sussistano obblighi di conformità, sicurezza o audit che richiedano isolamento logico o fisico dei dati e delle risorse, si richiede la fornitura in modalità tenant dedicato (single−tenant)	Obbligatorio		
RCY.76	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP dovrà garantire, tramite la disponibilità di un CMDB (Configuration Management Database) aggiornato, la tracciabilità dei dispositivi hardware e software utilizzati per l'erogazione del servizio. Tali informazioni dovranno essere rese disponibili al Cliente su richiesta, ai fini di audit, sicurezza o gestione operativa.	Obbligatorio		
RCY.77	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP dovrà fornire strumenti che consentano di implementare misure adeguate a protezione dei sistemi, dei servizi, delle applicazioni anche se solo indirettamente coinvolti o impiegati per l'erogazione dei servizi al Cliente (es. sistemi di virtualizzazione, sistemi di trouble ticketing etc…), ivi inclusi per i modelli cloud i contesti di pertinenza del CSP e i sistemi, software, architetture e servizi condivisi.	Obbligatorio		
RCY.78	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP dovrà fornire strumenti per poter garantire che le connessioni da e verso il sistema, supportino i seguenti standard: VPN IPSec, TLS 1.2 o superiore, mTLS, API autenticate; autenticazione forte (mutual authentication con certificati) e utilizzo di API gateway. L'interconnessione deve seguire il principio minima di esposizione, garantendo conformità agli standard di sicurezza.	Obbligatorio		
RCY.79	Infrastruttura, Reti e Cloud Security (NET/INF)	La gestione e l'accesso tramite le API del CSP devono rispettare gli standard di sicurezza (es. OWASP Software Assurance Maturity Model, ISO 27034). Per tutte le API esposte dal servizio cloud deve essere dichiarata la conformità al Modello di interoperabilità, definito da AgID con le linee guida adottate ai sensi della normativa vigente. Qualora le API esposte siano conformi, devono essere condivise le specifiche dell'API in formato machine readable compatibile con le indicazioni del modello d'interoperabilità (e.g. OpenAPI3 per le API REST, WSDL per le API SOAP).	Obbligatorio		
RCY.80	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP dovrà fornire strumenti che consentano di implementate misure per garantire l'integrità, la sicurezza e la disponibilità di ambienti virtuali in linea con le conformità normative.	Obbligatorio		

RCY.82	Infrastruttura, Reti e Cloud Security (NET/INF)	Il sistema deve supportare il protocollo NTP assicurando la sincronizzazione oraria.	Obbligatorio		
RCY.83	Infrastruttura, Reti e Cloud Security (NET/INF)	Il servizio deve garantire la gestione di sistemi di rilevamento e contrasto di attacchi Denial of Service (DoS) e Distributed denial of Service (DDoS). Il CSP deve garantire la gestione del servizio su internet, contestualizzando le configurazioni rispetto alle tecnologie e asset, ottimizzando il servizio per ottenere il minor numero di falsi positivi e garantendo il massimo delle prestazioni all'assurance dei servizi.	Obbligatorio		
RCY.84	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP di servizi cloud deve adottare un sistema di Host Intrusion Detection System (HIDS) per rilevare e identificare eventi o sequenze di eventi che potrebbero compromettere un sistema, un dispositivo o la rete. Inoltre, deve implementare un Host Intrusion Prevention System (HIPS) per analizzare il traffico, rilevare la presenza di accessi non autorizzati o codice malevolo in esecuzione sui sistemi, e bloccare eventuali tentativi di attacco o traffico anomalo.	Obbligatorio		
RCY.85	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP dovrà mettere a disposizione servizi Antimalware che deve garantire la protezione dei sistemi server gestiti da qualsiasi tipologia di software malevolo eseguibile e non (es. virus, trojan, Worm, Key loggers, rootkit, ransomware etc.). Le "firme" di protezione devono essere aggiornate in tempo reale. Tutti gli eventi malware−related devono essere inviati ad una piattaforma centralizzata di collezionamento.	Obbligatorio		
RCY.86	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP dovrà fornire strumenti volti a supportare: − l'installazione di firewall perimetrali per limitare l'esposizione a livello di rete, di sistemi e servizi ai soli host/IP strettamente necessari, tracciando gli accessi o i tentativi di accesso; − l'implementazione di soluzioni di Network Detection & Response (NDR); − l'implementazione di soluzioni di tipo Network−based Intrusion Detection Systems (IDS) e Network−based Intrusion Prevention Systems (IPS) per la rilevazione di anomalie di sicurezza ed il blocco di possibili tentativi di attacco; − l'implementazione di meccanismi che permettono di effettuare in qualsiasi momento l'associazione dei seguenti campi per l'identificazione dei dispositivi collegati alla rete: Indirizzo IP, Host / Mac Address e Username o ID univoco dell'utente.	Obbligatorio		
RCY.87	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP dovrà fornire strumenti volti a supporto della protezione dei server DNS per garantire la disponibilità e integrità della risoluzione dei nomi.	Obbligatorio		
RCY.89	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP dovrà fornire strumenti a supporto della corretta configurazione dei dispositivi di rete (inclusi router, switch e firewall): − evidenziare condizioni di sovraccarico o eccezioni, quando si verificano; − registrare gli eventi (logging) e salvarli su un sistema separato; − integrarsi con meccanismi di controllo degli accessi (ad esempio per fornire autenticazione forte); − assicurare che le password per accedere a tali dispositivi non vengano inviate in chiaro; − disabilitare il "source routing", tecnica di specificare all'interno dell'header IP il tragitto (route) che il pacchetto deve seguire per mantenere il controllo all'interno del dispositivo di inoltro dei pacchetti.	Obbligatorio		
RCY.90	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP dovrà mettere a disposizione strumenti che consentano l'erogazione del servizio di NAT Management per la gestione delle regole di traduzione degli indirizzi IP configurati all'interno dell'infrastruttura di rete ed il piano di indirizzamento complessivo/pubblico.	Obbligatorio		
RCY.91	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP deve attuare i controlli opportuni per quanto concerne la sicurezza degli ambienti computazionali garantendo la protezione delle reti e dei sistemi da eventuali attacchi, da accessi e modifiche non autorizzate assicurando il monitoraggio dei componenti informatici e il funzionamento continuo ed ottimale dell'infrastruttura.	Obbligatorio		
RCY.92	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP deve adottare procedure/strumenti di change management per tenere traccia delle modifiche eseguite sulle configurazioni del sistema che, in ogni caso, non dovranno ridurre i livelli di sicurezza. In aggiunta, il CSP deve prevedere la definizione di un processo formale che documenti la fase di autorizzazione, l'analisi di impatto in termini di sicurezza e implementazione delle modifiche e dell'installazione delle patch all'interno di processi, sistemi o strutture aziendali.	Obbligatorio		

RCY.93	Monitoraggio, Logging e Incident Management (MON/IR)	Il CSP deve garantire fornire strumenti che consentano un'adeguata gestione delle utenze e degli accessi ai servizi e ai sistemi, assicurando il tracciamento di tutti gli accessi effettuati dagli utenti, la registrazione e conservazione dei log relativi agli accessi e alle attività svolte, con particolare attenzione agli utenti con credenziali privilegiate e/o Amministratori di Sistema, per i quali devono essere previsti specifici meccanismi di controllo, monitoraggio e rendicontazione, secondo le normative vigenti e le best practice di settore.	Obbligatorio		
RCY.94	Monitoraggio, Logging e Incident Management (MON/IR)	Il CSP dovrà fornire strumenti che consentano di garantire che i sistemi, le applicazioni, i servizi e le infrastrutture utilizzati per l'erogazione del servizio siano in grado di generare eventi e log rilevanti ai fini della sicurezza, e audit log. Tali log dovranno essere raccolti, conservati (in tempi concordati con il Clienti) e correlati mediante apposite piattaforme (es. SIEM), e su richiesta piattaforme proprietarie del cliente, al fine di consentire attività di monitoraggio, analisi e rilevazione di eventuali anomalie di sicurezza.	Obbligatorio		
RCY.95	Monitoraggio, Logging e Incident Management (MON/IR)	Il CSP dovrà fornire strumenti volti a garantire un servizio di Real Time Monitoring h24x7 finalizzato alla rilevazione e analisi di attacchi informatici e minacce, e alla gestione di anomalie e incidenti di sicurezza nel perimetro di erogazione dei servizi al Cliente che dovrà comprendere: – personale specializzato in un centro specializzato (SOC) in grado di correlare gli eventi di sicurezza intercettati, analizzare gli alert generati dalla piattaforma di monitoraggio e correlazione, attivare le opportune procedure e processi per la gestione degli incidenti – La gestione degli incidenti di sicurezza identificati attraverso un team operativo specializzato in grado di intervenire tempestivamente per il contenimento, il contrasto e la risoluzione dell'incidente e/o attacco informatico. – La produzione degli incident report che relazionano le cause dell'incidente rilevato, gli eventuali danni provocati e le azioni di contrasto e ripristino intraprese. – La registrazione e memorizzazione degli incidenti avvenuti/individuati	Obbligatorio		
RCY.96	Monitoraggio, Logging e Incident Management (MON/IR)	Il CSP dovrà comunicare nei tempi e nei modi, previsti dalle normative vigenti (es. GDPR, Direttiva NIS, ecc.) e concordati con il Cliente, ogni incidente occorso sui sistemi che gestiscono dati e informazioni del Cliente. Il CSP dovrà provvedere, inoltre, alla stima dei possibili impatti sulla sicurezza delle informazioni, sugli asset e sui servizi erogati al Cliente, e prevedere una RCA per ciascun caso con esito positivo o negativo, altresì il report post–incident. Il CSP deve segnalare tempestivamente al Cliente eventuali accessi non autorizzati a dati del Gruppo FS che possano causare perdite, divulgazioni o alterazioni dei dati, nel rispetto della normativa vigente. Deve altresì collaborare con il Cliente ad un piano di comunicazione e coordinamento per i rapporti con le Autorità competenti (es. Garante, ACN)	Obbligatorio		
RCY.97	Monitoraggio, Logging e Incident Management (MON/IR)	Dovranno essere altresì tempestivamente comunicate, nei tempi e nei modi concordati con il Clienti, le eventuali rilevazioni di anomalie di sicurezza sui sistemi del CSP, e/o di supply direttamente coinvolti nell'erogazione dei servizi al Gruppo FS.	Obbligatorio		
RCY.98	Monitoraggio, Logging e Incident Management (MON/IR)	Il CSP dovrà proteggere adeguatamente i Log raccolti mediante sistemi e tecniche che ne garantiscono l'inalterabilità, la non cancellabilità e la conservazione per tutto il tempo ritenuto congruo e comunque non inferiore a quanto indicato dalle normative vigenti.	Obbligatorio		
RCY.99	Monitoraggio, Logging e Incident Management (MON/IR)	Il CSP dovrà adottare soluzioni adeguate a protezione del perimetro (garantendone il costante aggiornamento sia automatico che, se necessario, manuale) attraverso: File Integrity Tool per la verifica dell'integrità dei file per assicurare che i file critici di sistema (compresi eseguibili, librerie e file di configurazione) non siano stati alterati.	Obbligatorio		

RCY.100	Sicurezza Fisica (SF)	Il CSP deve garantire la protezione degli asset informatici da attacchi esterni, accessi e modifiche non autorizzate, assicurando il funzionamento continuo ed ottimale dell'infrastruttura di sicurezza, nonché monitorare il comportamento dei sistemi ed apportare le modifiche necessarie alle configurazioni delle politiche di sicurezza perimetrale. L'accesso fisico agli edifici che ospitano l'infrastruttura IT dell'organizzazione deve essere limitato agli individui autorizzati mediante le seguenti misure di sicurezza e deve rispettare il principio del minimo privilegio, ovvero ciascun lavoratore deve poter accedere solo a quelle funzioni/servizi/dati necessari allo svolgimento delle proprie mansioni lavorative: – controllo accessi all'ingresso degli edifici (reception e/o servizio di guardiania); – manutenzione pianificata dei sistemi critici; – il personale deve essere dotato di badge personale o di altro mezzo di identificazione (e.g. PIN).	Obbligatorio		
RCY.101	Sicurezza Fisica (SF)	Apparecchiature, informazioni o software che gestiscono dati o informazioni del Cliente non devono essere portate al di fuori dell'ambiente del CSP senza preventiva autorizzazione. Tutte le apparecchiature da riutilizzare o da smaltire, che contengono supporti di memorizzazione, devono essere controllate per assicurare che le informazioni del Cliente siano state rimosse o sovrascritte in modo sicuro, prima del loro smaltimento/riutilizzo.	Obbligatorio		
RCY.102	Sicurezza Fisica (SF)	Il CSP deve aver adottato misure di sicurezza per prevenire o far fronte ad un possibile incendio/allagamento del Data Center primario che ospita le macchine dell'organizzazione. Il CSP deve svolgere delle attività di monitoraggio della temperatura interna del Data Center primario per tutelare le macchine in esso presenti. I cavi di rete ed i punti di accesso alla rete nel data center primario devono essere protetti mediante controlli fisici. Gli edifici che ospitano l'infrastruttura IT del data center primario dell'organizzazione	Obbligatorio		

REQUISITI MINIMI O DISTINTIVI TECNICI - MIGLIORATIVI - di cui par. 1.1 del Capitolato Tecnico					
ID - Capitolato Tecnico	**Ambito**	**Descrizione**	**Tipologia**	**Dichiarazione di possesso**	**Note**
R8	Data Acquisition & Ingestion − Big Data	Capacità della piattaforma di supportare lo scaling automatico delle risorse in base al volume dei dati ricevuto con un limite di throughput massimo documentato (espresso in GB/min o record/sec) in grado di gestire carichi concorrenti senza degrado delle performance.	Migliorativo		
R10	Data Acquisition & Ingestion − Streaming	Il sistema mette a disposizione moduli specifici per il riconoscimento di eventi duplicati o non ordinati in modo da garantire un'elaborazione "exactly−once".	Migliorativo		
R12	Data Acquisition & Ingestion − ETL/ELT	La piattaforma mette a disposizione strumenti di suggerimento per l'ottimizzazione delle prestazioni in ambito ETL o ELT.	Migliorativo		
R14	Storage & Processing − Data Lakehouse	La federazione dei cataloghi dei metadati del Lake house è attiva e consente di sincronizzare le modifiche sugli oggetti e sulle query engine in modo da avere sempre una vista aggiornata e coerente a tutti gli utenti che operano sulla piattaforma.	Migliorativo		
R15	Storage & Processing − Data Lakehouse	La piattaforma gestisce le risorse di calcolo (autoscaling) in funzione di carico, priorità e tipologia di query, con ottimizzazione dei costi.	Migliorativo		
R17	Storage & Processing − Query Engine	La piattaforma consente di effettuare data enrichment in tempo reale utilizzando fonti esterne (API, lookup su database o servizi di terze parti) direttamente durante il processing.	Migliorativo		
R18	Storage & Processing − Query Engine	La piattaforma consente di gestire in modo efficiente carichi analitici misti, supportando contemporaneamente query interattive a bassa latenza e processi batch intensivi senza interferenze o degrado delle prestazioni	Migliorativo		
R20	Storage & Processing − Stream Processing	La piattaforma supporta la crittografia dei dati in transito e a riposo	Migliorativo		
R22	Storage & Processing − Data Lake	Il sistema abilita un logging di accesso a ciascuno dei suoi oggetti	Migliorativo		
R23	Storage & Processing − Data Lake	Lo storage degli oggetti offre livelli di classe di storage distinti per soddisfare la necessità di storage "hot" con accesso frequente e performante, storage "cool" a cui si accede meno spesso e storage "cold" a cui si accede raramente.	Migliorativo		
R25	Storage & Processing − Data Transformation	La piattaforma consente l'implementazione di trasformazioni semantiche (i.e. standardizzazione, mapping di codici, regole di business) e di trasformazioni condizionali o parametriche (i.e. basate su logiche dinamiche).	Migliorativo		
R27	Storage & Processing − Data Warehouse	Lo storage si integra con strumenti di Business Intelligence e reporting più diffusi sul mercato quali Power BI, Tableau, Qlik Sense.	Migliorativo		
R29	Digital & Transformation − AI Tools	La piattaforma fornisce ambienti collaborativi multiutente che permettono la creazione di workspace condivisi e sandbox sicure per la sperimentazione, con gestione granulare di ruoli, permessi, versioning e isolamento delle risorse.	Migliorativo		
R30	Digital & Transformation − AI Tools	La piattaforma supporta la creazione di pipeline automatizzate per attività di data preparation, feature engineering e model training, integrabili con strumenti MLOps e con workflow orchestration per l'esecuzione e la gestione end−to−end dei processi di AI.	Migliorativo		
R32	Digital & Transformation − Gen AI	La piattaforma dispone di un Model Registry integrato per la registrazione, il versioning, la governance e la tracciabilità dei modelli e degli agenti AI disponibili.	Migliorativo		

R33	Digital & Transformation – Gen AI	La piattaforma supporta il provisioning di unità di throughput garantite (PTU) o di risorse computazionali equivalenti dedicate, al fine di assicurare prestazioni costanti e a bassa latenza per carichi mission−critical e di garantire prevedibilità dei costi operativi anche in scenari di utilizzo intensivo.	Migliorativo		
R34	Digital & Transformation – Gen AI	La piattaforma garantisce controlli nativi o integrabili di sicurezza e conformità (AI Guardrails) per garantire l'affidabilità dei contenuti generati, inclusi filtri automatici di contenuto tossico o sensibile e meccanismi di moderazione.	Migliorativo		
R36	Digital & Transformation – Model Training	La piattaforma supporta nativamente il ciclo completo di sviluppo Machine Learning, comprendente data preparation, feature engineering, training, hyperparameter tuning e model registry, in ambienti integrati, automatizzati e governati.	Migliorativo		
R38	Digital & Transformation – Model Deployment	La piattaforma fornisce funzionalità di monitoraggio e osservabilità dei modelli in produzione, consentendo di identificare tempestivamente problemi di prestazioni o errori, possibilità di scaling.	Migliorativo		
R40	Data & AI Serve – AI Real Time Endpoints	La piattaforma supporta il model serving su endpoint in tempo reale (real−time), garantendo bassa latenza e alta disponibilità, con configurazione personalizzabile della capacità computazionale per assicurare performance costanti delle API di inferenza anche a carichi elevati o frequenze di chiamata elevate.	Migliorativo		
R42	Data & AI Serve – API	La piattaforma garantisce un'autenticazione sicura con protocolli OAuth2, API Key, JWT, certificato digitale.	Migliorativo		
R44	Containerization	La piattaforma offre un'infrastruttura gestita o containerizzabile per l'esposizione dei modelli come servizio, con supporto a protocolli standard e capacità di personalizzazione dell'infrastruttura e configurazione di scalabilità e alta disponibilità (autoscaling automatico, e bilanciamento del carico) per garantire efficienza e resilienza del servizio di inferenza.	Migliorativo		
R46	Data & AI Serve – SQL Access	La piattaforma offre un query optimizer supporta approcci sia cost−based che rule−based che generano piani di esecuzione adattivi basati su statistiche aggiornate.	Migliorativo		
R47	Data & AI Serve – SQL Access	La piattaforma dispone di masking dinamico dei dati per proteggere informazioni sensibili.	Migliorativo		
R49	Visualization – Dashboarding	Lo strumento di BI supporta la creazione di dashboard interattive e report con funzionalità di drill− down, slicing e pivoting su più dimensioni, incluse capacità OLAP e modelli multidimensionali.	Migliorativo		
R50	Visualization – Dashboarding	Lo strumento di BI consente agli utenti di visualizzare e analizzare reti e grafi di relazioni.	Migliorativo		
R52	Visualization – Geospatial Analysis	Lo strumento di BI offre supporto nativo a tipi di dato geografico (GEOGRAPHY), funzioni spaziali (ad es. buffer, intersection, ST_*, clustering) e visualizzazioni geografiche avanzate (heatmap, layers, shape/GeoJSON).	Migliorativo		
R54	Visualization – Self Service BI	Il servizio di data visualization mette a disposizione modalità di conversational BI nativa per poter interrogare la base dati con Natural Language Query (NLQ) con più di una lingua straniera.	Migliorativo		
R56	Integration – Data Orchestration	La piattaforma mette a disposizione l'orchestrazione assistita da AI e guidata dai metadata in linea con approcci moderni di data fabric.	Migliorativo		
REQUISITI MINIMI O DISTINTIVI DI SICUREZZA - MIGLIORATIVI - di cui par. 1.2 del Capitolato Tecnico					
ID - Capitolato Tecnico	**Ambito**	**Descrizione**	**Tipologia**	**Dichiarazione di Possesso**	**Note**

RCY.8	Governance e Compliance (GOV)	Il CSP del servizio cloud deve dimostrare il possesso di seguenti certificazioni opzionali di sicurezza e conformità riconosciute, garantendo il rispetto degli standard di settore per la protezione dei dati e la gestione della sicurezza: • CSA STAR Level 2 • ISO/IEC 42001 • ISO/IEC 27017 • ISO/IEC 27018 •ISO/IEC 27002 •ISO/IEC 27701 •ISO/IEC 27031 • ISO/IEC 22301 • SOC 2 • SOC 3	Migliorativo		
RCY.30	Sicurezza delle Informazioni e dei Dati (INF)	Il servizio prevede l'implementazione di un sistema di gestione dei diritti digitali (DRM) per proteggere le informazioni del cliente e i software più critici che vengono utilizzati al di fuori del controllo dell'organizzazione.	Migliorativo		
RCY.31	Sicurezza delle Informazioni e dei Dati (INF)	Il CSP dovrà adottare soluzioni adeguate a protezione del perimetro (garantendone il costante aggiornamento sia automatico che, se necessario, manuale) attraverso: Data Loss Prevention (DLP) per monitorare i flussi di dati all'interno della rete dell'organizzazione ed evidenziare eventuali anomalie.	Migliorativo		
RCY.81	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP dovrà fornire strumenti per implementare e mantenere un sistema centralizzato per la gestione delle configurazioni, assicurandosi che:	Migliorativo		
RCY.88	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP potrà supportare l'adozione di soluzioni adeguate a protezione del perimetro (garantendone il costante aggiornamento sia automatico che, se necessario, manuale) attraverso: Controllo accessi alla rete dei dispositivi, ristretto utilizzando tecnologie di Network Access Control (NAC), in grado di verificare la configurazione del dispositivo e gestire opportunamente l'accesso	Migliorativo		

Profili Professionali di cui al par. II. 3 del Capitolato Tecnico					
Profili Professionali	**Anni di esperienza richiesti**	**Anni esperienza nel ruolo**	**Numero di CV presentati**	**Numero di zip presentati per figura contenenti le certificazioni di ogni profilo professionale**	**Numero di certificati complessivi presentati per profilo professionale**
Project Manager	6 anni	4 anni			
Cloud Application Architect	8 anni	4 anni			
Cloud Application Specialist	6 anni	2 anni			
Cloud System Engineer	6 anni	4 anni			
Cloud SecOps Specialist	6 anni	2 anni			

Catalogo Servizi Cloud di cui al par. II. 4 del Capitolato Tecnico				
Ambito	**Categoria**	**Specifiche tecniche**	**Metrica di Consuntivazione**	**Tool**
Virtualizzazione	General purpose - small	1 vCPU, 2 GB RAM		
	General purpose - medium	2 vCPU, 4 GB RAM		
	General purpose - large	2 vCPU, 8 GB RAM		
	General purpose - xlarge	4 vCPU, 16 GB RAM		
	Compute optimized - medium	1 vCPU, 2 GB RAM		
	Compute optimized - large	2 vCPU, 4 GB RAM		
	Compute optimized - xlarge	4 vCPU, 8 GB RAM		
	Memory optimized - medium	1 vCPU, 8 GB RAM		
	Memory optimized - large	2 vCPU, 16 GB RAM		
	Memory optimized - xlarge	4 vCPU, 32 GB RAM		
	Storage optimized - large	2 vCPU, 16 GB RAM		
	Storage optimized - xlarge	4 vCPU, 32 GB RAM		
Storage	Block Storage Hot	SSD, High IOPS (≥5.000), latenza <1 ms		
	Block Storage Warm	HDD, medio IOPS, accesso regolare		
	Block Storage Cold	HDD, basso costo, accesso non frequente		
	Object Storage Hot	Accesso frequente, latenza bassa, ≥99,9% availability		
	Object Storage Cool	Accesso saltuario, prezzo ridotto, latenza media		
	Object Storage Cold	Accesso raro, recupero lento (ore), ≥99,99% durability		
	Object Storage Archive	Archiviazione a lungo termine, retrieval in ore		
	File Storage Hot (NAS)	NFS/SMB, throughput elevato, uso applicazioni core		
	File Storage Warm (NAS)	NFS/SMB, uso regolare, medio throughput		
	File Storage Cold (NAS)	NFS/SMB, alta capacità, basso throughput, archiviazione		
BAAS	Backup per VM/Server	Protezione istanza fino a 500 GB		
	Backup per VM/Server	Protezione istanza fino a 1 TB		
	Backup per VM/Server	Protezione istanza fino a 2 TB		
	Backup Storage	Storage attivo (SSD/HDD) – Standard		
	Backup Storage	Storage a lungo termine (Archive)		
	Backup Storage	Replica cross-region		
	Endpoint Backup	Dispositivo utente (PC/Notebook) con 1 TB incluso		
	Endpoint Backup	Storage aggiuntivo oltre 1 TB		
	Database Backup	DB relazionale fino a 100 GB		
	Database Backup	DB relazionale fino a 500 GB		
	Database Backup	DB relazionale >500 GB		
	Retention	Conservazione backup 30 giorni		
	Retention	Conservazione backup 1 anno		
	Retention	Conservazione backup 5 anni (compliance)		
PAAS	Kubernetes Managed	Cluster 3 nodi (4 vCPU, 8 GB RAM)		
	Serverless Functions	1M richieste incluse		
	AI/ML Service	Training CPU/GPU dedicato (specificare inoltre la quantità esatta di GPU H100/B200 disponibili nella UE)		
	Classe 1	-RPO: ≥72 ore		
		-RTO:≥72 ore		
		Note:Backup off-site, recovery manuale, nessuna automazione		

DRAAS	Classe 2	-RPO: 8–72 ore -RTO:<24 ore Note:Replica asincrona o backup frequenti, recovery semi-automatico		
	Classe 3	-RPO: 4–8 ore -RTO:4–8 ore Note:Replica più frequente, automazione parziale, orchestrazione DR		
	Classe 4	-RPO: 1–4 ore -RTO:1–4 ore Note:Replica quasi real-time, orchestrazione DR avanzata, test periodici		
	Classe 5	-RPO: <1 ora (anche pochi minuti) -RTO:<1 ora Note:Replica sincrona, hot site sempre pronto, failover automatico		
	Test DR annuale	Incluso nel canone		
Eventuali Items aggiunti al catalogo a cura del CSP				
Ambito	**Categoria**	**Specifiche tecniche**	**Metrica di Consuntivazione**	**Tool**

RICHIESTA DI INFORMAZIONI

"Servizi IaaS e PaaS in ambito Cloud e servizi specialistici di supporto tecnico-funzionale per la gestione, il monitoraggio e l'evoluzione delle infrastrutture digitali".

Contents

Oggetto: Richiesta di informazioni per l'affidamento dei Servizi IaaS e PaaS in ambito Cloud e dei Servizi Specialistici di supporto tecnico-funzionale per la gestione, il monitoraggio e l'evoluzione delle infrastrutture digitali, gestita con sistemi telematici.

PREMESSE

Il presente documento vuole fornire le principali informazioni affinché gli operatori economici possano formulare le proprie proposte sulla cui base FSTechnology valuterà le proposte relative a quanto in oggetto; in particolare i Servizi Cloud di tipo infrastrutturale e le relative piattaforme (IaaS e PaaS), gestite da Cloud Service Provider operanti a livello internazionale, nonché i Servizi Specialistici di supporto tecnico-funzionale per la gestione, il monitoraggio delle infrastrutture e la definizione dei modelli di erogazione dei servizi. Restano esclusi dal perimetro della presente RFI i fornitori di piattaforme applicative proprietarie (SaaS) e i servizi verticali basati su tali piattaforme.

La presente procedura pertanto è finalizzata alla raccolta di informazioni utili per la successiva definizione delle strategie di approvvigionamento. Essa non costituisce, pertanto, una procedura di gara né un impegno da parte della Società Procedente alla successiva aggiudicazione di un appalto o contratto.

CONTESTO

Il Gruppo Ferrovie dello Stato Italiane (FS) rappresenta uno dei principali attori del sistema della mobilità nazionale e internazionale, con una presenza estesa su oltre 17.000 km di rete ferroviaria, 32.000 km di rete stradale, oltre 2 milioni di passeggeri trasportati al giorno, e attività distribuite in più di 10 Paesi esteri. Il Gruppo si articola in una molteplicità di società operative che operano in differenti mercati quali il trasporto passeggeri, merci, infrastrutture, servizi tecnologici e digitali, mobilità urbana, sicurezza, certificazione, energia e finanza.

Il percorso di trasformazione digitale del Gruppo FS si basa su un modello di erogazione ibrido, che integra ambienti on-premise e cloud per garantire resilienza, sicurezza e capacità evolutiva e prevede la reale possibilità di incrementare la quota parte dei servizi gestiti in Cloud rispetto all'attuale rapporto Cloud vs On Premise. L'adozione di architetture cloud-native, piattaforme PaaS e strumenti avanzati di data analytics si inserisce in un contesto operativo in cui coesistono:

- centinaia di sedi e stabilimenti dislocati su tutto il territorio nazionale e estero;
- un portafoglio applicativo ampio ed eterogeneo, con esigenze specifiche in termini di interoperabilità e modernizzazione;

- presenza di sistemi legacy verticali e una crescente adozione di container e servizi cloud gestiti;
- esigenze di sovereign cloud e compliance territoriale nella localizzazione dei dati e dei workload;
- vincoli stringenti sulla continuità operativa e sulla sicurezza informatica dei servizi digitali mission-critical.

In tale contesto, il percorso di evoluzione e modernizzazione dell'infrastruttura digitale del Gruppo si sviluppa tenendo conto della sua complessità organizzativa e tecnologica, tipica di una realtà multi-aziendale, multi-paese e soggetta a vincoli regolatori diversificati.

Architettura logica della Data platform

Il Gruppo FS ha avviato, inserendolo tra i suoi progetti più importanti, anche lo studio e l'implementazione di una Data Platform la cui architettura è di seguito rappresentata. Quest'ultima è articolata in layer logici, ciascuno dedicato a una specifica fase del ciclo di vita del dato: dalla raccolta iniziale fino all'utilizzo attraverso applicazioni e servizi. Ogni layer comprende una serie di servizi selezionabili e attivabili in funzione del contesto operativo, delle prestazioni richieste e degli obiettivi di business.

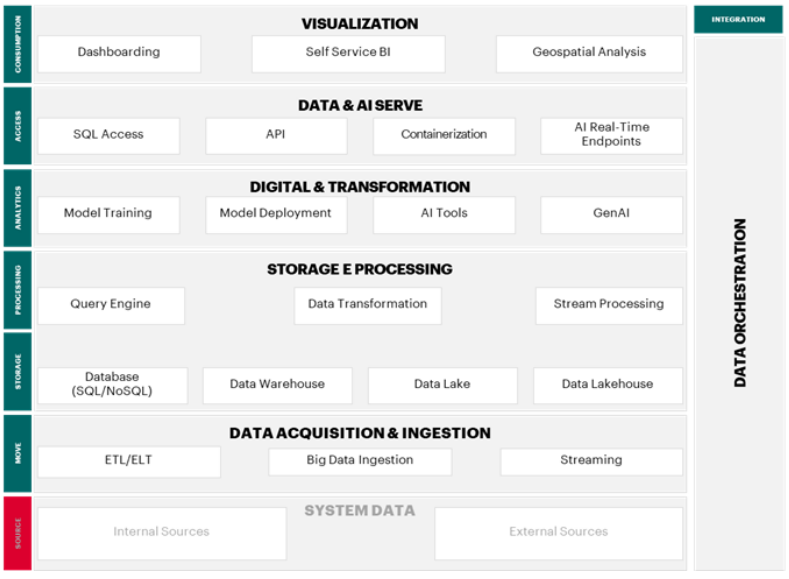

Figura 1 Architettura logica dei Servizi di riferimento

I. DESCRIZIONE DELL'OGGETTO E DEGLI OBIETTIVI

La Richiesta di Informazioni (RFI) ha per oggetto i Servizi Cloud di tipo infrastrutturale e le relative piattaforme (IaaS e PaaS), nonché i Servizi Specialistici di supporto tecnico-funzionale a supporto della gestione, del monitoraggio e dell'evoluzione delle infrastrutture digitali della Società Procedente.

L'obiettivo dell'iniziativa è acquisire informazioni e contributi tecnico-economici dal mercato al fine di supportare la Società Procedente nella definizione della successiva strategia di approvvigionamento, volta ad assicurare la disponibilità di servizi Cloud e professionali in linea con i più elevati standard di efficienza, sicurezza e scalabilità.

In particolare, la presente RFI si propone di:

- Raccogliere informazioni tecniche e qualitative sui servizi IaaS e PaaS erogabili, con riferimento a soluzioni Cloud e modelli architetturali ibridi;
- Valutare le capacità operative, tecnologiche e organizzative degli operatori economici nel fornire servizi specialistici di gestione, automazione e supporto tecnico alle infrastrutture digitali;
- Acquisire indicazioni utili in merito alle strategie di migrazione da On Premise a Cloud, ai modelli contrattuali e alle opzioni di servizio più idonee a garantire continuità operativa, sicurezza e ottimizzazione dei costi;
- Supportare un'eventuale fase successiva di approfondimento a sostegno della strategia interna di procurement, fornendo elementi utili alla definizione di modelli di erogazione e gestione dei servizi più efficienti e sostenibili per la Società Procedente.

Non saranno prese in considerazione offerte o proposte economiche vincolanti in questa fase, in quanto la presente RFI ha finalità esclusivamente conoscitive e non costituisce impegno all'affidamento da parte della Società Procedente.

L'iniziativa risponde a driver strategici ben definiti, tra cui:

- Resilienza e continuità operativa: assicurare la piena disponibilità dei servizi mission-critical attraverso architetture robuste e affidabili;
- Sicurezza e compliance: garantire l'aderenza ai requisiti normativi e regolatori nazionali ed europei in materia di protezione dei dati e gestione dei servizi digitali;
- Efficienza e ottimizzazione dei costi: promuovere un'evoluzione progressiva dell'attuale assetto infrastrutturale verso soluzioni cloud-based, nel rispetto della sostenibilità economica;

- Innovazione tecnologica: abilitare l'adozione di tecnologie avanzate, quali piattaforme PaaS e soluzioni di intelligenza artificiale, a supporto della trasformazione digitale e dello sviluppo di nuovi modelli di servizio.

II. DETTAGLI SULLA RICHIESTA DI INFORMAZIONI

L'iniziativa è finalizzata a raccogliere dal mercato informazioni tecniche, organizzative e qualitative a supporto della strategia di trasformazione digitale e cloud. Le informazioni richieste sono organizzate in quattro sezioni, ciascuna mirata ad approfondire specifici ambiti di interesse:

1. **Requisiti Minimi e valutativi**: sezione volta a verificare la presenza di capacità tecniche, organizzative e di sicurezza necessarie a garantire affidabilità, resilienza e conformità normativa. I requisiti sono articolati in due categorie:
    - **Requisiti minimi o distintivi tecnici e di sicurezza**: riguardano aspetti infrastrutturali, di sicurezza, disponibilità dei servizi e conformità, considerati indispensabili per la Società Procedente o distintivi. Per ciascun requisito sarà verificata la presenza o l'assenza presso l'Operatore Economico, al fine di attestare il possesso delle capacità richieste.
    - **Requisiti valutativi tecnici e di sicurezza a carattere qualitativo**: rappresentano ambiti nei quali viene richiesto all'Operatore Economico di fornire informazioni qualitative e descrittive in merito alle proprie soluzioni, metodologie e approcci operativi, con l'obiettivo di raccogliere elementi utili a comprendere il livello di maturità, innovazione ed efficienza dei servizi offerti.
2. **Use Case e Scenari di Migrazione Cloud**: sezione dedicata alla valutazione di soluzioni, strumenti e approcci metodologici per la gestione di scenari concreti di migrazione e modernizzazione infrastrutturale e applicativa.
3. **Profili Professionali**: sezione dedicata alla descrizione delle competenze e delle qualifiche professionali disponibili presso l'Operatore Economico, con particolare riferimento a certificazioni, esperienze e specializzazioni tecniche e gestionali. L'obiettivo è raccogliere informazioni utili a comprendere il livello di maturità e approfondimento delle competenze rese disponibili nell'ambito dei servizi oggetto della presente richiesta
4. **Catalogo Servizi Cloud**: sezione finalizzata alla raccolta e alla strutturazione di un catalogo dei servizi Cloud di tipo IaaS e PaaS, elaborato a partire da un pre-inventario non esaustivo fornito dalla Società Procedente. L'Operatore Economico è invitato a integrare e completare le informazioni con le proprie specifiche di servizio, potendo inserire più occorrenze per ciascuna tipologia di servizio e/o fornendo ulteriori dettagli tecnici ritenuti pertinenti.
5. **Criteri di sostenibilità**: sezione finalizzata alla raccolta delle certificazioni o attestazioni dell'Operatore Economico in ambito sostenibilità.

II. 1 REQUISITI MINIMI E VALUTATIVI

L'Operatore Economico è invitato a indicare e il possesso dei requisiti minimi tecnici e di sicurezza, differenziati nella tipologia dei requisiti in necessari ("Obbligatori"), per assicurare l'erogazione dei servizi secondo gli standard attesi o distintivi ("Migliorativi"), rappresentanti elementi di eccellenza e valore aggiunto proposti dall'Operatore rispetto alle prestazioni base.

II. 1.1 REQUISITI MINIMI O DISTINTIVI TECNICI

ID	Ambito	Descrizione	Tipologia
R1	Governance	Chiarisce ruoli e responsabilità tra provider e cliente nella gestione della sicurezza	Obbligatorio
R2	Infrastruttura	Presenza di almeno tre Availability Zone fisicamente separate all'interno di una regione situata nell'Unione Europea	Obbligatorio
R3	Affidabilità	Garanzia di SLA per servizi IaaS e PaaS (calcolo, storage, database)	Obbligatorio
R4	Prestazioni	Capacità della piattaforma di scalare orizzontalmente e verticalmente	Obbligatorio
R5	Localizzazione	Presenza di regioni cloud fisicamente localizzate nell'UE/SEE	Obbligatorio
R6	Localizzazione	Possibilità di vincolare l'erogazione dei servizi alla sola UE	Obbligatorio
R7	Data Acquisition & Ingestion - Big Data	La capacità si riferisce al processo attraverso cui grandi volumi di dati, provenienti da fonti eterogenee, vengono raccolti, trasferiti e preparati per essere archiviati ed elaborati in sistemi come Data Lake o Data Warehouse.	Obbligatorio
R8	Data Acquisition & Ingestion - Big Data	Capacità della piattaforma di supportare lo scaling automatico delle risorse in base al volume dei dati ricevuto con un limite di throughput massimo documentato (espresso in GB/min o record/sec) in grado di gestire carichi concorrenti senza degrado delle performance.	Migliorativo
R9	Data Acquisition & Ingestion - Streaming	Questa capacità consente l'estrazione, l'ingestione e l'elaborazione continua dei dati come flussi di eventi in tempo reale, incluse le integrazioni di	Obbligatorio

		flusso, e li fornisce ai sistemi di destinazione per un consumo immediato.	
R10	Data Acquisition & Ingestion - Streaming	Il sistema mette a disposizione moduli specifici per il riconoscimento di eventi duplicati o non ordinati in modo da garantire un'elaborazione “exactly-once”.	Migliorativo
R11	Data Acquisition & Ingestion - ETL/ELT	Il principio si riferisce alle seguenti due capacity: 1. Batch capacity: capacità di elaborare grandi volumi di dati a intervalli regolari; 2. Micro-batch capacity: capacità di elaborare piccoli volumi di dati in modo frequente, con tempi di aggiornamento molto più rapidi.	Obbligatorio
R12	Data Acquisition & Ingestion - ETL/ELT	La piattaforma mette a disposizione strumenti di suggerimento per l'ottimizzazione delle prestazioni in ambito ETL o ELT.	Migliorativo
R13	Storage & Processing - Data Lakehouse	Lo storage gestisce la varietà e il volume di dati di strutture variabili attraverso un’ampia gamma di carichi di lavoro analitici che spaziano dall’analisi tradizionale alla data science. I dati possono essere fisicamente distribuiti.	Obbligatorio
R14	Storage & Processing - Data Lakehouse	La federazione dei cataloghi dei metadati del Lake house è attiva e consente di sincronizzare le modifiche sugli oggetti e sulle query engine in modo da avere sempre una vista aggiornata e coerente a tutti gli utenti che operano sulla piattaforma.	Migliorativo
R15	Storage & Processing - Data Lakehouse	La piattaforma gestisce le risorse di calcolo (autoscaling) in funzione di carico, priorità e tipologia di query, con ottimizzazione dei costi.	Migliorativo
R16	Storage & Processing - Query Engine	Il Query Engine è il componente della Data Platform che gestisce e ottimizza l’esecuzione delle interrogazioni sui dati. Deve essere	Obbligatorio

		in grado di accedere, leggere e analizzare i dati in modo efficiente	
R17	Storage & Processing - Query Engine	La piattaforma consente di effettuare data enrichment in tempo reale utilizzando fonti esterne (API, lookup su database o servizi di terze parti) direttamente durante il processing.	Migliorativo
R18	Storage & Processing - Query Engine	La piattaforma consente di gestire in modo efficiente carichi analitici misti, supportando contemporaneamente query interattive a bassa latenza e processi batch intensivi senza interferenze o degrado delle prestazioni	Migliorativo
R19	Storage & Processing - Stream Processing	Questa capacità gestisce dati che vengono scritti ad alta frequenza e volume. Le query vengono eseguite in tempo reale sia per la valutazione dei dati rispetto ai modelli, sia per la sintesi degli eventi. I dati sono misti per struttura e dimensione.	Obbligatorio
R20	Storage & Processing - Stream Processing	La piattaforma supporta la crittografia dei dati in transito e a riposo	Migliorativo
R21	Storage & Processing - Data Lake	Archivio centralizzato che permette di raccogliere, memorizzare e gestire grandi volumi di dati eterogenei (strutturati, semi-strutturati e non strutturati), così come sono, senza necessità di trasformarli immediatamente.	Obbligatorio
R22	Storage & Processing - Data Lake	Il sistema abilita un logging di accesso a ciascuno dei suoi oggetti	Migliorativo
R23	Storage & Processing - Data Lake	Lo storage degli oggetti offre livelli di classe di storage distinti per soddisfare la necessità di storage "hot" con accesso frequente e performante, storage "cool" a cui si accede meno spesso e storage "cold" a cui si accede raramente.	Migliorativo
R24	Storage & Processing - Data Transformation	Questa capacità rappresenta il processo mediante il quale i dati vengono convertiti, puliti e	Obbligatorio

		ristrutturati per essere resi coerenti, affidabili e utilizzabili nei sistemi di analisi o integrazione. Comprende operazioni come la normalizzazione dei formati, la conversione dei tipi di dato, la rimozione dei duplicati, l'arricchimento con informazioni aggiuntive e l'applicazione di regole di business.	
R25	Storage & Processing - Data Transformation	La piattaforma consente l'implementazione di trasformazioni semantiche (i.e. standardizzazione, mapping di codici, regole di business) e di trasformazioni condizionali o parametriche (i.e. basate su logiche dinamiche).	Migliorativo
R26	Storage & Processing - Data Warehouse	Sistema centralizzato che raccoglie dati strutturati da diverse fonti, li integra e li organizza per supportare analisi, reporting e business intelligence. È ottimizzato per query complesse, conserva dati storici e permette di ottenere rapidamente insight utili per le decisioni aziendali.	Obbligatorio
R27	Storage & Processing - Data Warehouse	Lo storage si integra con strumenti di Business Intelligence e reporting più diffusi sul mercato quali Power BI, Tableau, Qlik Sense.	Migliorativo
R28	Digital & Transformation – AI Tools	Capacità della piattaforma di offrire un ecosistema integrato di strumenti e servizi di AI-as-a-Service, abilitando lo sviluppo, la sperimentazione e la gestione collaborativa di soluzioni di intelligenza artificiale.	Obbligatorio
R29	Digital & Transformation – AI Tools	La piattaforma fornisce ambienti collaborativi multiutente che permettono la creazione di workspace condivisi e sandbox sicure per la sperimentazione, con gestione granulare di ruoli, permessi, versioning e isolamento delle risorse.	Migliorativo

R30	Digital & Transformation – AI Tools	La piattaforma supporta la creazione di pipeline automatizzate per attività di data preparation, feature engineering e model training, integrabili con strumenti MLOps e con workflow orchestration per l'esecuzione e la gestione end-to-end dei processi di AI.	Migliorativo
R31	Digital & Transformation - Gen AI	Capacità della piattaforma di abilitare, integrare e rendere operativi servizi di intelligenza artificiale generativa.	Obbligatorio
R32	Digital & Transformation - Gen AI	La piattaforma dispone di un Model Registry integrato per la registrazione, il versioning, la governance e la tracciabilità dei modelli e degli agenti AI disponibili.	Migliorativo
R33	Digital & Transformation - Gen AI	La piattaforma supporta il provisioning di unità di throughput garantite (PTU) o di risorse computazionali equivalenti dedicate, al fine di assicurare prestazioni costanti e a bassa latenza per carichi mission-critical e di garantire prevedibilità dei costi operativi anche in scenari di utilizzo intensivo.	Migliorativo
R34	Digital & Transformation - Gen AI	La piattaforma garantisce controlli nativi o integrabili di sicurezza e conformità (AI Guardrails) per garantire l'affidabilità dei contenuti generati, inclusi filtri automatici di contenuto tossico o sensibile e meccanismi di moderazione.	Migliorativo
R35	Digital & Transformation - Model Training	Capacità della piattaforma di abilitare, orchestrare e ottimizzare l'intero ciclo di vita dell'addestramento dei modelli di machine learning, garantendo un'integrazione fluida tra preparazione dei dati, training, tuning, versioning e monitoraggio delle performance.	Obbligatorio

R36	Digital & Transformation - Model Training	La piattaforma supporta nativamente il ciclo completo di sviluppo Machine Learning, comprendente data preparation, feature engineering, training, hyperparameter tuning e model registry, in ambienti integrati, automatizzati e governati.	Migliorativo
R37	Digital & Transformation - Model Deployment	La capacità della piattaforma di gestire in modo scalabile, sicuro e governato la messa in produzione dei modelli di intelligenza artificiale, garantendo continuità operativa e osservabilità.	Obbligatorio
R38	Digital & Transformation - Model Deployment	La piattaforma fornisce funzionalità di monitoraggio e osservabilità dei modelli in produzione, consentendo di identificare tempestivamente problemi di prestazioni o errori, possibilità di scaling.	Migliorativo
R39	Data & AI Serve – AI Real Time Endpoints	La capacità di esporre modelli di AI/ML come endpoint scalabili, sicuri e a bassa latenza per l'inferenza in tempo reale.	Obbligatorio
R40	Data & AI Serve - AI Real Time Endpoints	La piattaforma supporta il model serving su endpoint in tempo reale (real-time), garantendo bassa latenza e alta disponibilità, con configurazione personalizzabile della capacità computazionale per assicurare performance costanti delle API di inferenza anche a carichi elevati o frequenze di chiamata elevate.	Migliorativo
R41	Data & AI Serve API	La capacità API (Application Programming Interface) rappresenta un insieme di regole, protocolli e strumenti che permettono a diversi software di comunicare tra loro.	Obbligatorio
R42	Data & AI Serve - API	La piattaforma garantisce un'autenticazione sicura con protocolli OAuth2, API Key, JWT, certificato digitale.	Migliorativo

R43	Data & AI Serve - Containerization	Supporto per la distribuzione e l'esecuzione di carichi di lavoro containerizzati.	Obbligatorio
R44	Containerization	La piattaforma offre un'infrastruttura gestita o containerizzabile per l'esposizione dei modelli come servizio, con supporto a protocolli standard e capacità di personalizzazione dell'infrastruttura e configurazione di scalabilità e alta disponibilità (autoscaling automatico, e bilanciamento del carico) per garantire efficienza e resilienza del servizio di inferenza.	Migliorativo
R45	Data & AI Serve - SQL Access	Capacità della piattaforma proposta di fornire un accesso standardizzato, affidabile ed efficiente ai dati relazionali tramite SQL (Structured Query Language), in conformità con gli standard internazionali. Questa capacità assicura che il sistema possa offrire funzionalità di interrogazione, gestione e sicurezza dei dati strutturati, nel rispetto delle esigenze di scalabilità aziendale, interoperabilità e conformità.	Obbligatorio
R46	Data & AI Serve - SQL Access	La piattaforma offre un query optimizer supporta approcci sia cost-based che rule-based che generano piani di esecuzione adattivi basati su statistiche aggiornate.	Migliorativo
R47	Data & AI Serve - SQL Access	La piattaforma dispone di masking dinamico dei dati per proteggere informazioni sensibili.	Migliorativo
R48	Visualization - Dashboarding	Supporto per dashboard altamente interattive e per l'esplorazione dei dati attraverso la manipolazione visiva dei grafici. La capacità di visualizzazioni interattive dei dati, incluse tabelle, grafici e testo in linguaggio naturale, si organizza intorno ad	Obbligatorio

		aree tematiche logiche per comunicare una data story.	
R49	Visualization - Dashboarding	Lo strumento di BI supporta la creazione di dashboard interattive e report con funzionalità di drill-down, slicing e pivoting su più dimensioni, incluse capacità OLAP e modelli multidimensionali.	Migliorativo
R50	Visualization - Dashboarding	Lo strumento di BI consente agli utenti di visualizzare e analizzare reti e grafi di relazioni.	Migliorativo
R51	Visualization - Geospatial Analysis	La capacità di costruire mappe, grafici, statistiche e cartogrammi a partire da dati geospaziali per rivelare pattern e relazioni.	Obbligatorio
R52	Visualization - Geospatial Analysis	Lo strumento di BI offre supporto nativo a tipi di dato geografico (GEOGRAPHY), funzioni spaziali (ad es. buffer, intersection, ST_*, clustering) e visualizzazioni geografiche avanzate (heatmap, layers, shape/GeoJSON).	Migliorativo
R53	Visualization - Self Service BI	Questa capacità consente agli utenti di connettersi ai dati, produrre e condividere analisi senza dipendere dall'IT per l'operatività delle analisi.	Obbligatorio
R54	Visualization - Self Service BI	Il servizio di data visualization mette a disposizione modalità di conversational BI nativa per poter interrogare la base dati con Natural Language Query (NLQ) con più di una lingua straniera.	Migliorativo
R55	Integration - Data Orchestration	La gestione aumentata dei dati utilizza il machine learning e l'intelligenza artificiale per automatizzare attività come la qualità dei dati, l'integrazione, la preparazione, la catalogazione, la gestione dei carichi di lavoro, la scoperta di insight e la condivisione. Applica la significatività statistica e il contesto aziendale per migliorare le attività umane e supportare ruoli come i citizen integrator e i citizen data scientist. Nelle	Obbligatorio

		architetture moderne, è essenziale per gestire rapidamente grandi volumi di dati multistrutturati, spostando le pratiche da un design personalizzato verso data fabric guidati dai metadati e assistiti dall'intelligenza artificiale.	
R56	Integration - Data Orchestration	La piattaforma mette a disposizione l'orchestrazione assistita da AI e guidata dai metadata in linea con approcci moderni di data fabric.	Migliorativo

II. 1.2 REQUISITI MINIMI O DISTINTIVI DI SICUREZZA

ID	Ambito	Descrizione	Tipologia
RCY.1	Governance e Compliance (GOV)	Il CSP deve porre in essere tutti i controlli e le misure tecnologiche ed organizzative necessarie a garantire un adeguato livello di sicurezza logica a tutto il dominio dei sistemi, servizi, dati e informazioni del Cliente.	Obbligatorio
RCY.2	Governance e Compliance (GOV)	È fatto richiamo al CSP nell'utilizzo di un comportamento etico e riservato in tutta la filiera della gestione delle informazioni del Cliente con cui verrà in contatto e di cui dovrà salvaguardare l'integrità e la disponibilità per il proprio mandato o per autorizzazione diretta del Cliente.	Obbligatorio
RCY.3	Governance e Compliance (GOV)	Il CSP dovrà garantire che il modello di gestione della sicurezza, le architetture e le tecnologie impiegate per l'erogazione del servizio siano soggetti a un'evoluzione continua, in linea con gli standard di sicurezza, le normative vigenti e le best practice di settore, al fine di garantire un livello adeguato di protezione nel tempo.	Obbligatorio
RCY.4	Governance e Compliance (GOV)	I datacenter e le informazioni/servizi in Cloud devono risiedere su territorio nazionale o all'interno dello Spazio Economico Europeo.	Obbligatorio
RCY.5	Governance e Compliance (GOV)	Il CSP dovrà garantire la possibilità a Ferrovie dello Stato di effettuare audit, ispezioni, verifiche di sicurezza e monitoraggi con proprio personale o tramite società terze, per verificare la rispondenza di quanto prescritto a quanto eseguito, garantendo il sostegno e la	Obbligatorio

		collaborazione adeguata e necessaria allo svolgimento delle attività di audit e verifica.	
RCY.6	Governance e Compliance (GOV)	Il CSP si impegna a garantire il rispetto di tutti gli standard normativi e le prescrizioni operative previste dalla Direttiva NIS 2, adeguando la fornitura per tutta la durata del contratto. A tal fine, dovrà assicurare la piena conformità alla normativa vigente, in particolare: - le misure di sicurezza stabilite all'allegato B del Decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81, di cui all'articolo 1, comma 2, lettera b), del Decreto-Legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla Legge 18 novembre 2019, n. 133; - le misure di sicurezza di base previste nell'Allegato 2 della Determinazione dell'Agenzia per la Cybersicurezza Nazionale n. 164179 del 14 aprile 2025, attuativa del Decreto Legislativo 4 settembre 2024, n. 138 (cd. "Decreto NIS"); - gli elementi essenziali di cybersicurezza dei beni e dei servizi informatici di cui all'Allegato 1 del Decreto del Presidente del Consiglio dei Ministri 30 aprile 2025, attuativo della Legge 28 giugno 2024, n. 90. Il CSP si impegna a garantire la piena conformità al Regolamento (UE) 2016/679 (GDPR), in tutte le attività di trattamento dei dati personali, inclusi i casi di trasferimento dei dati all'estero. Altresì, nel rispetto delle leggi, norme e direttive vigenti, tra cui il Regolamento UE 2016/679 General Data Protection Regulation (GDPR) e relativi decreti e regolamenti attuativi, i principi guida nella definizione e nell'attuazione del modello di sicurezza prendono a riferimento i principali standard e best practice internazionali, tra i quali si citano a titolo esemplificativo e non esaustivo i seguenti e successive revisioni: • COBIT5; • NIST Cybersecurity Framework for Critical Infrastructure, SP 800-145, SP 800-144, SP 500-299; • ENISA Security and Resilience in	Obbligatorio

		Governmental Clouds; • Cloud Control Matrix.	
RCY.7	Governance e Compliance (GOV)	Il CSP del servizio cloud deve dimostrare il possesso di seguenti certificazioni di sicurezza e conformità riconosciute, garantendo il rispetto degli standard di settore per la protezione dei dati e la gestione della sicurezza: • ISO/IEC 27001:2022 (Obbligatoria) • CSA STAR Level 1 (Obbligatoria) • ACN (Ex-AGID) (Obbligatoria per servizi PA) • PCI-DSS Level 4 (Obbligatoria per gestione transazioni su circuiti di pagamento)	Obbligatorio
RCY.8	Governance e Compliance (GOV)	Il CSP del servizio cloud deve dimostrare il possesso di seguenti certificazioni opzionali di sicurezza e conformità riconosciute, garantendo il rispetto degli standard di settore per la protezione dei dati e la gestione della sicurezza: • CSA STAR Level 2 • ISO/IEC 42001 • ISO/IEC 27017 • ISO/IEC 27018 •ISO/IEC 27002 •ISO/IEC 27701 •ISO/IEC 27031 • ISO/IEC 22301 • SOC 2 • SOC 3	Migliorativo
RCY.9	Governance e Compliance (GOV)	I processi di gestione del rischio riguardanti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione. Ovvero sono presenti ed aggiornate almeno su base annuale le politiche e le procedure per la definizione, l'implementazione e l'applicazione del modello di responsabilità della sicurezza condivisa rispetto a soggetti esterni e/o Amministrazioni terze (Shared Security Responsibility Model-SSRM).	Obbligatorio
RCY.10	Governance e Compliance (GOV)	Il CSP deve adottare un programma di gestione della sicurezza della supply chain che comprenda: La verifica e il monitoraggio della sicurezza dei propri sub-fornitori;	Obbligatorio

		L'obbligo per i sub-fornitori di aderire a requisiti di sicurezza equivalenti.	
RCY.11	Governance e Compliance (GOV)	Il CSP deve garantire che tutto il personale, in particolare il Top Management, abbia completato un programma di formazione iniziale e aggiornamenti periodici (almeno annuali) sulla sicurezza informatica.	Obbligatorio
RCY.12	Governance e Compliance (GOV)	Il CSP deve mantenere un inventario aggiornato di tutti gli asset, includendo hardware, software, dispositivi di rete e risorse virtuali. Tale inventario deve: - Essere integrato con un sistema di Asset Management centralizzato. - Specificare per ciascun asset informazioni critiche come proprietà, ubicazione, versione, stato e criticità rispetto alla sicurezza.	Obbligatorio
RCY.13	Governance e Compliance (GOV)	Il CSP dovrà adottare framework e attestazioni di sicurezza conformi agli standard internazionali (es. SLSA – Supply-chain Levels for Software Artifacts o NIST Secure Software Development Framework), per garantire la sicurezza della propria catena di fornitura software e la tracciabilità del processo di sviluppo.	Obbligatorio
RCY.14	Governance e Compliance (GOV)	Il CSP dovrà garantire la chiara identificazione e la definizione formale dei ruoli e delle responsabilità in ambito IT Security e Data Protection. Questo includerà l'identificazione delle persone coinvolte nella gestione delle informazioni, dei dati e nel trattamento dei dati personali, con una comunicazione chiara dei ruoli e delle responsabilità assegnate all'organizzazione	Obbligatorio
RCY.15	Gestione Identità e Accessi (IAM)	Il CSP dovrà garantire l'adozione di un modello di sicurezza "Zero Trust" come approccio strategico alla sicurezza informatica che protegge l'organizzazione eliminando la fiducia implicita e convalidando continuamente ogni fase di un'interazione digitale.	Obbligatorio

RCY.16	Gestione Identità e Accessi (IAM)	Il CSP dovrà garantire l'adeguato presidio della sicurezza logica attraverso la presenza di politiche e procedure di sicurezza delle informazioni dell'intera organizzazione che indirizzano la gestione delle utenze e degli accessi ai sistemi informatici in funzione del livello autorizzativo (es. Admin, utenti base, utenti amministratore, etc.) garantendo la revisione periodica delle utenze, password policy e adeguate misure prescrittive per amministratori di sistema e le utenze privilegiate secondo i principi di SOC 2 e CSA STAR.	Obbligatorio
RCY.17	Gestione Identità e Accessi (IAM)	Il CSP dovrà garantire l'adeguata gestione delle utenze e degli accessi ai servizi e ai sistemi mediante meccanismi di gestione delle password per valutarne complessità, scadenza, non riutilizzabilità delle precedenti, etc.	Obbligatorio
RCY.18	Gestione Identità e Accessi (IAM)	Il CSP dovrà garantire l'adeguata gestione degli accessi ai sistemi e ai servizi attraverso sistemi di autenticazione multi-fattore, garantendo un processo di autenticazione forte (MFA)	Obbligatorio
RCY.19	Gestione Identità e Accessi (IAM)	Il CSP dovrà fornire strumenti che consentano di garantire che tutte le utenze siano associate univocamente a persone fisiche identificabili e, per utenze Machine-to-Machine, attribuite a un unico soggetto responsabile.	Obbligatorio
RCY.20	Gestione Identità e Accessi (IAM)	Il CSP dovrà fornire strumenti che consentano di garantire l'adeguata gestione delle utenze e degli accessi ai servizi e ai sistemi mediante implementazione di controlli che permettano di definire quali operazioni possa compiere uno specifico utente nel rispetto dei principi di "Least Privilege" e "Need to Know".	Obbligatorio
RCY.21	Gestione Identità e Accessi (IAM)	Il CSP dovrà fornire strumenti che consentano di garantire l'adeguata gestione delle utenze e degli accessi ai servizi e ai sistemi mediante implementazione di controlli specifici cadenzati sulle utenze con privilegi ampi per impedire operazioni illecite.	Obbligatorio

RCY.22	Gestione Identità e Accessi (IAM)	l processo di autenticazione e autorizzazione deve essere disaccoppiato. L'autenticazione deve essere gestita dall'Identity Provider di Gruppo (AzureAD) mediante meccanismi di modern authentication (es. OAuth2) e soggetta a politiche di Multi-Factor Authentication (MFA). L'autorizzazione deve essere gestita a livello applicativo, prevedendo diversi livelli di profilazione basati sui coni di visibilità coerenti con ruoli e responsabilità degli utenti. È inoltre richiesto il riesame periodico dei diritti di accesso, con cadenza più frequente per gli utenti privilegiati (es. ogni 6 mesi) e processi di provisiong e de-provisiong.	Obbligatorio
RCY.23	Gestione Identità e Accessi (IAM)	Il CSP dovrà implementare meccanismi di accesso temporaneo (Just-in-Time) o credenziali effimere, al fine di ridurre il rischio derivante da privilegi permanenti o non necessari, garantendo che l'accesso amministrativo avvenga solo per il tempo strettamente indispensabile all'esecuzione delle attività autorizzate.	Obbligatorio
RCY.24	Gestione Identità e Accessi (IAM)	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 dell'accesso (ad esempio password, token o biometrico).	Obbligatorio
RCY.25	Sicurezza delle Informazioni e dei Dati (INF)	I servizi erogati dal CSP dovranno in particolare assicurare sempre il migliore isolamento possibile dei dati e delle informazioni del Cliente anche per strumenti, sistemi o servizi condivisi e non dedicati, e garantirne la riservatezza nei confronti di accessi non autorizzati o non necessari.	Obbligatorio

RCY.26	Sicurezza delle Informazioni e dei Dati (INF)	Il CSP dovrà garantire che le chiavi di crittografia di sua responsabilità – ad eccezione di casi specifici nei quali sarà pertinenza del Gruppo FS - siano generate in modo sicuro impedendo la diffusione delle chiavi di cifratura con soggetti non autorizzati. Su esplicita richiesta del Cliente, il CSP dovrà abilitare la modalità BYOK.	Obbligatorio
RCY.27	Sicurezza delle Informazioni e dei Dati (INF)	Il CSP dovrà garantire la protezione dei dati, mediante cifratura, mascheramento, anonimizzazione, segregazione: esistenza di tecniche di cifratura dei dati memorizzati (es. dati memorizzati nei database o nelle memorie di massa). In particolare, Il CSP dovrà garantire la protezione dei dati, sia a riposo che in transito, attraverso le seguenti misure: Cifratura: Utilizzo di algoritmi di cifratura riconosciuti come sicuri in conformità con gli standard internazionali (es. AES-256). per proteggere la riservatezza delle informazioni sensibili, nonché delle informazioni soggette a requisiti legali e normativi. Integrità dei dati: Implementazione di tecniche per verificare se le informazioni critiche sono state alterate, ad esempio tramite funzioni hash o firme digitali. Mascheramento dei dati: Adozione di tecniche di data masking per minimizzare la visualizzazione e lettura di dati personali, applicando il principio del "need to know" per limitare l'accesso alle informazioni. Queste misure devono essere integrate nella soluzione offerta dal CSP per garantire il rispetto delle normative vigenti e la protezione delle informazioni dell'organizzazione	Obbligatorio
RCY.28	Sicurezza delle Informazioni e dei Dati (INF)	Il CSP dovrà garantire la cancellazione dei dati e dismissione sicura dei dispositivi HW/SW utilizzati nell'ambito dell'erogazione dei servizi al Cliente, incluse le Postazioni di Lavoro del personale coinvolto dal CSP.	Obbligatorio
RCY.29	Sicurezza delle Informazioni e dei Dati (INF)	Deve essere prevista la definizione di policy e procedure per abilitare il labeling, handling e la sicurezza sui dati.	Obbligatorio

RCY.30	Sicurezza delle Informazioni e dei Dati (INF)	Il servizio prevede l'implementazione di un sistema di gestione dei diritti digitali (DRM) per proteggere le informazioni del cliente e i software più critici che vengono utilizzati al di fuori del controllo dell'organizzazione.	Migliorativo
RCY.31	Sicurezza delle Informazioni e dei Dati (INF)	Il CSP dovrà adottare soluzioni adeguate a protezione del perimetro (garantendone il costante aggiornamento sia automatico che, se necessario, manuale) attraverso: Data Loss Prevention (DLP) per monitorare i flussi di dati all'interno della rete dell'organizzazione ed evidenziare eventuali anomalie.	Migliorativo
RCY.32	Sicurezza Applicativa (APPSEC)	Il CSP dovrà fornire strumenti che supportino l'adeguato presidio della sicurezza logica attraverso la gestione del ciclo di sviluppo sicuro del software, garantendo l'aderenza agli standard e alla normativa di settore quali OWASP e AGID e assicurando la scrittura di codice sicuro delle applicazioni nel loro specifico ambiente di sviluppo. Il CSP dovrà mettere a disposizione funzionalità e strumenti che supportino l'adozione di un approccio 'security by design' nello sviluppo e nella gestione del software, consentendo l'integrazione di misure di sicurezza fin dalle fasi iniziali del ciclo di vita applicativo, in conformità con le best practice di settore (es. OWASP, Secure SDLC).	Obbligatorio
RCY.33	Sicurezza Applicativa (APPSEC)	Il CSP deve mettere a disposizione la possibilità di creare ambienti distinti che consentano al cliente di svolgere le attività di sviluppo separatamente dall'ambiente di Esercizio	Obbligatorio
RCY.34	Sicurezza Applicativa (APPSEC)	In caso di applicazione di tipo web, il CSP dovrà fornire strumenti volti a garantirne la protezione mediante utilizzo di Web Application Firewall & API Protection per la protezione dei sistemi a livello di applicazione.	Obbligatorio

RCY.35	Sicurezza Applicativa (APPSEC)	Il CSP dovrà fornire e mantenere disponibili strumenti che consentano al Cliente di monitorare e tracciare in modo trasparente i costi infrastrutturali, i costi delle componenti software, delle librerie e delle dipendenze utilizzate, al fine di permettere una visibilità completa e una gestione ottimale delle spese operative	Obbligatorio
RCY.36	Sicurezza Applicativa (APPSEC)	L'applicazione deve assicurare, attraverso opportuni meccanismi di convalida, che tutti i parametri in input, specificati dall'utente, siano congruenti a quanto atteso. In particolare, sui dati acquisiti in ingresso, l'applicazione deve prevedere l'implementazione di meccanismi di controllo che limitino il set di caratteri o valori, inseribili dall'utente, solo a quelli congruenti ai campi richiesti e/o alle form di pertinenza, al fine di identificare ed annullare gli effetti di errori quali valori out-of-range o non pertinenti, caratteri invalidi negli stream, dati mancanti, etc. Per quanto riguarda i caratteri speciali, se presenti/richiesti in input, sono considerati pericolosi poiché la loro combinazione non può essere considerata semplice 'testo'.	Obbligatorio
RCY.37	Sicurezza Applicativa (APPSEC)	Il CSP deve mettere a disposizione strumenti che supportino la possibilità di rendere disponibile un account di test per ogni ruolo ed un URL utilizzabili dal cliente per effettuare ogni tipo di verifica necessaria per il rilascio di nuove evolutive.	Obbligatorio
RCY.38	Business Continuity e Disaster Recovery (BC/DR)	Il CSP dovrà essere dotato di procedure e sistemi in grado di garantire il backup e recovery dei dati e dei sistemi, garantendo la protezione delle copie di backup mediante opportune misure di sicurezza fisica e logica, che devono essere opportunamente cifrate. Il CSP dovrà così condurre dei test periodici, dandone evidenza al Cliente.	Obbligatorio

RCY.39	Business Continuity e Disaster Recovery (BC/DR)	Il CSP dovrà garantire la continuità del servizio in caso di interruzioni o malfunzionamenti, in conformità con gli SLA e i parametri RTO/RPO concordati con il Cliente. In caso di servizi critici, il CSP dovrà assicurare la Business Continuity e Disaster Recovery attraverso: - Un piano di disaster recovery, che stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati (CED) e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. - Un piano di continuità operativa (business continuity), che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. - L'implementazione di un modello e di tecnologie di High Availability che permettano, tramite l'adozione di strumenti tecnologici ridondati, di avere un sistema altamente disponibile ai propri utenti.	Obbligatorio
RCY.40	Business Continuity e Disaster Recovery (BC/DR)	Il CSP deve fornire strumenti che possano prevedere apposite procedure di roll back al fine di ripristinare lo stato iniziale di qualsiasi sistema o servizio, qualora dovessero presentarsi problemi imprevisti e irrisolvibili durante la procedura di aggiornamento per effetto di un cambiamento.	Obbligatorio
RCY.41	Threat & Vulnerability Management (TVM)	Il CSP deve fornire strumenti a supporto del processo di Threat Intelligence per raccogliere, analizzare ed elaborare le informazioni relative alle potenziali minacce che potrebbero impattare il servizio e/o l'organizzazione servita	Obbligatorio
RCY.42	Threat & Vulnerability Management (TVM)	Il CSP dovrà effettuare attività periodiche e schedulate di security assessment (a titolo esemplificativo VA, PT, SAST, IAST, DAST) per la verifica del livello di sicurezza di infrastrutture, sistemi e codice sviluppato mediante la ricerca di vulnerabilità o debolezze che, se sfruttate potrebbero comprometterne il livello di sicurezza, individuando le possibili azioni di rimedio. Il CSP si impegna a condividere l'esito degli assessment e del relativo piano di rimedio	Obbligatorio

		concordando le priorità di intervento e i relativi tempi	
RCY.43	Threat & Vulnerability Management (TVM)	Il servizio deve supportare la costante distribuzione di release software, aggiornamenti di sicurezza e, ove necessario, workaround o misure di Virtual patching per mitigare le vulnerabilità identificate, anche quelle rilevate dagli assessment di sicurezza e dai servizi di security advisory. A tal fine, il CSP è responsabile della definizione di un piano di distribuzione per l'aggiornamento dei sistemi, la gestione del rilascio di configurazioni sicure verificate, e l'installazione tempestiva di patch raccomandate da produttori o terzi. Tutte le attività devono essere pianificate e attuate in modo da assicurare il corretto funzionamento dei sistemi, senza comprometterne i livelli di servizio. Il CSP dovrà evidenziare e documentare l'efficacia degli interventi eseguiti mediante la ripetizione delle azioni che avevano consentito di individuare le vulnerabilità, nonché di tenere traccia di ogni aggiornamento o workaround applicato, assicurando la trasparenza e la tracciabilità di tutte le modifiche apportate.	Obbligatorio
RCY.44	Threat & Vulnerability Management (TVM)	Il CSP si impegna a condividere in modo tempestivo le azioni di adeguamento tecnologico per release hardware/software disponibili per tutti i sistemi e servizi ICT che concorrono anche indirettamente nell'erogazione del servizio al Cliente. Il CSP dovrà inoltre provvedere al supporto delle indicazioni di mitigation da seguire.	Obbligatorio

RCY.45	Threat & Vulnerability Management (TVM)	Il CSP deve supportare la costante distribuzione del software e degli aggiornamenti di sicurezza sui sistemi/piattaforme che mitighino le vulnerabilità che insistono sulle tecnologie a supporto dei sistemi che erogano il servizio.	Obbligatorio
RCY.46	Threat & Vulnerability Management (TVM)	Il CSP deve garantire la protezione degli endpoint e delle postazioni, nonché device mobile che accedono alle informazioni del Cliente, attraverso opportuni strumenti (es. MDM)	Obbligatorio
RCY.47	Container Security (CS)	Il CSP dovrà fornire strumenti a supporto della implementazione di pipeline di integrazione e distribuzione continua (CI/CD) sicure, prevedendo la scansione automatica delle immagini container e dei registri per rilevare vulnerabilità, configurazioni non sicure o pacchetti obsoleti, assicurando l'uso esclusivo di immagini verificate e firmate digitalmente.	Obbligatorio
RCY.48	Container Security (CS)	Tutti i ServiceAccount utilizzati da entità tecniche (CI/CD, operatori, tool di automazione, script, ecc.) devono disporre esclusivamente dei permessi strettamente necessari al proprio scopo, assegnati tramite Role/ClusterRole e RoleBinding/ClusterRoleBinding specifici per ambito namespace (o cluster-wide solo se indispensabile) e con token soggetti a rotazione secondo le policy aziendali.	Obbligatorio
RCY.49	Container Security (CS)	Il CSP deve fornire strumenti che supportino la segmentazione logica e fisica della rete cluster, distinguendo tra ingressi pubblici, traffico interno al cluster, accessi amministrativi e canali di egress. L'architettura deve prevedere confini definiti tra questi domini, tramite firewall, VLAN, subnet dedicate o policy SDN.	Obbligatorio

RCY.50	Container Security (CS)	Il CSP deve fornire strumenti che consentano la raccoltae di metriche e log dei container e dei pod in esecuzione nel cluster utilizzando componenti installati e gestiti all'interno del cluster (es. OpenShift Monitoring con Prometheus, Cluster Logging Operator con Fluentd e Loki) o soluzioni esterne integrate garantendo la visualizzazione centralizzata e un sistema di alerting continuo sui workload.	Obbligatorio
RCY.51	Container Security (CS)	Il CSP deve fornire strumenti che assicurino che le immagini container utilizzate nei workload devono provenire solo da registry certificati, privati o con firma verificabile. È obbligatorio configurare policy di pull da registry fidati ed evitare immagini pubbliche non controllate.	Obbligatorio
RCY.52	Container Security (CS)	Il CSP deve fornire strumenti che supportino il controllo continuo di compliance e vulnerabilità del cluster, tramite strumenti di analisi statica, runtime e policy con capacità di audit e enforcement.	Obbligatorio
RCY.53	Container Security (CS)	Il CSP deve garantire che sia possibile che le immagini dei container siano sottoposte a controllo di sicurezza tramite opportuni servizi di vulnerability assessment.	Obbligatorio
RCY.54	Container Security (CS)	Il CSP deve fornire funzionalità Security Context Constraints (SCC) che consentano al cliente di limitare l'esecuzione dei pod a utenti non root. Devono essere attivi i profili restricted o equivalenti, e deve essere evitata qualsiasi configurazione che consenta escalationi fino al livello di Root.	Obbligatorio
RCY.55	Container Security (CS)	Il CSP deve mettere a disposizione strumenti che consentano diimpedire l'esecuzione di container con flag privileged: true. I profili SCC associati ai namespace applicativi devono escludere privileged e utilizzare solo profili ristretti, controllati da policy.	Obbligatorio
RCY.56	Container Security (CS)	Il CSP deve fornire funzionalità di auditing e policy-as-code (es. OPA/Gatekeeper, Kyverno, Red Hat Advanced Cluster Security) che consentano di sottoporre il cluster a controlli continui di compliance. Le policy devono poter bloccare o segnalare configurazioni non conformi (deny/admit).	Obbligatorio

RCY.57	Container Security (CS)	Il CSP deve fornire funzionalità che consentano al Cliente di organizzare i workload in namespace separati per team, applicazione o dominio funzionale. Devono essere definiti ruoli RBAC e risorse quota per ciascun namespace, garantendo l'isolamento logico tra i tenant e la visibilità granulare sui log.	Obbligatorio
RCY.58	Container Security (CS)	Il CSP deve mettere a disposizione meccanismi che permettano al Cliente di definire NetworkPolicy per ciascun namespace applicativo, al fine di segmentare il traffico in ingresso, uscita e laterale tra i pod. Le funzionalità devono consentire la configurazione di policy specifiche per ogni tipo di workload applicando il principio "default deny".	Obbligatorio
RCY.59	Container Security (CS)	Il CSP deve fornire strumenti che consentano di utilizzare immagini firmate dalla notazione per assicurarsi che le immagini provengano da origini attendibili e non vengano modificate in modo dannoso.	Obbligatorio
RCY.60	Container Security (CS)	Il CSP deve mettere a disposizione configurazioni SCC o Admission Contraller che consentano al Cliente di impedire che i pod non siano configurati per condividere il PID namespace (hostPID: true) o lo spazio dei nomi IPC (hostIPC: true) dell'host, salvo casi eccezionali documentati.	Obbligatorio
RCY.61	Container Security (CS)	Il CSP deve fornire meccanismi che consentano di vietare modifiche arbitrarie ai parametri sysctl. È ammesso solo l'uso di sysctl "sicuri" (es. kernel.shm_rmid_forced, net.ipv4.tcp_syncookies) definiti nei SCC o PodSecurity standards. L'uso di unsafe sysctl deve essere bloccato da policy.	Obbligatorio
RCY.62	Container Security (CS)	Il CSP deve mettere a disposizione strumenti che supportino l'utilizzo di immagini container prive di binari potenzialmente pericolosi per l'ambiente cluster (es. wget, curl, iptables, sysctl, package manager), favorendo la minimizzazione delle immagini (distroless, scratch) e audit periodici sul contenuto delle immagini.	Obbligatorio

RCY.63	Container Security (CS)	Il CSP deve favorire funzionalità che consentano di limitare i container all'uso di profili scc consentiti. L'accesso a profili privilegiati deve essere limitato a casi documentati e monitorati.	Obbligatorio
RCY.64	Container Security (CS)	Il CSP deve mettere a disposizione la possibilità di configurare al Cliente la limitazione del pod all'uso di ProcMountTypes consentiti (Unmasked, Default).	Obbligatorio
RCY.65	Container Security (CS)	Il CSP deve fornire funzionalità SCC che consentano al Cliente di impedire che un pod possa girare con allowPrivilegeEscalation abilitato.	Obbligatorio
RCY.66	Container Security (CS)	Il CSP deve mettere a disposizione la possibilità di configurare il File system ROOT in modalità read only (readOnlyRootFilesystem) per evitare che binari malevoli possano girare sul PATH del cluster.	Obbligatorio
RCY.67	Container Security (CS)	Il CSP deve fornire strumenti SCC che consentano di minimizzare l'ammissione di container con NET_RAW capabilities o capability addizionali.	Obbligatorio
RCY.68	Container Security (CS)	Il CSP deve mettere a disposizione meccanismi che consentano di controllare l'assegnazione di SCC a utenti e service account affinché solo gli account che richiedono privilegi specifici possano avere accesso a profili permissivi; tutti gli altri devono essere vincolati a SCC restricted.	Obbligatorio
RCY.69	Container Security (CS)	Il CSP deve fornire funzionalità che consentano al Cliente di garantire la presenza di NetworkPolicy attive per ogni namespace non infrastrutturale del cluster profilate in base al tipo di traffico atteso.	Obbligatorio
RCY.70	Container Security (CS)	Il CSP deve mettere a disposizione funzionalità che supportino l'utilizzo di secrets montati come file all'interno dei pod (VolumeMount), anziché come variabili d'ambiente.	Obbligatorio
RCY.71	Container Security (CS)	Il CSP deve fornire strumenti che consentano di filtrare l'ammissione di immagini ammettendo soltanto quelle provenienti da registry sicuri e conosciuti.	Obbligatorio
RCY.72	Container Security (CS)	Il CSP deve mettere a disposizione funzionalità che permettano di limitare o proibire l'uso del default namespace.	Obbligatorio

RCY.73	Container Security (CS)	Il CSP deve mettere a disposizione soluzioni di sicurezza per il monitoraggio continuo delle risorse cluster e workload, in grado di rilevare comportamenti anomali, configurazioni pericolose e vulnerabilità (come sistemi di Cloud Native Application Protection Platform (CNAPP), Cloud Security Posture Management (CSPM) e Cloud Workload Protection Platform (CWPP)).	Obbligatorio
RCY.74	Container Security (CS)	Il CSP deve mettere a disposizione meccanismi automatici di drift detection che consentano al Cliente di rilevare gli sconstamenti tra i template Infrastructure-as-Code (es. Helm, Terraform, Ansible) e lo stato effettivo delle risorse distribuite. Gli scostamenti devono generare alert e richiedere approvazione per riconciliazione.	Obbligatorio
RCY.75	Infrastruttura, Reti e Cloud Security (NET/INF)	Disponibilità di ambienti multi-tenant e deploy multi-region al fine di poter indirizzare segregazioni logiche e fisiche, altresì SLA relativi a Business Continuity e Disaster Recovery. Nel caso in cui siano trattati dati sensibili o critici, siano coinvolte infrastrutture o servizi strategici per la continuità operativa del Gruppo, o sussistano obblighi di conformità, sicurezza o audit che richiedano isolamento logico o fisico dei dati e delle risorse, si richiede la fornitura in modalità tenant dedicato (single-tenant)	Obbligatorio
RCY.76	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP dovrà garantire, tramite la disponibilità di un CMDB (Configuration Management Database) aggiornato, la tracciabilità dei dispositivi hardware e software utilizzati per l'erogazione del servizio. Tali informazioni dovranno essere rese disponibili al Cliente su richiesta, ai fini di audit, sicurezza o gestione operativa.	Obbligatorio
RCY.77	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP dovrà fornire strumenti che consentano di implementare misure adeguate a protezione dei sistemi, dei servizi, delle applicazioni anche se solo indirettamente coinvolti o impiegati per l'erogazione dei servizi al Cliente (es. sistemi di virtualizzazione, sistemi di trouble ticketing etc…), ivi inclusi per i modelli cloud i contesti	Obbligatorio

		di pertinenza del CSP e i sistemi, software, architetture e servizi condivisi.	
RCY.78	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP dovrà fornire strumenti per poter garantire che le connessioni da e verso il sistema, supportino i seguenti standard: VPN IPSec, TLS 1.2 o superiore, mTLS, API autenticate; autenticazione forte (mutual authentication con certificati) e utilizzo di API gateway. L'interconnessione deve seguire il principio minima di esposizione, garantendo conformità agli standard di sicurezza.	Obbligatorio
RCY.79	Infrastruttura, Reti e Cloud Security (NET/INF)	La gestione e l'accesso tramite le API del CSP devono rispettare gli standard di sicurezza (es. OWASP Software Assurance Maturity Model, ISO 27034). Per tutte le API esposte dal servizio cloud deve essere dichiarata la conformità al Modello di interoperabilità, definito da AgID con le linee guida adottate ai sensi della normativa vigente. Qualora le API esposte siano conformi, devono essere condivise le specifiche dell'API in formato machine readable compatibile con le indicazioni del modello d'interoperabilità (e.g. OpenAPI3 per le API REST, WSDL per le API SOAP).	Obbligatorio
RCY.80	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP dovrà fornire strumenti che consentano di implementate misure per garantire l'integrità, la sicurezza e la disponibilità di ambienti virtuali in linea con le conformità normative.	Obbligatorio

RCY.81	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP dovrà fornire strumenti per implementare e mantenere un sistema centralizzato per la gestione delle configurazioni, assicurandosi che: - Tutte le configurazioni dei dispositivi e del software siano documentate e approvate. - Siano effettuati controlli periodici per garantire che le configurazioni siano aggiornate e allineate agli standard di sicurezza più recenti. Inoltre, devono essere predisposte procedure per il monitoraggio delle modifiche alle configurazioni, compreso un sistema di versioning e una politica di approvazione delle modifiche critiche.	Migliorativo
RCY.82	Infrastruttura, Reti e Cloud Security (NET/INF)	Il sistema deve supportare il protocollo NTP assicurando la sincronizzazione oraria.	Obbligatorio
RCY.83	Infrastruttura, Reti e Cloud Security (NET/INF)	Il servizio deve garantire la gestione di sistemi di rilevamento e contrasto di attacchi Denial of Service (DoS) e Distributed denial of Service (DDoS). Il CSP deve garantire la gestione del servizio su internet, contestualizzando le configurazioni rispetto alle tecnologie e asset, ottimizzando il servizio per ottenere il minor numero di falsi positivi e garantendo il massimo delle prestazioni all'assurance dei servizi.	Obbligatorio
RCY.84	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP di servizi cloud deve adottare un sistema di Host Intrusion Detection System (HIDS) per rilevare e identificare eventi o sequenze di eventi che potrebbero compromettere un sistema, un dispositivo o la rete. Inoltre, deve implementare un Host Intrusion Prevention System (HIPS) per analizzare il traffico, rilevare la presenza di accessi non autorizzati o codice malevolo in esecuzione sui sistemi, e bloccare eventuali tentativi di attacco o traffico anomalo.	Obbligatorio

RCY.85	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP dovrà mettere a disposizione servizi Antimalware che deve garantire la protezione dei sistemi server gestiti da qualsiasi tipologia di software malevolo eseguibile e non (es. virus, trojan, Worm, Key loggers, rootkit, ransomware etc.). Le "firme" di protezione devono essere aggiornate in tempo reale. Tutti gli eventi malware-related devono essere inviati ad una piattaforma centralizzata di collezionamento.	Obbligatorio
RCY.86	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP dovrà fornire strumenti volti a supportare: - l'installazione di firewall perimetrali per limitare l'esposizione a livello di rete, di sistemi e servizi ai soli host/IP strettamente necessari, tracciando gli accessi o i tentativi di accesso; - l'implementazione di soluzioni di Network Detection & Response (NDR); - l'implementazione di soluzioni di tipo Network-based Intrusion Detection Systems (IDS) e Network-based Intrusion Prevention Systems (IPS) per la rilevazione di anomalie di sicurezza ed il blocco di possibili tentativi di attacco; - l'implementazione di meccanismi che permettono di effettuare in qualsiasi momento l'associazione dei seguenti campi per l'identificazione dei dispositivi collegati alla rete: Indirizzo IP, Host / Mac Address e Username o ID univoco dell'utente.	Obbligatorio
RCY.87	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP dovrà fornire strumenti volti a supporto della protezione dei server DNS per garantire la disponibilità e integrità della risoluzione dei nomi.	Obbligatorio
RCY.88	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP potrà supportare l'adozione di soluzioni adeguate a protezione del perimetro (garantendone il costante aggiornamento sia automatico che, se necessario, manuale) attraverso: Controllo accessi alla rete dei dispositivi, ristretto utilizzando tecnologie di Network Access Control (NAC), in grado di verificare la configurazione del dispositivo e gestire opportunamente l'accesso	Migliorativo

RCY.89	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP dovrà fornire strumenti a supporto della corretta configurazione dei dispositivi di rete (inclusi router, switch e firewall): - evidenziare condizioni di sovraccarico o eccezioni, quando si verificano; - registrare gli eventi (logging) e salvarli su un sistema separato; - integrarsi con meccanismi di controllo degli accessi (ad esempio per fornire autenticazione forte); - assicurare che le password per accedere a tali dispositivi non vengano inviate in chiaro; - disabilitare il "source routing", tecnica di specificare all'interno dell'header IP il tragitto (route) che il pacchetto deve seguire per mantenere il controllo all'interno del dispositivo di inoltro dei pacchetti.	Obbligatorio
RCY.90	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP dovrà mettere a disposizione strumenti che consentano l'erogazione del servizio di NAT Management per la gestione delle regole di traduzione degli indirizzi IP configurati all'interno dell'infrastruttura di rete ed il piano di indirizzamento complessivo/pubblico.	Obbligatorio
RCY.91	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP deve attuare i controlli opportuni per quanto concerne la sicurezza degli ambienti computazionali garantendo la protezione delle reti e dei sistemi da eventuali attacchi, da accessi e modifiche non autorizzate assicurando il monitoraggio dei componenti informatici e il funzionamento continuo ed ottimale dell'infrastruttura.	Obbligatorio
RCY.92	Infrastruttura, Reti e Cloud Security (NET/INF)	Il CSP deve adottare procedure/strumenti di change management per tenere traccia delle modifiche eseguite sulle configurazioni del sistema che, in ogni caso, non dovranno ridurre i livelli di sicurezza. In aggiunta, il CSP deve prevedere la definizione di un processo formale che documenti la fase di autorizzazione, l'analisi di impatto in termini di sicurezza e implementazione delle modifiche e dell'installazione delle patch all'interno di processi, sistemi o strutture aziendali.	Obbligatorio

RCY.93	Monitoraggio, Logging e Incident Management (MON/IR)	Il CSP deve garantire fornire strumenti che consentano un'adeguata gestione delle utenze e degli accessi ai servizi e ai sistemi, assicurando il tracciamento di tutti gli accessi effettuati dagli utenti, la registrazione e conservazione dei log relativi agli accessi e alle attività svolte, con particolare attenzione agli utenti con credenziali privilegiate e/o Amministratori di Sistema, per i quali devono essere previsti specifici meccanismi di controllo, monitoraggio e rendicontazione, secondo le normative vigenti e le best practice di settore.	Obbligatorio
RCY.94	Monitoraggio, Logging e Incident Management (MON/IR)	Il CSP dovrà fornire strumenti che consentano di garantire che i sistemi, le applicazioni, i servizi e le infrastrutture utilizzati per l'erogazione del servizio siano in grado di generare eventi e log rilevanti ai fini della sicurezza, e audit log. Tali log dovranno essere raccolti, conservati (in tempi concordati con il Clienti) e correlati mediante apposite piattaforme (es. SIEM), e su richiesta piattaforme proprietarie del cliente, al fine di consentire attività di monitoraggio, analisi e rilevazione di eventuali anomalie di sicurezza.	Obbligatorio
RCY.95	Monitoraggio, Logging e Incident Management (MON/IR)	Il CSP dovrà fornire strumenti volti a garantire un servizio di Real Time Monitoring h24x7 finalizzato alla rilevazione e analisi di attacchi informatici e minacce, e alla gestione di anomalie e incidenti di sicurezza nel perimetro di erogazione dei servizi al Cliente che dovrà comprendere: - personale specializzato in un centro specializzato (SOC) in grado di correlare gli eventi di sicurezza intercettati, analizzare gli alert generati dalla piattaforma di monitoraggio e correlazione, attivare le opportune procedure e processi per la gestione degli incidenti - La gestione degli incidenti di sicurezza identificati attraverso un team operativo specializzato in grado di intervenire tempestivamente per il contenimento, il contrasto e la risoluzione dell'incidente e/o attacco informatico. - La produzione degli incident report che relazionano le cause dell'incidente rilevato, gli eventuali danni provocati e le azioni di	Obbligatorio

		contrasto e ripristino intraprese. - La registrazione e memorizzazione degli incidenti avvenuti/individuati	
RCY.96	Monitoraggio, Logging e Incident Management (MON/IR)	Il CSP dovrà comunicare nei tempi e nei modi, previsti dalle normative vigenti (es. GDPR, Direttiva NIS, ecc.) e concordati con il Cliente, ogni incidente occorso sui sistemi che gestiscono dati e informazioni del Cliente. Il CSP dovrà provvedere, inoltre, alla stima dei possibili impatti sulla sicurezza delle informazioni, sugli asset e sui servizi erogati al Cliente, e prevedere una RCA per ciascun caso con esito positivo o negativo, altresì il report post-incident. Il CSP deve segnalare tempestivamente al Cliente eventuali accessi non autorizzati a dati del Gruppo FS che possano causare perdite, divulgazioni o alterazioni dei dati, nel rispetto della normativa vigente. Deve altresì collaborare con il Cliente ad un piano di comunicazione e coordinamento per i rapporti con le Autorità competenti (es. Garante, ACN)	Obbligatorio
RCY.97	Monitoraggio, Logging e Incident Management (MON/IR)	Dovranno essere altresì tempestivamente comunicate, nei tempi e nei modi concordati con il Clienti, le eventuali rilevazioni di anomalie di sicurezza sui sistemi del CSP, e/o di supply direttamente coinvolti nell'erogazione dei servizi al Gruppo FS.	Obbligatorio
RCY.98	Monitoraggio, Logging e Incident Management (MON/IR)	Il CSP dovrà proteggere adeguatamente i Log raccolti mediante sistemi e tecniche che ne garantiscono l'inalterabilità, la non cancellabilità e la conservazione per tutto il tempo ritenuto congruo e comunque non inferiore a quanto indicato dalle normative vigenti.	Obbligatorio
RCY.99	Monitoraggio, Logging e Incident Management (MON/IR)	Il CSP dovrà adottare soluzioni adeguate a protezione del perimetro (garantendone il costante aggiornamento sia automatico che, se necessario, manuale) attraverso: File Integrity Tool per la verifica dell'integrità dei file per assicurare che i file critici di sistema (compresi eseguibili, librerie e file di configurazione) non siano stati alterati.	Obbligatorio

RCY.100	Sicurezza Fisica (SF)	Il CSP deve garantire la protezione degli asset informatici da attacchi esterni, accessi e modifiche non autorizzate, assicurando il funzionamento continuo ed ottimale dell'infrastruttura di sicurezza, nonché monitorare il comportamento dei sistemi ed apportare le modifiche necessarie alle configurazioni delle politiche di sicurezza perimetrale. L'accesso fisico agli edifici che ospitano l'infrastruttura IT dell'organizzazione deve essere limitato agli individui autorizzati mediante le seguenti misure di sicurezza e deve rispettare il principio del minimo privilegio, ovvero ciascun lavoratore deve poter accedere solo a quelle funzioni/servizi/dati necessari allo svolgimento delle proprie mansioni lavorative: - controllo accessi all'ingresso degli edifici (reception e/o servizio di guardiania); - manutenzione pianificata dei sistemi critici; - il personale deve essere dotato di badge personale o di altro mezzo di identificazione (e.g. PIN).	Obbligatorio
RCY.101	Sicurezza Fisica (SF)	Apparecchiature, informazioni o software che gestiscono dati o informazioni del Cliente non devono essere portate al di fuori dell'ambiente del CSP senza preventiva autorizzazione. Tutte le apparecchiature da riutilizzare o da smaltire, che contengono supporti di memorizzazione, devono essere controllate per assicurare che le informazioni del Cliente siano state rimosse o sovrascritte in modo sicuro, prima del loro smaltimento/riutilizzo.	Obbligatorio
RCY.102	Sicurezza Fisica (SF)	Il CSP deve aver adottato misure di sicurezza per prevenire o far fronte ad un possibile incendio/allagamento del Data Center primario che ospita le macchine dell'organizzazione. Il CSP deve svolgere delle attività di monitoraggio della temperatura interna del Data Center primario per tutelare le macchine in esso presenti. I cavi di rete ed i punti di accesso alla rete nel data center primario devono essere protetti mediante controlli fisici. Gli edifici che ospitano l'infrastruttura IT del data center primario dell'organizzazione	Obbligatorio

		devono essere fisicamente protetti contro incidenti o attacchi di sicurezza. Le infrastrutture IT del data center primario devono essere protette contro sbalzi o interruzioni di corrente.	

II. 1.3 REQUISITI VALUTATIVI TECNICI A CARATTERE QUALITATIVO

1. Si richiede di fornire l'elenco completo delle principali certificazioni di sicurezza in possesso dell'Operatore Economico e di indicare il livello di conformità attuale o la roadmap pianificata rispetto alle normative NIS2 e DORA, descrivendo le modalità di gestione del patching dell'infrastruttura, indicando come viene garantito che i sistemi siano costantemente aggiornati, le tempistiche di applicazione degli aggiornamenti, le interazioni previste con il cliente, la gestione di eventuali eccezioni e le politiche di extended support adottate. Il patching deve essere integrato in pipeline CI/CD e pratiche DevOps, con automazione e controlli di sicurezza nel ciclo di vita. Devono essere indicati anche l'impatto economico delle politiche di patching e gli strumenti di monitoraggio dei costi associati.

2. Si richiede di illustrare in dettaglio il modello di responsabilità condivisa applicato e di specificare gli strumenti nativi messi a disposizione del cliente per la gestione della sicurezza, chiarendo come il patching rientra nel modello di responsabilità, indicando chi è responsabile dell'applicazione delle patch, le procedure operative e le modalità di comunicazione verso il cliente. Il patching deve essere gestito tramite processi automatizzati e strumenti di osservabilità integrati nelle pipeline CI/CD, garantendo trasparenza sui costi delle attività di sicurezza e sulle responsabilità economiche tra provider e cliente.

3. Si richiede di descrivere le modalità di interconnessione tra le Availability Zone (AZ), evidenziando le best practices adottate per garantire resilienza, latenza ridotta e continuità operativa. Inoltre, ove disponibili, fornire benchmark di riferimento che attestino le performance infrastrutturali tra le AZ, con particolare attenzione a throughput, latenza e disponibilità.

4. Si richiede di descrivere la modalità di gestione nel caso in cui un sistema operativo, database o componente non possa essere aggiornato o migrato alle versioni supportate dal Cloud a causa di vincoli applicativi.
   Nello specifico indicare:
   - Quali politiche adottate (es. isolamento in 'bolla', estensione del supporto, virtualizzazione dedicata).
   - Impatto sui costi (es. maggiorazione per ambienti legacy).
   - Garanzia di continuità del servizio e livello di SLA applicabile.

- Eventuali limiti temporali o obblighi di remediation

5. Si richiede di dettagliare le condizioni di applicabilità degli SLA (Service Level Agreement) garantiti, specificando le metriche di disponibilità previste e le politiche di credito in caso di disservizi o mancato rispetto degli SLA contrattuali, includendo le tempistiche di patching come parte degli SLA, indicando eventuali finestre di manutenzione, tempi massimi per l'applicazione delle patch critiche e le politiche di gestione delle eccezioni. Gli SLA devono includere metriche di deployment frequency, lead time for changes e MTTR, oltre alle politiche di credito e all'impatto economico dei downtime, con strumenti di previsione e controllo dei costi.

6. Si richiede di illustrare i meccanismi di auto-scaling disponibili per i workload di computing, inclusi servizi serverless, evidenziando la capacità della piattaforma di adattarsi dinamicamente ai carichi di lavoro. Deve essere indicato l'uso di Infrastructure as Code (IaC) e pipeline automatizzate per il provisioning e lo scaling, insieme alla capacità di ottimizzare i costi in scenari di scaling dinamico, con alert su sprechi o overprovisioning.

7. Si richiede di fornire, ove possibile, benchmark e dati prestazionali, al fine di supportare la valutazione tecnica delle soluzioni.

8. Si richiede di descrivere in dettaglio le politiche di data residency applicate, specificando le modalità con cui viene garantito che i dati non vengano trasferiti, replicati o processati al di fuori del territorio dell'Unione Europea, salvo esplicita richiesta e sotto il controllo del cliente. Descrivere come il servizio garantisce l'immunità da leggi extraterritoriali e il controllo sugli accessi amministrativi (Operational Sovereignty).

9. Si richiede di illustrare i meccanismi di controllo messi a disposizione del cliente per monitorare e gestire la localizzazione dei dati, inclusi strumenti di configurazione, auditing e alerting.

10. Si richiede di condividere quali siano le garanzie sugli SLA per servizi IaaS e PaaS (calcolo, storage, database). Si richiede di condividere se il CSP garantisca l'aderenza agli obiettivi (Minimum Service Level Objective - SLO) corrispondenti ai seguenti indicatori di servizio (Service Level Indicator - SLI), garantendone il rispetto nei rapporti contrattuali nella forma di accordi relativi ai livelli di servizio (SLA). A titolo di esempio si condividono delle informazioni di dettaglio che si intendono ricevere:
    - Disponibilità pari al 99,9%, intesa come percentuale di tempo mensile in cui il servizio cloud è accessibile e usabile, escludendo eventi catastrofici.
    - Supporto tecnico per emergenze operativo 24/7/365.
    - Tempo massimo di risposta agli incidenti critici pari a 1 ora.
    - Minor release: preavviso minimo di 3 giorni con release note.

- Major release: preavviso minimo di 1 mese con release note.

11. Si richiede di descrivere le capacità relative ai processi che consentono di raccogliere, trasferire e preparare grandi volumi di dati provenienti da sorgenti eterogenee, rendendoli disponibili in un Data Lake o in un Data Warehouse, dettagliando come la soluzione si dimostri efficace nel garantire scalabilità, affidabilità e flessibilità, supportando in modalità batch diversi formati di dati e connessioni a molteplici sistemi, e indicando quali soluzioni vengono prospettate per migrare applicativi legacy mantenuti attivi solo per garantire l'accesso ai dati per obblighi normativi (es. contenziosi o conservazione decennale).

12. Si richiede di descrivere le capacità in ambito Stream Data Integration e l'insieme di tecniche e processi che consentono di raccogliere, integrare e trasformare dati in movimento (streaming) provenienti da sorgenti eterogenee, così da renderli coerenti, arricchiti e pronti per l'analisi in tempo reale. Descrivere quali tipologie di fonti di dati in streaming vengono supportate verso i sistemi di destinazione (come Data Lake, database o dashboard), garantendo una gestione continua e affidabile dei flussi informativi.
    Confermare e descrivere come vengano soddisfatte le principali caratteristiche dello Stream Data Integration, ovvero:
    - Integrazione continua: combinare dati provenienti da sorgenti diverse (sensori, log, applicazioni, API, code di messaggi) in tempo reale.
    - Trasformazione dinamica: consentire pulizia, arricchimento e aggregazione dei dati durante il flusso.
    - Scalabilità: supportare grandi volumi di eventi grazie a infrastrutture distribuite.
    - Bassa latenza: rendere i dati disponibili per analisi o automazioni in modo quasi istantaneo.
    - Affidabilità e resilienza: garantire un'elaborazione esatta e il recupero automatico in caso di errori.
    - Compatibilità multipiattaforma: integrare sistemi di messaggistica e cloud (ad es. Kafka, Kinesis, Event Hubs, Pub/Sub).

13. Si richiede di descrivere le modalità di orchestrazione e i meccanismi di scalabilità automatica, specificando come vengono gestiti i picchi di carico e l'esecuzione concorrente dei job. Dettagliare i livelli di throughput, i tempi medi di elaborazione e i meccanismi di retry, checkpoint e recovery in caso di errore, al fine di garantire l'affidabilità e la consistenza dei dati. La soluzione deve consentire la configurazione dinamica della frequenza di esecuzione, l'integrazione di pipeline batch e micro-batch nella stessa architettura, offrendo strumenti di monitoraggio, logging e ottimizzazione delle performance. Deve essere evidenziata l'integrazione con orchestratori CI/CD e automazione dei workflow, indicando il modello di costo basato su consumo e la disponibilità di strumenti di chargeback/showback per accountability.

14. Si richiede di descrivere la capacità di Data Lakehouse, evidenziando:
    - Gestione e analisi dei dati: archiviazione unificata di dati strutturati, semi-strutturati e non strutturati, con query SQL performanti, ottimizzazione automatica di partizioni e indici, e gestione dinamica delle risorse di calcolo (autoscaling) in funzione di carico, priorità e tipo di query, con ottimizzazione dei costi
    - Machine Learning e asset complementari: integrazione nativa con framework ML (PyTorch, TensorFlow) per training e deployment, e condivisione di asset aggiuntivi come notebook, modelli ML e dati non strutturati all'interno di un catalogo unificato e governato
    - Unificazione, condivisione e governance: piattaforma integrata per archiviazione ed elaborazione, con data sharing zero-copy personalizzabile (row/column-level), catalogo unificato, tracciabilità delle origini e lineage dei dati

15. Si richiede di specificare le capacità in ambito Query Processing, con capacità di prestazioni, scalabilità ed efficienza nell'elaborazione di carichi analitici complessi e concorrenti, integrando ottimizzazione automatica, elasticità del compute e capacità intelligenti di tuning

16. Si richiede di descrivere la capability di Stream Processing, evidenziando come la piattaforma soddisfi i requisiti di High-frequency ingestion e Real-time querying.

    Per High-frequency ingestion, indicare:
    - Le tecnologie e gli approcci utilizzati per garantire scalabilità, buffering e gestione dei picchi di dati.
    - Il supporto a protocolli e formati eterogenei per l'ingestione dei dati.
    - Le strategie adottate per ottimizzare la latenza e garantire l'elaborazione quasi in tempo reale.

    Per Real-time querying, illustrare:
    - Come la piattaforma supporta query e riepilogo degli eventi rispetto a modelli o regole definite.
    - I motori di query utilizzati per assicurare tempi di risposta rapidi.
    - La possibilità di configurare regole personalizzate per identificare pattern o anomalie nei dati.
    - Le modalità di visualizzazione dei risultati, ad esempio tramite dashboard interattive.
    - Eventuali notifiche o azioni automatiche generate in base ai risultati delle query in tempo reale

17. Si richiede di descrivere le capabilities del Data Lake, illustrando come la piattaforma gestisca volumi di dati eterogenei in crescita, adattandosi dinamicamente ai carichi di lavoro per garantire prestazioni costanti.
    Evidenziare il supporto nativo a formati strutturati e semi-strutturati con interrogazione diretta dei metadati, la gestione multi-livello dello storage (Hot, Cool, Cold) con versioning, sicurezza, governance e logging dettagliato.
    Indicare, infine, come il sistema supporti integrazione e notifiche verso sistemi esterni tramite API o servizi di messaggistica, consentendo l'analisi dei dati in tempo reale.

18. Descrivere come la capacità di Data Transformation consente l'implementazione di modelli di Data Processing supportando:
    - Trasformazioni strutturali e semantiche
    - Applicazione di regole di business
    - Controlli di qualità del dato
    - Tracciabilità dei processi.

    Indicare, inoltre, come la soluzione integra funzionalità di monitoraggio, automazione e interoperabilità con orchestratori esterni, garantendo efficienza, scalabilità e governance delle pipeline.

19. Si richiede di descrivere come la capacità soddisfa i requisiti di un sistema di Data Warehouse, evidenziando:
    - le capacità di archiviazione basate su, Tecnologie di database relazionali, Tecnologie di database scalabili, Database key-value e NoSQL
    - le capacità di gestire scaling elastico automatico per workload di data warehouse con picchi di query simultanee
    - Modellazione e gestione dei dati: supporto a schemi dimensionali (Star/Snowflake), dimensioni a cambiamento lento (SCD) e Data Marts tematici
    - Analisi, BI e innovazione: integrazione con strumenti di BI (PowerBI, Tableau, QlikSense), supporto a Data Lake, architetture cloud-native e Machine Learning
    - Governance, sicurezza e operatività: tracciabilità dei dati e lineage, gestione ruoli, sicurezza e conformità normativa, monitoraggio, backup, disaster recovery, alta disponibilità e scalabilità
    - Soluzioni per la migrazione di applicativi legacy mantenuti attivi esclusivamente per garantire l'accesso ai dati in caso di obblighi normativi (es. contenziosi o conservazione decennale), indicando approcci, strumenti e modalità per assicurare disponibilità e conformità dei dati nel tempo

20. Si richiede di descrivere come la piattaforma supporta l'AI-as-a-Service, fornendo:
    - Ambienti collaborativi multiutente con workspace condivisi e sandbox sicure
    - Accesso a modelli pre-addestrati

- Creazione di pipeline automatizzate per la data preparation, feature engineering e training dei modelli integrabili con strumenti di MLOps e CI/CD

21. Si richiede di descrivere come la piattaforma supporta la capacità di Generative AI, specificando in che modo consente il fine-tuning dei modelli generativi tramite strumenti guidati, low-code o visuali, e la disponibilità di Foundation Model gestiti con context window estesa per garantire coerenza e rilevanza delle risposte.
    Indicare come la piattaforma gestisce il Model Registry per versioning, governance e tracciabilità dei modelli e degli agenti AI, e come assicura prestazioni costanti e prevedibili mediante unità di throughput dedicate o risorse equivalenti. Descrivere, inoltre:
    - Il supporto della piattaforma a modelli multimodali
    - La presenza di controlli di sicurezza e conformità
    - L'offerta di servizi di embedding
    - L'integrazione con database vettoriali per ricerca semantica, filtraggio contestuale e retrieval ottimizzato
    - Le funzionalità di monitoraggio e logging, per tracciare metriche operative, volumi di interazione e performance dei modelli e agenti AI

22. Si richiede di descrivere come la piattaforma supporta e ottimizza il ciclo di vita del Model Training, includendo data preparation, training, hyperparameter tuning, versioning e monitoraggio delle performance.
    Indicare come assicura tracciabilità e riproducibilità degli esperimenti tramite Experiment Tracking e Model Lineage, integra feature store e model registry per la gestione centralizzata dei modelli.
    Evidenziare, infine, come permette di gestire l'auto-scaling dinamico e fornisce workspace collaborativi e ambienti runtime personalizzabili per la data science.

23. Si richiede di descrivere in che modo la piattaforma gestisce il deployment, il serving e la supervisione operativa dei modelli AI in produzione, illustrando le modalità di distribuzione su endpoint real-time e batch, con supporto ad ambienti containerizzati e accesso tramite API standard o servizi gestiti.
    Specificare come la piattaforma garantisce prestazioni elevate e prevedibili e come integra funzionalità di monitoraggio e osservabilità per rilevare tempestivamente problemi, anomalie o errori, con possibilità di scaling automatico.
    Evidenziare, infine, le misure adottate per assicurare scalabilità, sicurezza, continuità del servizio e una gestione operativa efficiente dei modelli AI in produzione.

24. Si richiede di descrivere come la piattaforma abilita il deployment di modelli e soluzioni di Machine Learning per l'inferenza in tempo reale, evidenziando:
    - La capacità di esporre endpoint accessibili da sistemi esterni, garantendo bassa latenza e alta disponibilità per applicazioni critiche

- Le opzioni di configurazione della capacità computazionale degli endpoint, che consentono di mantenere prestazioni costanti anche in presenza di carichi elevati o richieste frequenti

25. Si richiede di descrivere la capacità, gli standard tecnologici e i protocolli adottati (ad esempio REST, SOAP, GraphQL o altri), unitamente ai formati di scambio dati utilizzati (JSON, XML, CSV, ecc.). Confermare la disponibilità di meccanismi di versionamento o gestione delle evoluzioni (es. v1, v2, ecc.);
    Elencare le modalità di autenticazione e sicurezza disponibili (API Key, OAuth2, JWT, certificati digitali, VPN o altre), con specifica delle eventuali policy di autorizzazione e dei profili di accesso.
    Definire le caratteristiche prestazionali rilevanti, tra cui frequenza di utilizzo, volumi medi di chiamata, tempi di risposta e disponibilità di strumenti di monitoraggio e logging.

26. Si richiede di condividere in che modo la piattaforma supporta la containerizzazione e la gestione dell'infrastruttura per l'esposizione dei Model-as-a-Service, evidenziando la flessibilità architetturale con infrastrutture gestite o containerizzabili, le possibilità di personalizzazione delle risorse e dei protocolli, le funzionalità di autoscaling e bilanciamento del carico per garantire efficienza e resilienza, e le soluzioni adottate per assicurare alta disponibilità e continuità operativa in ambienti di produzione critici. Deve essere descritta la gestione dei container tramite pipeline CI/CD e strumenti di osservabilità, fornendo trasparenza sui costi di container e cluster, con meccanismi di chargeback/showback.

27. Si richiede di definire come la capacità supporta tecniche avanzate di indicizzazione (ad esempio columnstore, bitmap, partizionamento e materialized views) e dispone di un query optimizer in grado di generare piani di esecuzione adattivi basati su statistiche aggiornate. In termini di sicurezza e controllo degli accessi descrivere come la capacità consente la gestione granulare di ruoli e privilegi, con supporto a row-level e column-level security, masking dinamico dei dati e audit trail completo delle query, garantendo conformità a normative vigenti.

28. Si richiede di descrivere le capacità della piattaforma in ambito visualization & dashboarding, evidenziando:
    - Creazione di report pixel-perfect esportabili in PDF ed Excel, con design accessibile e ottimizzato per dispositivi mobili.
    - Possibilità di integrare dashboard e report in siti web o applicazioni.
    - Funzionalità di interattività avanzata, come drill-down, slicing e pivoting.
    - Prestazioni elevate garantite tramite refresh near-real-time, caching e architetture distribuite.

- Gestione dell'integrazione e preparazione dei dati provenienti da fonti eterogenee, tramite connettori nativi e strumenti self-service.
- Supporto a suggerimenti automatici per le visualizzazioni più adatte e possibilità di analizzare reti e grafi complessi.

29. Si richiede di descrivere in modo esaustivo come la piattaforma supporta la Geospatial Analysis, evidenziando:
    - Visualizzazione su mappe interattive: capacità di creare mappe dinamiche con sovrapposizione di più layer informativi, tematizzazione avanzata, operazioni di zoom e possibilità di esportare dati e immagini
    - Spatial querying e analisi avanzata: supporto nativo per query spaziali (es. buffer, intersect, within) e visualizzazioni avanzate come heatmaps, clusterizzazione e interpolazione, per evidenziare pattern, densità e relazioni geografiche complesse
    - Drill-down geografico interattivo: navigazione tra diversi livelli di dettaglio geografico per un'analisi granulare e dinamica
    - Integrazione con modelli ML: possibilità di collegare modelli di machine learning e regressione spaziale per supportare decisioni basate su dati geospazial

30. Si richiede di descrivere la capacità di Self Service Business Intelligence, con particolare attenzione ai seguenti aspetti:
    - Facilità d'uso e interfaccia intuitiva, che consentono un'esperienza utente semplice e accessibile, con funzionalità di drag-and-drop per la creazione di report e dashboard personalizzabili e interattive
    - Collaborazione e condivisione, permettendo la condivisione di report e dashboard tra utenti, con modalità di sola visualizzazione o modifica
    - Conversational BI e Natural Language Query (NLQ), tramite l'integrazione nativa di funzionalità di Business Intelligence conversazionale, supportando più lingue e abilitando un'interazione fluida e intuitiva con la base dati
    - Integrazione con intelligenza artificiale generativa, per abilitare casi d'uso avanzati come generazione automatica di insight, suggerimenti per visualizzazioni e risposte a domande complesse

31. Si richiede di descrivere come viene supportata la capacità di Data Orchestration e l'automazione di workflow complessi, evidenziando:
    - Schedulazione e monitoraggio avanzato: gestione di pipeline batch, microbatch e streaming, con dashboard intuitive e alert automatici;
    - Orchestrazione multidominio e AI-driven: coordinamento di task eterogenei in un unico workflow, con metadati e intelligenza artificiale per ottimizzare sequenza, priorità e scalabilità dinamica;

- Integrazione e self-service: compatibilità con orchestratori esterni in cloud e on-premise, con strumenti intuitivi che permettono agli utenti non IT di gestire autonomamente workflow complessi

II. 1.4 REQUISITI VALUTATIVI DI SICUREZZA A CARATTERE QUALITATIVO

1. Si richiede che l'architettura di sicurezza adottata sia basata su uno o più standard riconosciuti a livello internazionale, come ad esempio il Cloud Data Security Architecture (CDSA), MULTISAFE, il FedRAMP oppure il framework CAESARS, assicurando così un elevato livello di conformità, interoperabilità e resilienza.

2. Si richiede che il CSP adotti un approccio rigoroso e sistematico per garantire la conformità alle policy di sicurezza, agli standard di settore e ai requisiti normativi. A tal fine, si richiede se siano previste revisioni e valutazioni indipendenti su base annuale, finalizzate all'identificazione e alla correzione di eventuali non conformità rispetto a policy, procedure interne e obblighi di compliance.

3. Si richiede che l'infrastruttura dei data center sia progettata secondo i più elevati standard di affidabilità, resilienza e sicurezza ambientale. Tutti i servizi critici inclusi alimentazione elettrica, raffreddamento (temperatura e umidità), approvvigionamento idrico, connettività di rete e telecomunicazioni siano costantemente monitorati tramite sistemi automatizzati e personale qualificato, manutenuti e testati regolarmente secondo un piano di manutenzione preventiva e verifiche programmate, protetti contro accessi non autorizzati, interferenze fisiche e potenziali danni accidentali o dolosi. L'ambiente operativo sia dotato di controlli ambientali automatizzati, tra cui sistemi HVAC ridondati, UPS (gruppi di continuità), generatori di backup e connessioni internet multicarrier, per garantire la continuità del servizio anche in caso di guasti o interruzioni programmate/non programmate. Inoltre, l'architettura del data center si richiede preveda meccanismi di fail-over automatici, con ridondanza a livello di alimentazione, rete e sistemi critici, assicurando la disponibilità e l'integrità delle operazioni 24/7.

4. Si richiede che il CSP garantisca la mitigazione di rischi ambientali e prevenga accessi non autorizzati, inoltre le apparecchiature critiche siano collocate lontano da aree soggette a elevati rischi naturali o industriali. Tali sistemi si richiede debbano essere supportati da componenti ridondanti ubicati a una distanza adeguata, per garantire la continuità operativa anche in caso di guasti o disastri localizzati.

5. Si richiede che il CSP applichi un processo definito di gestione delle modifiche e controllo qualità, con test strutturati e criteri di rilascio chiari, volti a garantire disponibilità, riservatezza e integrità dei sistemi. Si richiede verifica del codice per rilevare vulnerabilità, anche se sviluppato da terzi, per assicurare la rimozione di elementi di debug prima del

rilascio. Si richiede siano previsti processi per documentare problemi noti e gestire segnalazioni di bug o vulnerabilità in modo tempestivo e tracciato.

6. Si richiede che il CSP definisca e applichi policy e procedure specifiche, supportate da processi aziendali e controlli tecnici, per prevenire e limitare l'installazione di software non autorizzato su tutti i dispositivi end-point e le infrastrutture IT di proprietà o gestite, al fine di garantire la sicurezza e l'integrità degli asset tecnologici, riducendo il rischio di vulnerabilità o compromissioni legate a software non controllato.

7. Si richiede che il CSP adotti policy, procedure e controlli tecnici per inventariare e documentare I flussi di dati all'interno delle applicazioni e infrastrutture distribuite, inclusi quelli condivisi con terze parti, al fine di valutare e gestire eventuali impatti di conformità normativa, contrattuale e rischi associati ai dati.

8. Si richiede che il fornitore di servizi cloud implementi e mantenga adeguate misure di sicurezza fisica per prevenire accessi non autorizzati ai propri data center, infrastrutture e aree operative che ospitano o trattano dati sensibili del cliente. Si richiede che tali misure includano, in funzione del livello di rischio, controlli fisici e/o elettronici (ad esempio barriere, sorveglianza, autenticazione fisica e procedure di accesso controllato) volti a garantire la protezione continua delle risorse informative e dei sistemi.

9. Si richiede che la proposta preveda un inventario aggiornato delle proprie risorse critiche, classificandole in base alla loro importanza per il business, ai requisiti di servizio e alla continuità operativa, e assegni la responsabilità di gestione a ruoli specifici.

10. Si richiede che il fornitore di servizi cloud implementi politiche e procedure documentate per la gestione delle chiavi crittografiche. Si richiede che sia prevista la possibilità che ogni chiave possa essere associata ad un proprietario o ruolo responsabile, in modo da garantire la tracciabilità e il controllo sull'uso, la rotazione, la revoca e la protezione delle chiavi durante l'intero ciclo di vita.

11. Si richiede che siano definite e applicate politiche e procedure per la gestione completa delle chiavi crittografiche, comprendendo l'intero ciclo di vita, i protocolli di sicurezza, gli algoritmi utilizzati e i controlli di accesso. Si richiede che qualsiasi modifica significativa ai meccanismi crittografici sia comunicata alle parti interessate, specialmente in presenza di responsabilità condivise.

12. Si richiede che siano definite politiche, procedure e misure tecniche che garantiscano l'utilizzo di protocolli crittografici adeguati per la protezione dei dati sensibili, sia durante la conservazione sia durante la trasmissione, nel rispetto delle normative e dei requisiti di conformità applicabili.

13. Si richiede che sia previsto l'utilizzo di cifrari sicuri per una crittografia appropriata sulla piattaforma e dei dati (ad esempio AES-256. Si richiede che le chiavi possano essere mantenute dal consumatore del cloud o da un fornitore affidabile di gestione delle chiavi. La gestione e l'utilizzo delle chiavi possano essere compiti separati.

14. Si richiede che siano definite configurazioni di sicurezza di base per tutte le applicazioni, infrastrutture e componenti di rete, garantendo la conformità ai requisiti legali e normativi. Si richiede che qualsiasi deroga a tali configurazioni sia autorizzata secondo processi di gestione del cambiamento, e che la conformità ai requisiti sia verificata periodicamente.

15. Si richiede che siano condotte valutazioni periodiche dei rischi relativi alla gestione dei dati, considerando la localizzazione e il flusso dei dati sensibili, il rispetto dei requisiti di conservazione e smaltimento, e le misure di classificazione e protezione per prevenire accessi o utilizzi non autorizzati, perdite o alterazioni.

16. Si richiede che siano condotte valutazioni formali dei rischi a intervalli pianificati, o in concomitanza con modifiche significative ai sistemi informativi, utilizzando approcci qualitativi e quantitativi per stimare la probabilità e l'impatto dei rischi identificati. Si richiede di esplicitare il trattamento dei rischi intrinseci e residui tenendo conto di tutte le categorie di rischio, incluse audit, vulnerabilità, minacce e requisiti normativi.

17. Si richiede che siano identificati, valutati e prioritizzati i rischi legati all'accesso di terze parti ai sistemi e ai dati dell'organizzazione. Si richiede che sulla base dei risultati dell'analisi dei rischi, siano applicate misure adeguate a ridurre, monitorare e misurare la probabilità e l'impatto di accessi non autorizzati o inappropriati.

18. Si richiede che le credenziali degli account utente interni all'organizzazione o dei clienti (tenant) siano soggette a restrizioni, garantendo una gestione appropriata dell'identità, dei diritti e degli accessi, in conformità con politiche e procedure stabilite. Si richiede che sia garantito quanto segue: la verifica dell'identità e interoperabilità delle applicazioni di servizio (API) e dei processi informativi (ad esempio SSO e Federation), la gestione del ciclo di vita delle credenziali degli account. Si richiede che siano disponibili le modalità di autenticazione Application-to-Application e Machine-to-Machine per l'accesso alle risorse.

19. Si richiede che l'architettura di rete sia documentata chiaramente, evidenziando ambienti ad alto rischio e flussi di dati rilevanti per la conformità normativa. Si richiede che siano implementate misure tecniche di sicurezza a più livelli per rilevare e rispondere in modo tempestivo ad attacchi di rete, incluso traffico anomalo e attacchi DDoS.

20. Si richiede un adeguato servizio di assistenza e supporto in lingua italiana 24 ore al giorno, 7 giorni alla settimana per tutto l'anno.

II. 1.5 MODALITA' DI RISPOSTA

Nella tabella seguente sono riportate le linee guida per la strutturazione del riscontro alle richieste informative relative ai Requisiti minimi e valutativi.

Voce	Descrizione
Obiettivo	Confermare la presenza o assenza dei requisiti minimi o distintivi tecnici e di sicurezza, descrivendo inoltre la proposta di gestione di ogni requisito qualitativo da parte dell'Operatore Economico.
Contenuti richiesti	• Specificati in ciascuna sezione
Livello qualitativo atteso della risposta	• Grado di copertura dei requisiti minimi o distintivi tecnici e di sicurezza
	• Chiarezza e qualità delle descrizioni tecniche fornite
	• Grado di maturità e robustezza delle soluzioni proposte in termini di sicurezza, affidabilità e scalabilità
Formato richiesto	• Documento: File word
	• Lingua del documento: Italiano
	• Lunghezza massima: La lunghezza massima consentita sarà di 40 pagine così ripartite: 25 pagine (A4) per i requisiti valutativi tecnici a carattere qualitativo e ulteriori 15 pagine (A4) per i requisiti valutativi di sicurezza a carattere qualitativo – Copertina, indice e allegati esclusi. Per i requisiti minimi o distintivi (tecnici e di sicurezza) è richiesto di riportare, nello stesso documento negli allegati, la tabella con l'aggiunta di una colonna dedicata, nella quale l'Operatore Economico dovrà indicare, mediante il valore "Y" (Yes) o "N" (No), il rispetto o meno del requisito (con ulteriore colonna di note da popolare con link a documentazione pubblica consultabile a conferma di quanto indicato ed ulteriori informazioni qualora ritenuto necessario)
	• Font: Arial 10 pt
	• Interlinea: 1,5

II. 2 USE CASE E SCENARI DI MIGRAZIONE CLOUD

Nell'ambito della presente RFI, è richiesto all'Operatore Economico di presentare soluzioni, strumenti e approcci metodologici applicabili a scenari concreti di migrazione e modernizzazione infrastrutturale e applicativa, con riferimento agli Use Case proposti. Al fine di garantire l'effettiva realizzazione delle soluzioni proposte, è necessario che queste rispettino una serie di pre-requisiti architetturali e di integrazione considerati fondamentali dalla Società Procedente per assicurare interoperabilità, sicurezza e coerenza con il modello ibrido attualmente in essere:

- Interoperabilità con ambienti on-premise: Le applicazioni migrate o modernizzate devono poter comunicare in modo sicuro e affidabile con sistemi e servizi ancora presenti in ambienti on-premise, garantendo la continuità operativa e l'integrazione tra ambienti ibridi.
- Gestione del traffico in ingresso: Tutto il traffico in ingresso verso le applicazioni cloud deve essere veicolato tramite un API Gateway, che svolga funzioni di routing, autenticazione, rate limiting e monitoraggio, in conformità con le best practice di sicurezza e scalabilità.
- Gestione del traffico in uscita: Il traffico in uscita dalle applicazioni verso l'esterno deve essere instradato attraverso il Web Application Firewall aziendale, al fine di garantire la protezione da attacchi comuni (es. SQL injection, XSS) e il rispetto delle policy di sicurezza definite dall'organizzazione.

II. 2.1 USE CASE 1 - MIGRAZIONE DI MACCHINE VIRTUALI (VM) DA INFRASTRUTTURA ON-PREMISE A CLOUD

Contesto operativo

L'Ente dispone attualmente di un'infrastruttura on-premise basata su tecnologia VMware vSphere. Tali macchine ospitano servizi applicativi, database relazionali e componenti middleware critici per l'operatività interna. L'infrastruttura, pur risultando funzionale, presenta limiti crescenti in termini di scalabilità, resilienza, aggiornamento tecnologico e costi di gestione.

Obiettivo della migrazione

L'Ente intende avviare un processo di progressiva migrazione dell'ambiente virtuale verso un'infrastruttura cloud qualificata, in grado di garantire:

- Maggiore disponibilità e continuità operativa dei servizi
- Scalabilità elastica in risposta alle variazioni di carico
- Ottimizzazione dei costi infrastrutturali
- Aderenza a standard di sicurezza e compliance europei

Vincoli e requisiti specifici

La migrazione dovrà avvenire secondo un approccio "lift & shift", prevedendo il mantenimento delle seguenti condizioni:

- Conservazione delle configurazioni di rete e delle integrazioni applicative esistenti
- Applicazione di criteri di cifratura dei dati a riposo e in transito

- Attivazione di soluzioni di backup giornaliero con retention minima di 30 giorni
- Minimizzazione del downtime durante la fase di cutover

Richieste al fornitore

Si richiede di:

1. **Descrivere l'approccio metodologico adottato** per la discovery, l'assessment e la successiva migrazione delle VM, specificando eventuali framework proprietari o standard utilizzati.
2. **Elencare gli strumenti e le soluzioni tecnologiche impiegate**, sia nativi che di terze parti, per supportare l'intero ciclo di migrazione
3. **Illustrare le modalità con cui viene garantita la consistenza dei dati** durante la migrazione, con particolare attenzione alla replica in tempo reale o differita, e all'integrità applicativa.
4. **Descrivere il piano di validazione post-migrazione**, includendo test funzionali, verifica della connettività di rete, accesso ai volumi di storage, ripristino delle policy di sicurezza e configurazioni IAM.
5. **Fornire una stima dei tempi medi necessari** per completare la migrazione per gruppi di VM (batch), distinguendo eventualmente tra VM mission-critical e VM a basso impatto.
6. **Stimare i costi di run per un periodo temporale di 3/5** anni considerando le diverse classi di applicazioni (Sistemistiche, Mission Critical, High/Medium/Low Business Critical) e indicare gli strumenti disponibili per valutare in tempo reale scenari di ottimizzazione e consumo. Tali strumenti devono consentire analisi on demand, simulazioni di impatto e monitoraggio dei costi con aggiornamenti dinamici. Deve essere garantita la possibilità di integrare queste funzionalità con processi di governance e reporting aziendale

II. 2.2 USE CASE 2 - MIGRAZIONE DI APPLICAZIONI CONTAINERIZZATE DA INFRASTRUTTURA ON-PREMISE A CLOUD

Contesto operativo

L'Ente attualmente gestisce un cluster Kubernetes on-premise. Tali microservizi sono esposti mediante ingress controller e bilanciatori di carico interni, e supportano applicazioni business-critical, integrate con servizi interni e componenti esterni.

Obiettivo della migrazione

Il progetto mira a migrare l'intero cluster Kubernetes verso una piattaforma cloud gestita (es. Azure Kubernetes Service - AKS, Amazon EKS, Google GKE, Red Hat OpenShift), mantenendo la

piena continuità operativa e assicurando la portabilità e la compatibilità delle configurazioni esistenti.

Vincoli e requisiti specifici

La migrazione dovrà garantire:

- Trasferimento completo di Persistent Volume Claims (PVC), secrets, e configurazioni di rete
- Mantenimento delle definizioni di deployment attuali (manifest YAML, Helm charts)
- Aderenza agli standard Kubernetes ufficiali per assicurare interoperabilità e portabilità
- Integrazione fluida con i sistemi di autenticazione e monitoraggio già in uso

Richieste al fornitore

Si richiede di:

1. **Descrivere nel dettaglio la strategia di migrazione proposta**, indicando la metodologia utilizzata (es. backup/restore, replica, blue-green deployment, canary release).
2. **Illustrare come verranno gestiti i volumi persistenti**, i componenti di rete (Ingress, Load Balancer), i certificati SSL/TLS e la migrazione dei secrets.
3. **Fornire un piano strutturato di validazione post-migrazione**, che includa test funzionali, verifiche dei servizi esposti, analisi delle dipendenze e riconfigurazione degli accessi.
4. **Dettagliare le misure di rollback previste**, specificando in quali casi sarà possibile un ritorno sicuro all'ambiente originario.
5. **Indicare le soluzioni di monitoraggio, logging e osservabilità** che verranno messe in atto nel nuovo ambiente cloud (es. Prometheus, Grafana, Fluentd, ELK stack, servizi nativi)
6. **Stimare i costi di run per un periodo temporale di 3/5** anni considerando le diverse classi di applicazioni (Sistemistiche, Mission Critical, High/Medium/Low Business Critical) e indicare gli strumenti disponibili per valutare in tempo reale scenari di ottimizzazione e consumo. Tali strumenti devono consentire analisi on demand, simulazioni di impatto e monitoraggio dei costi con aggiornamenti dinamici. Deve essere garantita la possibilità di integrare queste funzionalità con processi di governance e reporting aziendale

II. 2.3 USE CASE 3 - MIGRAZIONE DI MACCHINE VIRTUALI (VM) DA UN PROVIDER CLOUD AD ALTRO PROVIDER (OPERATORE ECONOMICO)

Contesto operativo

L'Ente dispone attualmente di un'infrastruttura IaaS erogata da un provider cloud (Provider A) impiegate per applicazioni interne, servizi web e basi dati. Per motivi legati a strategia multi-cloud, ottimizzazione dei costi, sicurezza e sovranità dei dati, è stata avviata una valutazione per la migrazione dell'intero parco VM verso un differente provider (Provider B), che presenti caratteristiche più vantaggiose in termini economici, di compliance normativa (e.g. GDPR, NIS2) e di localizzazione dei dati.

Obiettivo della migrazione

Eseguire una migrazione completa delle macchine virtuali dall'attuale cloud provider A verso il cloud provider B in modalità **"lift & shift"**, minimizzando l'interruzione dei servizi e mantenendo inalterate configurazioni e integrazioni, con possibilità di successivo **refactoring applicativo**.

Vincoli e requisiti specifici:

- Necessità di mantenere IP privati, configurazioni firewall e regole di sicurezza
- Migrazione trasparente di volumi, snapshot e storage associato
- Mantenimento delle dipendenze applicative e delle policy di sicurezza esistenti
- Continuità operativa durante la migrazione, con downtime limitato

Richieste al fornitore

Si richiede di:

1. **Descrivere la metodologia di migrazione inter-cloud** proposta, specificando se basata su replica continua, esportazione/importazione di immagini, orchestrazione o altri approcci.
2. **Indicare gli strumenti nativi o di terze parti adottati**, come ad esempio CloudEndure, HCX, Migrate for Compute Engine, vMotion cross-cloud, ecc.
3. **Illustrare le misure adottate per garantire la sicurezza del traffico dati** durante il trasferimento, inclusi protocolli di cifratura, VPN dedicate e segmentazione della rete.
4. **Fornire un piano di test e validazione post-cutover**, comprensivo di controlli su networking, sicurezza, storage e performance.
5. **Specificare le modalità di migrazione incrementale**, se previste, per minimizzare il downtime e garantire continuità dei servizi.
6. **Stimare i costi di run per un periodo temporale di 3/5** anni considerando le diverse classi di applicazioni (Sistemistiche, Mission Critical, High/Medium/Low Business Critical) e indicare gli strumenti disponibili per valutare in tempo reale scenari di ottimizzazione e consumo. Tali strumenti devono consentire analisi on demand, simulazioni di impatto e

monitoraggio dei costi con aggiornamenti dinamici. Deve essere garantita la possibilità di integrare queste funzionalità con processi di governance e reporting aziendale

II. 2.4 USE CASE 4 - MIGRAZIONE DI APPLICAZIONI CONTAINERIZZATE DA UN PROVIDER CLOUD A UN ALTRO PROVIDER (OPERATORE ECONOMICO)

Contesto operativo

L'Ente attualmente esegue un cluster Kubernetes gestito presso un provider cloud, all'interno. Questi microservizi erogano API REST, utilizzano code di messaggistica e database NoSQL, e sono integrati con diversi sistemi di sicurezza, logging e monitoraggio. L'Ente intende migrare l'intero cluster verso un nuovo provider cloud – gestito o self-hosted – al fine di rafforzare la strategia multi-cloud, garantire una maggiore sovranità dei dati e ottimizzare i costi operativi.

Obiettivo della migrazione

Trasferire in modo sicuro e trasparente l'intero ambiente applicativo containerizzato da un provider cloud a un altro, assicurando la continuità operativa, la compatibilità con gli standard Kubernetes ufficiali e la portabilità delle configurazioni esistenti.

Vincoli e requisiti specifici:

- Migrazione di registry immagini, Persistent Volume Claim (PVC), Ingress, e policy di rete.
- Integrazione nel nuovo ambiente con i sistemi esistenti di Identity & Access Management (IAM), monitoraggio, logging e audit.
- Necessità di preservare la configurazione delle risorse Kubernetes (Helm chart, manifest YAML).
- Trasferimento sicuro dei dati e capacità di migrazione trasparente di volumi e snapshot associati.

Richieste al fornitore

Si richiede di:

1. **Descrivere la metodologia proposta per la migrazione inter-cloud**, specificando se basata su replica continua, esportazione di immagini, orchestrazione, backup/restore o strategie blue-green deployment.
2. **Spiegare come viene garantita la portabilità delle immagini container**, delle configurazioni di cluster e dei volumi persistenti, assicurando la continuità delle dipendenze applicative.
3. **Illustrare le modalità di gestione della configurazione del cluster di destinazione**, incluse le configurazioni di rete, ingress controller, certificati e policy.

4. **Fornire un piano dettagliato di test e validazione post-migrazione**, con attenzione a sicurezza, performance e integrazione con gli strumenti di osservabilità.

5. **Dettagliare la strategia di rollback** in caso di errori o malfunzionamenti nel cluster target.

6. **Illustrare le opzioni di supporto per ambienti ibridi o multi-cloud**, incluse funzionalità di monitoraggio centralizzato, gestione delle policy e sicurezza.

7. **Stimare i costi di run per un periodo temporale di 3/5** anni considerando le diverse classi di applicazioni (Sistemistiche, Mission Critical, High/Medium/Low Business Critical) e indicare gli strumenti disponibili per valutare in tempo reale scenari di ottimizzazione e consumo. Tali strumenti devono consentire analisi on demand, simulazioni di impatto e monitoraggio dei costi con aggiornamenti dinamici. Deve essere garantita la possibilità di integrare queste funzionalità con processi di governance e reporting aziendale

II. 2.5 USE CASE 5 - INTEGRAZIONE IOT PER BI EVOLUTA E CONVERSAZIONALE

Contesto operativo

L'Ente intende valutare una soluzione cloud-native per l'integrazione in tempo reale di piattaforme IoT eterogenee, al fine di abilitare una gestione avanzata dei flussi dati provenienti da sensori e dispositivi distribuiti. Le piattaforme IoT coinvolte utilizzano protocolli differenti (MQTT, API REST, Kafka) e presentano formati e frequenze di pubblicazione non omogenei. La soluzione dovrà garantire elevate prestazioni, sicurezza, scalabilità e capacità di analisi evoluta.

Obiettivo della soluzione

Realizzare una piattaforma cloud-native che abiliti l'integrazione in tempo reale di piattaforme IoT eterogenee, assicuri l'ingestione, la normalizzazione e la correlazione dei flussi dati ad elevate prestazioni, ed offra una Business Intelligence evoluta con dashboard interattive e reporting conversazionale per insight immediati e azionabili.

Vincoli e requisiti specifici:

- Integrazione in tempo reale di due piattaforme IoT eterogenee che trasmettono eventi via MQTT, API REST e Kafka, con formati dati e frequenze differenti.

- Ingestione, normalizzazione e correlazione dei flussi in modo scalabile e sicuro, con latenza minima tra generazione del segnale e disponibilità nel sistema di Business Intelligence.

- Pipeline di data processing ad alte prestazioni fino a 15.000 eventi/s, con arricchimento semantico, deduplicazione e auto-scaling orizzontale per sostenere picchi fino al +300% rispetto ai volumi medi.

- Data Lakehouse per analisi storiche e predittive, con BI evoluta che abilita dashboard geospaziali real-time e reporting conversazionale in linguaggio naturale, fornendo insight tempestivi sui KPI operativi e di performance.

- Abilitazione ML: utilizzo dei dati consolidati per training di algoritmi di predizione e loro inferenza in tempo reale.

Richieste al fornitore

Si richiede di:

1. **Disegnare l'architettura logica della soluzione,** in linea con la reference architecture dell'Ente, esplicitando le opzioni valutate e le motivazioni delle scelte finali.

2. **Disegnare l'architettura fisica della soluzione,** dettagliando l'utilizzo di risorse Cloud IaaS/PaaS/SaaS.

3. **Analizzare il comportamento della soluzione in scenari di crescita esponenziale dei segnali al secondo,** descrivendo i meccanismi di scalabilità, resilienza e bilanciamento del carico su tutte le componenti per prevenire colli di bottiglia e garantire la continuità di servizio.

II. 2.6 MODALITA' DI RISPOSTA

Nella tabella seguente sono riportate le linee guida per la strutturazione del riscontro alle richieste informative relative agli Use Case.

Voce	Descrizione
Obiettivo	Descrivere la soluzione, gli strumenti, l'approccio metodologico proposto dall'Operatore Economico sullo specifico Use case proposto
Contenuti richiesti	• Specificati in ciascun Use case nella sezione "Richieste al fornitore"
Livello qualitativo atteso della risposta	• Qualità e chiarezza della metodologia proposta
	• Grado di innovazione dell'approccio
	• Grado di copertura delle informazioni fornite rispetto ai contenuti richiesti
Formato richiesto	• Documento: File word
	• Lunghezza massima: 4 pagine (A4) per Use Case (Copertina e indice esclusi), per un totale di 20 pagine
	• Lingua del documento: italiano
	• Font: Arial 10 pt
	• Interlinea: 1,5

II. 3 PROFILI PROFESSIONALI

La Società Procedente si riserva di verificare che i profili professionali indicati dall'Operatore Economico presentino caratteristiche coerenti con i requisiti minimi descritti per ciascuna figura di riferimento.

I profili richiesti sono i seguenti:

Profili Professionali	Anni di esperienza richiesti	Anni esperienza nel ruolo
Project Manager	6 anni	4 anni
Cloud Application Architect	8 anni	4 anni
Cloud Application Specialist	6 anni	2 anni
Cloud System Engineer	6 anni	4 anni
Cloud SecOps Specialist	6 anni	2 anni

Le figure professionali, dipendenti e/o Partner della società committente proposti dovranno essere ricondotte a quelle di seguito descritte, laddove i requisiti espressi sono considerati requisiti minimi.

Saranno presi in considerazione esclusivamente i CV forniti in formato europeo con chiara indicazione negli anni di esperienza nel ruolo e su progetti specifici afferenti al ruolo proposto.

Le persone che l'offerente potrà candidare per i profili richiesti dovranno rispondere a requisiti precisi in termini di responsabilità, competenze e livello d'istruzione in assenza dei quali il candidato non sarà ritenuto idoneo.

II. 3.1 PROJECT MANAGER

Il Profilo professionale deve essere in possesso di una laurea triennale o di una cultura equivalente, con un'anzianità lavorativa di almeno 6 anni e comprovata esperienza nella gestione di progetti complessi di IT, Digital & Business Transformation nel settore trasporti o ambiti affini, di cui almeno 4 anni maturati nello svolgimento della specifica funzione su progetti analoghi.

È richiesta una conoscenza approfondita del settore pubblico, maturata attraverso esperienze dirette in progetti, preferibilmente presso la Pubblica Amministrazione italiana.

Il candidato dovrà inoltre possedere:

- Esperienza di Advisory in ambito ICT, con particolare riferimento alla definizione di piani operativi, modelli di governance IT, disegno di scenari alternativi e sviluppo di business case;
- Elevate competenze di Program & Project Management;

- Conoscenza certificata della lingua inglese con livello minimo C1 Advanced, comprovata da una delle seguenti certificazioni: Cambridge CAE, IELTS (7.0–8.0), TOEFL iBT (≥95), TOEIC (945–990);

Il candidato deve possedere almeno una delle seguenti certificazioni:

- PMI / PMP / ISIPM / IPMA / AgilePM® / Scrum Master / ITIL 4 / TOGAF / PRINCE2® / COBIT

In aggiunta ai requisiti sopra indicati, il candidato deve aver maturato almeno 4 anni di esperienza comprovata nel ruolo di Responsabile di Progetto, con responsabilità diretta nella gestione e nel coordinamento di team di lavoro e con le seguenti caratteristiche:

- Responsabilità complessiva di tutte le attività progettuali, assicurando il rispetto di tempi, costi, standard di qualità e obiettivi di progetto;
- Coordinamento e motivazione del team di lavoro, garantendo coerenza con gli obiettivi strategici e la massima efficacia ed efficienza operativa;
- Capacità di individuare e gestire criticità e rischi progettuali, proponendo soluzioni e azioni correttive tempestive;
- Abilità nel relazionarsi con i vertici organizzativi e nel rappresentare in modo chiaro e sintetico lo stato di avanzamento dei progetti.

Di seguito si riporta, a titolo indicativo e non esaustivo, una tabella con i principali requisiti minimi richiesti per la figura professionale.

Figura Professionale	**Requisiti minimi obbligatori**				
	Certificazione IT (almeno una delle seguenti)	Certificazione Lingua Inglese	Anzianità lavorativa	Comprovata esperienza nella specifica funzione	Istruzione
Project Manager	• PMI • PMP • ISIPM • IPMA •AgilePM • Scrum Master • ITIL 4 • TOGAF • PRINCE2 • COBIT	C1 Advanced (Certificazioni: • Cambridge CAE • IELTS (7.0–8.0) • TOEFL iBT (≥95) • TOEIC (945–990))	6 anni	4 anni	Laurea triennale o di una cultura equivalente

II. 3.2 CLOUD APPLICATION ARCHITECT

Il Profilo professionale deve essere in possesso di una laurea triennale o di vecchio ordinamento, o di una cultura equivalente, con un'anzianità lavorativa complessiva di almeno 8 anni, di cui almeno 4 maturati nello svolgimento della specifica funzione di Cloud Application Architect.

È richiesta una comprovata esperienza nella progettazione, evoluzione e manutenzione di architetture applicative basate su paradigma Cloud, in grado di coniugare la complessità funzionale con soluzioni tecnologiche scalabili, sicure e allineate ai requisiti della Pubblica Amministrazione.

Il Professionista dovrà inoltre possedere:

- Esperienza nel disegno, progettazione, implementazione e certificazione di architetture applicative Cloud per servizi efficienti, resilienti, manutenibili e collaborativi;
- Competenze nella definizione di strategie, piani di migrazione e controllo di applicazioni e sistemi verso il Cloud;
- Capacità di allineare le scelte architetturali di Cloud Computing con la strategia IT complessiva dell'Amministrazione;
- Conoscenza delle principali tecnologie e standard del settore, tra cui:
    - Framework di containerizzazione (Docker, rkt, LXC);
    - Servizi di virtualizzazione per l'hosting di istanze compute, equivalenti a macchine virtuali gestite su piattaforme cloud;
    - Orchestrator (Kubernetes, Marathon);
    - Cluster scheduler (Docker Swarm, Apache Mesos);
    - Overlay network framework (Flannel, Weave, Calico);
    - Standard di riferimento: OVF, OCCI, CIMI, OCI, TOSCA;
    - Tecnologie di virtualizzazione (VMware, Virtual PC, Citrix);
    - Progettazione di architetture Cloud-based e RESTful APIs.
- Esperienza nell'applicazione di metodologie DevOps su progetti complessi e nell'integrazione di soluzioni Cloud all'interno di architetture Enterprise;
- Conoscenza approfondita di linguaggi e piattaforme di sviluppo: Python, Java, Perl, Ruby, Scala, Node.js, Clojure, C++, JavaScript, PHP, .NET;
- Competenza nell'utilizzo di servizi DNS, CDN e reti virtuali private offerti da piattaforme cloud;
- Capacità di eseguire analisi post-evolutive per valutare benefici, KPI, scalabilità, risparmi e agilità dei sistemi implementati;
- Abilità nel dirigere o supportare l'integrazione dei sistemi, coordinandosi con team interni e fornitori di servizi IAAS/PAAS;
- Conoscenza delle normative di riferimento: Legge n. 4/2004, CAD e aggiornamenti, normativa privacy, Piano Triennale per l'informatica nella PA.

Il candidato deve possedere almeno una delle seguenti certificazioni cloud:

a) Cloud Architect Certification rilasciata da provider di servizi cloud pubblici o privati (es. AWS, Azure, Google Cloud, Oracle, IBM, ecc.)
b) Certificazioni equivalenti rilasciate da enti terzi indipendenti (es. TOGAF, Open Group, CSA, Cloud Credential Council, ecc.)

Di seguito si riporta, a titolo indicativo e non esaustivo, una tabella con i principali requisiti minimi richiesti per la figura professionale.

Figura Professionale	**Requisiti minimi obbligatori**				
	Certificazione IT	Certificazione Lingua Inglese	Anzianità lavorativa	Comprovata esperienza nella specifica funzione	Istruzione
Cloud Application Architect	• Cloud Architect Certification rilasciata da provider di servizi cloud pubblici o privati (es. AWS, Azure, Google Cloud, Oracle, IBM, ecc.) • Certificazioni equivalenti rilasciate da enti terzi indipendenti (es. TOGAF, Open Group, CSA, Cloud Credential Council, ecc.)	B2 upper-intermediate (Certificazioni: Cambridge FCE, IELTS 5.5-6.5, TOEFL iBT 72, TOEIC 785-944))	8 anni	4 anni	Laurea triennale o di una cultura equivalente

II. 3.3 CLOUD APPLICATION SPECIALIST

Il Profilo professionale deve essere in possesso di una laurea triennale o di vecchio ordinamento, o di una cultura equivalente, con un'anzianità lavorativa complessiva di almeno 6 anni, di cui almeno 2 maturati nello svolgimento della specifica funzione di Cloud Application Specialist.

È richiesta una comprovata esperienza nell'implementazione e integrazione di soluzioni applicative basate su Cloud Computing, garantendo il corretto delivery di progetti e l'allineamento con le scelte architetturali e strategiche dell'Amministrazione.

Il Professionista dovrà inoltre possedere:

- Esperienza nella gestione del delivery di progetti di adozione di soluzioni Cloud;
- Competenze tecnologiche approfondite sulle soluzioni Cloud e capacità di fungere da riferimento tecnico per il team di progetto;
- Esperienza nella guida dell'implementazione di soluzioni Cloud e nel supporto allo sviluppo e integrazione dei componenti;
- Capacità di contribuire alla definizione dei requisiti funzionali coerenti con le scelte architetturali;
- Conoscenza delle principali tecnologie e standard del settore, tra cui:
    - Framework di containerizzazione: Docker, rkt;

  - Servizi di virtualizzazione per l'hosting di istanze compute, equivalenti a macchine virtuali gestite su piattaforme cloud;
  - Sistemi operativi: Desktop, Server, Mobile;
  - Orchestrator: Kubernetes, Marathon;
  - Cluster scheduler: Docker Swarm, Apache Mesos;
  - Overlay network framework: Flannel, Weave, Calico;
  - Architetture web-based RESTful APIs;
  - Tecnologie di virtualizzazione: VMware, Virtual PC, Citrix.
- Esperienza nell'applicazione di metodologie DevOps su progetti complessi;
- Capacità di gestire servizi cloud per DNS, distribuzione di contenuti (CDN) e reti virtuali private;
- Competenza nell'utilizzo di linguaggi e piattaforme di sviluppo cloud native: Python, Java, Perl, Ruby, Scala, Node.js, Clojure, C++, JavaScript, PHP, .NET;
- Capacità di verificare prestazioni, integrazione e conformità delle soluzioni Cloud ai requisiti progettuali.

Il candidato deve possedere almeno una delle seguenti certificazioni Cloud:

- Certificazioni rilasciate da provider di servizi cloud pubblici o privati, relative a ruoli tecnici quali: Cloud Engineer, DevOps Engineer, Security Specialist, Network Engineer, SRE, System Administrator;
- Certificazioni equivalenti rilasciate da enti terzi indipendenti, che attestino competenze in ambito DevOps, Cloud Security, Infrastructure Management, e Application Delivery.

Di seguito si riporta, a titolo indicativo e non esaustivo, una tabella con i principali requisiti minimi richiesti per la figura professionale.

Figura Professionale	**Requisiti minimi obbligatori**				
	Certificazione IT	Certificazione Lingua Inglese	Anzianità lavorativa	Comprovata esperienza nella specifica funzione	Istruzione
Cloud Application Specialist	• Certificazioni rilasciate da provider di servizi cloud pubblici o privati, relative a ruoli tecnici quali: Cloud Engineer, DevOps Engineer, Security Specialist, Network Engineer, SRE, System Administrator; • Certificazioni equivalenti rilasciate da enti terzi indipendenti, che attestino competenze in ambito DevOps, Cloud Security, Infrastructure	B2 upper-intermediate (Certificazioni: Cambridge FCE, IELTS 5.5-6.5, TOEFL iBT 72, TOEIC 785-944))	6 anni	2 anni	Laurea triennale o di una cultura equivalente

	Management, e Application Delivery.				

II. 3.5 CLOUD SYSTEM ENGINEER

Il Profilo professionale deve essere in possesso di una laurea triennale o di vecchio ordinamento, o di una cultura equivalente, con un'anzianità lavorativa complessiva di almeno 6 anni, di cui almeno 4 maturati nello svolgimento della specifica funzione di Cloud System Engineer.

È richiesta una comprovata esperienza nella gestione operativa dei sistemi informatici basati su infrastrutture Cloud, con particolare attenzione all'integrazione dei sistemi, al deployment dei servizi e al supporto tecnico continuo. Il candidato dovrà inoltre possedere:

- Esperienza nella configurazione, integrazione e gestione di server, storage e reti virtuali in ambienti Cloud.
- Capacità di monitorare e ottimizzare le performance dei sistemi, garantendo alta disponibilità, resilienza e continuità dei servizi.
- Competenza nella gestione di ambienti multi-cloud e nella risoluzione di problematiche operative, incident management e troubleshooting.
- Esperienza nell'automazione di task operativi tramite strumenti come Ansible, Terraform, CloudFormation.
- Conoscenza delle best practice di sicurezza dei sistemi Cloud, incluse gestione delle identità, controlli di accesso e crittografia.
- Capacità di collaborare con team tecnici e sviluppatori per garantire il corretto funzionamento e la manutenzione dei servizi Cloud.
- Conoscenza delle normative e degli standard di settore relativi alla protezione dei dati e alla privacy, con particolare riferimento al GDPR.

Il Professionista deve possedere almeno una delle seguenti certificazioni:

- Certificazioni relative a ruoli tecnici quali: Cloud Administrator, Cloud Operations Specialist, Cloud Security Engineer, Data Engineer, Network Engineer, System Administrator;
- Certificazioni rilasciate da provider di servizi cloud pubblici o privati, oppure da enti indipendenti che attestino competenze in ambito infrastrutturale, sicurezza, automazione e gestione dei dati.

Di seguito si riporta, a titolo indicativo e non esaustivo, una tabella con i principali requisiti minimi richiesti per la figura professionale.

Figura Professionale	**Requisiti minimi obbligatori**

	Certificazione IT	Certificazione Lingua Inglese	Anzianità lavorativa	Comprovata esperienza nella specifica funzione	Istruzione
Cloud System Engineer	• Certificazioni relative a ruoli tecnici quali: Cloud Administrator, Cloud Operations Specialist, Cloud Security Engineer, Data Engineer, Network Engineer, System Administrator; • Certificazioni rilasciate da provider di servizi cloud pubblici o privati, oppure da enti indipendenti che attestino competenze in ambito infrastrutturale, sicurezza, automazione e gestione dei dati.	B2 upper-intermediate (Certificazioni: Cambridge FCE, IELTS 5.5-6.5, TOEFL iBT 72, TOEIC 785-944))	6 anni	4 anni	Laurea triennale o di una cultura equivalente

II. 3.6 CLOUD SECOPS SPECIALIST

Il Profilo professionale deve essere in possesso di una laurea triennale o di una cultura equivalente, con un'anzianità lavorativa complessiva di almeno 6 anni, di cui almeno 2 maturati nello svolgimento della specifica funzione di Cloud SecOps Specialist.

È richiesta una comprovata esperienza nella gestione delle operazioni di sicurezza in ambienti cloud, garantendo la protezione delle infrastrutture, delle applicazioni e dei dati attraverso attività di monitoraggio, rilevamento delle minacce, risposta agli incidenti e implementazione di controlli di sicurezza. Il candidato dovrà inoltre possedere:

- Esperienza nel gestire e monitorare le operazioni di sicurezza in ambienti cloud, identificando e rispondendo a minacce e vulnerabilità.
- Esperienza nell'implementare e mantenere controlli di sicurezza, come firewall, sistemi di rilevamento delle intrusioni e gestione degli accessi.
- Collaborare con team di ingegneria e architettura per progettare soluzioni sicure e resilienti.
- Conoscenza dei processi di automazione dei sistemi di sicurezza per migliorare l'efficienza operativa.
- Condurre indagini su incidenti di sicurezza e fornire risposte tempestive per mitigare i rischi.
- Mantenere la conformità con le normative e gli standard di sicurezza applicabili.
- Fornire formazione e supporto ai team interni su best practice di sicurezza.

Conoscenze richieste:

- Principi di sicurezza cloud e modelli di servizio (IaaS, PaaS, SaaS).
- Strumenti di gestione della postura di sicurezza del cloud (CSPM).
- Sistemi di gestione delle informazioni e degli eventi di sicurezza (SIEM).

- Tecniche di rilevamento delle minacce e gestione degli incidenti.
- Automazione della sicurezza e scripting (es. Python, Bash).
- Conoscenza delle normative di sicurezza e dei framework di conformità.
- Tecniche di gestione degli accessi e controllo delle identità (IAM).

Sono considerati un plus possedere almeno una delle seguenti certificazioni:

- GIAC Security Essentials (GSEC)
- EC-Council Certified Ethical Hacker (CEH)

Inoltre, il Professionista deve possedere almeno una delle seguenti certificazioni in ambito Cloud security:

- Certificazioni specifiche in ambito Cloud Security, rilasciate da provider di servizi cloud pubblici o privati, oppure da enti indipendenti
- Certificazioni che attestino competenze in ambiti quali: cybersecurity applicata al cloud, gestione delle identità e degli accessi, monitoraggio e risposta agli incidenti, conformità normativa, e architetture sicure

Di seguito si riporta, a titolo indicativo e non esaustivo, una tabella con i principali requisiti minimi richiesti per la figura professionale.

Figura Professionale	**Requisiti minimi obbligatori**				
	Certificazione IT	Certificazione Lingua Inglese	Anzianità lavorativa	Comprovata esperienza nella specifica funzione	Istruzione
Cloud SecOps Specialist	**Mandatorio**: CompTIA Security+ **Opzionali:** • GIAC Security Essentials (GSEC) • EC-Council Certified Ethical Hacker (CEH) **Ambito Cloud Security:** • Certificazioni specifiche in ambito Cloud Security, rilasciate da provider di servizi cloud pubblici o privati, oppure da enti indipendenti • Certificazioni che attestino competenze in ambiti quali: cybersecurity applicata al cloud, gestione delle identità e degli accessi, monitoraggio e risposta agli incidenti,	B2 upper-intermediate (Certificazioni: Cambridge FCE, IELTS 5.5-6.5, TOEFL iBT 72, TOEIC 785-944))	6 anni	2 anni	Laurea triennale o di una cultura equivalente

	conformità normativa, e architetture sicure				

II. 3.7 MODALITA' DI RISPOSTA

Nella tabella seguente sono riportate le linee guida per la strutturazione del riscontro alle richieste informative relative ai Profili Professionali.

Voce	Descrizione
Obiettivo	Conoscere il numero delle figure professionali, secondo i profili descritti, a disposizione del CSP ed operanti su Territorio Nazionale. A titolo di comprova, condividere per ciascuna figura professionale richiesta i Curriculum Vitae dei professionisti del CSP
Contenuti richiesti	• Le informazioni richieste e specificate per ciascun profilo professionale ove possibile
Livello qualitativo atteso della risposta	• Livello di esperienze maturate dal profilo professionale
	• Grado di conformità alle certificazioni, anni esperienze etc.
Documento	• Copertina di pagine 1, riportante il numero delle figure professionali richieste operanti su Territorio
	• Lingua dei cv: Italiano
	• Documento: CV in formato Europass o equivalente

Si specifica che saranno presi in considerazione esclusivamente i CV forniti in formato europeo o formati equivalenti purchè contengano le medesime sezioni, con chiara indicazione negli anni di esperienza nel ruolo e su progetti specifici afferenti al ruolo proposto. Le informazioni contenute dovranno rispondere a requisiti precisi in termini di responsabilità, competenze e livello d'istruzione in assenza dei quali il CV non sarà ritenuto idoneo.

II. 4 CATALOGO SERVIZI CLOUD

Di seguito è riportata una tabella riepilogativa che sintetizza, in maniera non esaustiva, il catalogo dei servizi Cloud di tipo IaaS e PaaS oggetto della presente richiesta.

L'Operatore Economico è invitato a integrare e completare il catalogo con le proprie specifiche di servizio, eventualmente inserendo più occorrenze per ciascuna tipologia di servizio e fornendo ulteriori dettagli tecnici ritenuti pertinenti incluse le politiche di Reservation o altre politiche che prevedono un'ottimizzazione dei costi (quali ad esempio politiche di scontistica, crediti, servizio di migrazione, etc.).

Saranno valutati come elementi migliorativi la presenza di tool a supporto dell'operatività quali:

- FinOps: strumenti configurabili per il monitoraggio e l'ottimizzazione automatica dei costi, che agiscono sulla base di policy definite dal cliente, specificando come questi siano in grado di rilevare anomalie di costo (es. “Bill shock”) e innescare in automatico azioni correttive
- DevOps: strumenti per l'automazione, CI/CD, gestione pipeline e deployment
- Governance centralizzata: piattaforme di gestione unificata delle risorse cloud, preferibilmente con supporto multicloud, per garantire compliance, sicurezza e controllo centralizzato delle configurazioni

Ambito	Categoria	Specifiche tecniche	Unità di Misura
Virtualizzazione	General purpose - small	1 vCPU, 2 GB RAM	€/mese
	General purpose - medium	2 vCPU, 4 GB RAM	€/mese
	General purpose - large	2 vCPU, 8 GB RAM	€/mese
	General purpose - xlarge	4 vCPU, 16 GB RAM	€/mese
	Compute optimized - medium	1 vCPU, 2 GB RAM	€/mese
	Compute optimized - large	2 vCPU, 4 GB RAM	€/mese
	Compute optimized - xlarge	4 vCPU, 8 GB RAM	€/mese
	Memory optimized - medium	1 vCPU, 8 GB RAM	€/mese
	Memory optimized - large	2 vCPU, 16 GB RAM	€/mese
	Memory optimized - xlarge	4 vCPU, 32 GB RAM	€/mese
	Storage optimized - large	2 vCPU, 16 GB RAM	€/mese
	Storage optimized - xlarge	4 vCPU, 32 GB RAM	€/mese
Storage	Block Storage Hot	SSD, High IOPS (≥5.000), latenza <1 ms	€/GB/mese
	Block Storage Warm	HDD, medio IOPS, accesso regolare	€/GB/mese

	Block Storage Cold	HDD, basso costo, accesso non frequente	€/GB/mese
	Object Storage Hot	Accesso frequente, latenza bassa, ≥99,9% availability	€/TB/mese
	Object Storage Cool	Accesso saltuario, prezzo ridotto, latenza media	€/TB/mese
	Object Storage Cold	Accesso raro, recupero lento (ore), ≥99,99% durability	€/TB/mese
	Object Storage Archive	Archiviazione a lungo termine, retrieval in ore	€/TB/mese
	File Storage Hot (NAS)	NFS/SMB, throughput elevato, uso applicazioni core	€/TB/mese
	File Storage Warm (NAS)	NFS/SMB, uso regolare, medio throughput	€/TB/mese
	File Storage Cold (NAS)	NFS/SMB, alta capacità, basso throughput, archiviazione	€/TB/mese
BAAS	Backup per VM/Server	Protezione istanza fino a 500 GB	€/istanza/mese
	Backup per VM/Server	Protezione istanza fino a 1 TB	€/istanza/mese
	Backup per VM/Server	Protezione istanza fino a 2 TB	€/istanza/mese
	Backup Storage	Storage attivo (SSD/HDD) – Standard	€/GB/mese
	Backup Storage	Storage a lungo termine (Archive)	€/GB/mese
	Backup Storage	Replica cross-region	€/GB/mese
	Endpoint Backup	Dispositivo utente (PC/Notebook) con 1 TB incluso	€/endpoint/mese
	Endpoint Backup	Storage aggiuntivo oltre 1 TB	€/TB/mese
	Database Backup	DB relazionale fino a 100 GB	€/istanza/mese
	Database Backup	DB relazionale fino a 500 GB	€/istanza/mese
	Database Backup	DB relazionale >500 GB	€/istanza/mese
	Retention	Conservazione backup 30 giorni	€/GB/mese
	Retention	Conservazione backup 1 anno	€/GB/mese

	Retention	Conservazione backup 5 anni (compliance)	€/GB/mese
PAAS	Kubernetes Managed	Cluster 3 nodi (4 vCPU, 8 GB RAM)	€/mese
	Serverless Functions	1M richieste incluse	€/milione richieste
	AI/ML Service	Training CPU/GPU dedicato (specificare inoltre la quantità esatta di GPU H100/B200 disponibili nella UE)	€/ora GPU
DRAAS	Classe 1	-RPO: ≥72 ore -RTO:≥72 ore Note:Backup off-site, recovery manuale, nessuna automazione	€/mese
	Classe 2	-RPO: 8–72 ore -RTO:<24 ore Note:Replica asincrona o backup frequenti, recovery semi-automatico	€/mese
	Classe 3	-RPO: 4–8 ore -RTO:4–8 ore Note:Replica più frequente, automazione parziale, orchestrazione DR	€/mese
	Classe 4	-RPO: 1–4 ore -RTO:1–4 ore Note:Replica quasi real-time, orchestrazione DR avanzata, test periodici	€/mese
	Classe 5	-RPO: <1 ora (anche pochi minuti) -RTO:<1 ora Note:Replica sincrona, hot site sempre pronto, failover automatico	€/mese
	Test DR annuale	Incluso nel canone	forfait

II. 4.1 MODALITA' DI RISPOSTA

Nella tabella seguente sono riportate le linee guida per la strutturazione del riscontro alle richieste informative sul Catalogo Servizi Cloud.

Voce	Descrizione

Obiettivo	Raccogliere e strutturare un catalogo aggiornato dei servizi Cloud IaaS e PaaS offerti dall'Operatore Economico, con dettaglio delle specifiche tecniche
Contenuti richiesti	• Compilazione delle informazioni contenute nel file allegato Catalogo Servizi Cloud • Compilazione delle informazioni relative ad eventuali tool a supporto dell'operatività
Livello qualitativo atteso della risposta	• Grado di copertura ed estensione degli item del catalogo servizi cloud
	• Qualità e chiarezza espositiva sui tool a supporto messi a disposizione (FinOps,DevOps, Governance centralizzata)
Documento	• Documento: File Excel "Catalogo Servizi Cloud" allegato • Documento eventuali tool : File word Lunghezza massima: 5 pagine (A4) Lingua del documento: italiano Font: Arial 10 pt Interlinea: 1,5

II. 5 CRITERI DI SOSTENIBILITÀ

In riferimento all'ambito sostenibilità, viene richiesto all'Operatore Economico di confermare il possesso delle seguenti certificazioni/attestazioni:

ID	Certificazione
1	Certificazione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) ISO 27001
2	Conformità dei datacenter e delle infrastrutture ICT allo standard ISO/IEC 30134
3	Provenienza dell'energia elettrica da fonti rinnovabili per una percentuale pari al 100% dei consumi annui fatturati[1]
4	Certificazione della parità di genere di cui all'articolo 46-bis del decreto legislativo n.198/2006
5	SA 8000 - Social Accountability

II. 5.1 MODALITA' DI RISPOSTA

Nella tabella seguente sono riportate le linee guida per la strutturazione del riscontro alle richieste informative sul Catalogo Servizi Cloud.

Voce	Descrizione
Obiettivo	Conoscere il possesso delle certificazioni / attestazioni in ambito sostenibilità
Contenuti richiesti	• Conferma delle certificazioni richieste
Livello qualitativo atteso della risposta	• Grado di conformità alle certificazioni

[1] Tale certificazione dovrà essere corredata da idonea documentazione di Garanzia d'Origine (GO) per l'Unione Europea oppure RECs per gli Stati Uniti e Canada e i-REC per gli altri Paesi

Documento	• Documento: File word, in cui l'Operatore Economico dovrà fornire apposita dichiarazione resa ai sensi del D.P.R. 445/2000 e s.m.i. e sottoscritta digitalmente dal proprio legale rappresentante o procuratore, includendo l'elenco totale o parziale delle certificazioni richieste possedute
	• Lingua: Italiano

Pier Paolo Argiolas

Firmato da Pier Paolo Argiolas il 18/02/2026 alle 13:06:08 CET

FERSERVIZI S.p.A.

ACCORDO QUADRO

PER I SERVIZI IAAS E PAAS IN AMBITO CLOUD E DEI SERVIZI SPECIALISTICI DI SUPPORTO TECNICO-FUNZIONALE PER LA GESTIONE, IL MONITORAGGIO E L'EVOLUZIONE DELLE INFRASTRUTTURE DIGITALI, GESTITA CON SISTEMI TELEMATICI – *CIG* [•]

[*in caso di gara a Lotti*
LOTTO [•] – Servizi **[o** Servizio**]** di [•] - CIG [•]
LOTTO [•]– Servizi **[o** Servizio**]** di [•] - CIG [•]**]**

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 1, codice fiscale e partita IVA 04207001001, in nome e per Conto di FSTechnology S.p.A. in persona di [•] in qualità di Procuratore munito dei necessari poteri per la sottoscrizione del presente Accordo Quadro (quest'ultima, di seguito, "Committente");

E

[**DENOMINAZIONE DELL'AGGIUDICATARIO**], con sede in [•], via [•], iscritta al registro delle imprese di [•] con il numero [•], codice fiscale [•] e partita IVA [•], in persona di [•] in qualità di [•] munito dei necessari poteri per la sottoscrizione del presente Accordo Quadro (di seguito, "Appaltatore").

Di seguito "**Parti**"

PREMESSO CHE

- Ferservizi è la Società di servizi appartenente al Gruppo Ferrovie dello Stato Italiane, che provvede alla gestione delle forniture e dei servizi *no core business* a supporto delle attività delle altre Società del Gruppo Ferrovie dello Stato Italiane;
- nell'ambito di tali forniture e servizi rientrano anche i servizi oggetto del presente affidamento;
- nel rispetto di quanto previsto dalla normativa vigente, Ferservizi ha avviato con comunicazione del [•].[•].[•], con l'Operatore indicato in epigrafe, una trattativa diretta svolta in modalità telematica, per l'affidamento dei Servizi IaaS e PaaS in ambito Cloud e dei Servizi Specialistici di supporto tecnico-funzionale per la gestione, il monitoraggio e l'evoluzione delle infrastrutture

digitali, gestita con sistemi telematici.

- l'Appaltatore, all'esito della verifica effettuata dal Committente, risulta in possesso dei requisiti di ordine generale e speciale richiesti dalla disciplina vigente in capo all'Appaltatore;

- **[eventuale da inserire: in caso di anticipata esecuzione per urgenza della fornitura:** *in data [•], è stata disposta ai sensi dell'art. 17 co.* ***(8 o 9)*** *del D.Lgs n. 36/2023 , l'anticipata esecuzione delle prestazioni di cui al presente contratto***]**
- **[eventuale** l'Appaltatore ha prestato la garanzia definitiva richiesta;**]**
- al presente Accordo Quadro sarà data attivazione con l'emissione di Ordini applicativi;
- le Parti si danno reciproco atto che quanto emerge dai documenti della procedura, dal presente Accordo Quadro e dai relativi Allegati, definisce in modo adeguato e completo gli impegni che scaturiscono dalla sottoscrizione del presente Accordo Quadro, nonché l'oggetto delle prestazioni da eseguire ad opera dell'Appaltatore, in ogni caso, ha consentito l'acquisizione di tutti gli elementi per un'idonea valutazione, sul piano tecnico ed economico, delle prestazioni, ai fini della formulazione, da parte dell'Appaltatore, della propria Offerta.

Tutto ciò premesso e fermo restando che quanto sopra costituisce parte integrante e sostanziale del presente Accordo Quadro, le Parti convengono quanto segue.

Articolo 1 - Definizioni

a) Accordo o Atto: il presente Accordo Quadro compresi tutti i suoi allegati, nonché i documenti ivi richiamati;

b) Appaltatore: [Denominazione dell'Appaltatore];

c) Capitolato Tecnico o CT: il documento che contiene la descrizione dei servizi e le relative modalità di esecuzione (All. [•]);

d) **[eventuale** Catalogo Ariba: il Catalogo elettronico dei prodotti acquistabili tramite la piattaforma di e-Requisitioning (Ariba) gestita da Ferservizi, di cui al successivo art. 8**]**;

e) Committente: Ferservizi in nome e per conto di FSTechnology S.p.A.

f) Deliverable: la realizzazione di ogni tipo di prodotti, idee, processi industriali, dati di qualsiasi genere, software di qualsiasi genere, codice sorgente, interfaccia, database, manuale, istruzione, procedura, studio o progettazione, inclusi i codici per computer - prodotti OEM (*Original Equipment Manufacturer*) e *firmware* di prodotto, nonché qualsiasi loro modifica, adattamento, sviluppo e/o miglioramento forniti a FS Tech in forza del Contratto;

g) Documenti d'Ordine: si intendono le offerte emesse di volta in volta dall'Appaltatore su richiesta del Committente. Tali Offerte conterranno le specifiche tecniche descrittive dei servizi, fermo restando

che eventuali condizioni normative presenti nelle stesse si riterranno come non apposte;

h) Condizioni Generali: il documento di cui all'art. 3;

i) Gruppo FS: il Gruppo Ferrovie dello Stato Italiane;

j) Offerta: l'Offerta economica [ovvero: tecnica ed economica] presentata in gara dall'Appaltatore e allegata materialmente al presente Accordo [**All.ti** (•) e (•)];

k) Ordine applicativo: il documento redatto in forma di Ordine di Acquisto, con il quale la Società emittente, con le modalità di seguito previste, richiede la fornitura oggetto del presente Accordo;

l) Parte: [Denominazione dell'Appaltatore] o anche il Committente singolarmente;

m) Parti: Committente e Appaltatore;

n) Responsabile dell'Accordo Quadro dell'Appaltatore: il soggetto di cui al successivo art. 25;

o) Società del Gruppo FS:

- FS S.p.A. e le società controllate direttamente e indirettamente da FS S.p.A. ai sensi dell'art. 2359 commi 1 e 2 Codice Civile (di seguito definite rispettivamente "FS" e "Società Controllate FS");

- Società collegate ossia soggette a influenza notevole di FS o di una delle Società Controllate FS ex art. 2359 comma 3 Codice Civile;

- Società di cui FS o una delle Società Controllate FS possiedono una partecipazione di minoranza nel capitale sociale.

La predetta nozione include anche le società di diritto estero per le quali ricorrano i medesimi presupposti partecipativi/di controllo di cui sopra;

p) Società emittente: FS Tech ovvero la Società del Gruppo FS espressamente autorizzata da FS Tech all'emissione dell'Ordine applicativo [**All.** (•)];

q) Soggetto Responsabile per la fase dell'Esecuzione o RFE: il soggetto Responsabile per la fase esecutiva dell'Accordo Quadro, di cui al successivo art. 26;

r) Termini di esecuzione: la data a decorrere dalla quale l'Appaltatore dovrà eseguire le prestazioni contrattuali, come indicato negli Ordini applicativi;

s) Unità Ordinante/i: gli uffici e/o le persone fisiche di FS Tech abilitati a emettere gli Ordini applicativi.

Articolo 2 – Premesse e Allegati

Le Premesse e gli Allegati costituiscono parte integrante e sostanziale del presente Accordo, anche al fine di meglio precisare le obbligazioni assunte dalla Parti.

Fanno parte del presente Accordo i seguenti allegati:

1. Dichiarazione ex art. 1341 c.c. dell'Appaltatore

2. Capitolato Tecnico
3. Offerta economica [ovvero: tecnica ed economica] presentata dall'Appaltatore
4. Garanzia definitiva
5. Dichiarazione sulla tracciabilità dei flussi finanziari
6. **[eventuale** *Chiarimenti di gara***]**
7. Polizza RC/Polizza Cyber
8. Copia quietanza pagamento imposta bollo

Articolo 3 – Disciplina applicabile

Per quanto non espressamente previsto nel presente Accordo Quadro, si applicheranno, le "*Condizioni Generali di Contratto per gli Appalti di forniture delle Società del Gruppo FS*", registrate presso l'Agenzia delle Entrate, Direzione Provinciale I di Roma, Ufficio Territoriale di Roma 1 Trastevere, al n. 5987, Serie 3, in data 23 giugno 2017, limitatamente alle disposizioni contenute nel Capo I; nel Capo II; negli artt. 43 e 44, nel Capo IV, Titolo II, Titolo III e Titolo IV; nel Capo V, consultabili nella sezione "Portale Acquisti di Gruppo - Le Regole del Gruppo" del sito https://eprocurement.gruppofs.it, che di seguito per brevità saranno chiamate "Condizioni Generali". Ogni richiamo a disposizioni del previgente D.Lgs. n. 50/2016 contenuto nelle Condizioni Generali dovrà intendersi riferito alle corrispondenti disposizioni del D.Lgs. n. 36/2023, per quanto applicabili agli appalti nei settori speciali.

Le Parti convengono che il termine "Fornitore" utilizzato nelle Condizioni Generali deve intendersi come equivalente a quello di Appaltatore utilizzato nel presente Accordo.

Resta fermo che, per tutto ciò che non sia stato espressamente previsto nel presente Contratto, le Parti rinviano alla disciplina dettata al riguardo dal codice civile, dal D.Lgs n. 36/2023 ove applicabile, e dalle altre norme vigenti in materia.

Si precisa che, laddove il Contratto dovesse prevedere il trattamento di dati personali, verrà predisposto uno specifico accordo di Data Protection sulla base di quelli che sono i template e le linee guida del Gruppo FS nel pieno rispetto della normativa applicabile in materia di dati personali, ivi incluso il Regolamento (UE) 2026/679 "GDPR" e successive modifiche e integrazioni nonché, più generalmente, la normativa di settore vigente.

La Parti altresì convengono che, ai fini della disciplina applicabile, l'ordine di prevalenza dei documenti è così definito:

1. Contratto;

2. Condizioni Generali di Contratto;

3. Eventuale Accordo di Data Protection (ADP).

Articolo 4 – Oggetto dell'Accordo Quadro

Il presente Accordo disciplina, ai sensi dell'art. 154 D.Lgs. 36/2023 e s.m.i., mediante condizioni generali pattuite in via preventiva, gli eventuali futuri Ordini

applicativi che saranno emessi nel corso di durata dell'Accordo medesimo, conformemente a quanto stabilito al successivo art. 9 tra l'Appaltatore e la Società emittente, per i servizi IaaS e PaaS in ambito Cloud e dei Servizi Specialistici di supporto tecnico-funzionale per la gestione, il monitoraggio e l'evoluzione delle infrastrutture digitali, gestita con sistemi telematici (di seguito per brevità "Servizio").

In particolare, i servizi oggetto del presente Accordo sono specificati nel Capitolato Tecnico (All. **[•]**).

[eventuale qualora sia previsto il Catalogo elettronico: *L'Appaltatore dovrà altresì provvedere alla creazione, gestione, aggiornamento e manutenzione del Catalogo elettronico sulla piattaforma Ariba***]**.

Il presente Accordo non costituisce alcun impegno della Società emittente ad acquistare, in tutto o in parte, il servizio oggetto dello stesso e, pertanto, l'Appaltatore non ha diritto ad avanzare pretese di alcun genere qualora non si proceda alla emissione di Ordini applicativi ovvero non si proceda all'emissione di Ordini applicativi sino all'esaurimento dell'importo massimo previsto nel presente Accordo.

Il presente Accordo non costituisce alcun vincolo di esclusiva in favore dell'Appaltatore.

Articolo 5 – Durata, Importo e Opzioni dell'Accordo Quadro

Il presente Accordo produrrà i suoi effetti a decorrere dalla data di ricezione, da parte del Committente, dell'accettazione della relativa proposta contrattuale, e avrà una durata di [•] [•] mesi.

Il periodo di [•] [•] mesi, entro il quale potranno essere emessi gli Ordini applicativi, inizierà a decorrere dalla data di perfezionamento dell'Accordo come sopra indicato**.**

L'importo massimo del presente Accordo è pari a *€ [•] IVA esclusa* **[in alternativa in caso di gara a Lotti prevedere**: per il Lotto (n. •) pari a € [•] IVA esclusa - per il Lotto (n. •) pari a € [•] IVA esclusa ecc.**].**

Restano fermi i termini previsti nei singoli Ordini applicativi, ancorché gli stessi dovessero avere scadenza oltre il termine di validità del presente Accordo Quadro.

L'Accordo potrà essere modificato durante il suo periodo di efficacia, senza una nuova procedura di affidamento, nel rispetto di quanto ivi stabilito e nei casi e alle condizioni previsti dal D.Lgs. n. 36/2023 e dalle Condizioni Generali, purché la sua struttura e l'operazione economica ad esso sottesa possano ritenersi inalterate.

Sono previste le seguenti opzioni:

[OPZIONE DI IMPORTO: *Ai sensi dell'art. 120, comma 1, lett. a), del D.Lgs. n. 36/2023 il Committente si riserva di modificare l'Accordo in corso di esecuzione e prima della sua scadenza naturale, con uno o più atti unilaterali, mediante la richiesta di ulteriori prestazioni analoghe a quelle oggetto del presente Accordo da erogare, agli stessi patti e alle medesime condizioni, per l'ulteriore importo di € [•] IVA esclusa* **[in alternativa in caso**

di gara a Lotti prevedere*: per il Lotto (n. •) per l'ulteriore importo di € [•] IVA esclusa - per il Lotto (n. •) per l'ulteriore importo di € [•] IVA esclusa,*]].

[OPZIONE DI PROROGA: *Ai sensi dell'art. 120, comma 10, del D.Lgs. n. 36/2023 Il Committente si riserva la facoltà di estendere - con uno o più atti unilaterali - la durata del presente Accordo, prima della scadenza della validità temporale dello stesso come sopra indicata, per un massimo di ulteriori [•]*[giorni/mesi/anni]*, agli stessi prezzi, patti e condizioni, [da inserire qualora la seguente previsione sia stata inserita nei documenti di gara/selezione: ovvero, previo accordo fra le Parti, alle più recenti condizioni di mercato ove più favorevoli per il Committente*]].

[ove si intenda prevedere il c.d. quinto d'obbligo, inserire la parte che segue: *Variazione fino a concorrenza del quinto dell'importo dell'Accordo Quadro**:** *Ai sensi dell'art. 120, comma 9, del D. Lgs. n. 36/2023, qualora in corso di esecuzione si renda necessario un aumento o una diminuzione delle prestazioni fino a concorrenza del quinto dell'importo contrattuale, il Committente potrà imporre all'Appaltatore l'esecuzione alle stesse condizioni previste nell'Accordo originario. In tal caso, l'Appaltatore non può fare valere il diritto alla risoluzione dell'Accordo.*].

Il Committente si riserva, inoltre, la facoltà di disporre una proroga del presente Accordo, agli stessi prezzi, patti e condizioni, al ricorrere delle condizioni previste dall'art. 120, comma 11, D.Lgs. n. 36/2023, e per il tempo strettamente necessario alla conclusione della procedura necessaria per l'individuazione di un nuovo contraente.

L'opzione [o Le opzioni] di cui sopra, qualora esercitata [o esercitate], sarà comunicata [o saranno comunicate] all'Appaltatore con posta elettronica certificata prima della scadenza del Contratto.

Con riferimento al valore complessivo dell'Accordo Quadro si precisa che, l'Appaltatore prende atto che non avrà nulla a che pretendere ad alcun titolo a fronte delle prestazioni non richieste, nel caso in cui al momento della scadenza dei termini suindicati, non sia stato consumato l'importo massimo dell'Accordo ovvero non siano state esercitate, in tutto o in parte, le opzioni sopra indicate e qualsiasi sia l'ammontare delle prestazioni sino al momento richieste.

Nessuna variazione alle prestazioni dovute potrà essere apportata su iniziativa dell'Appaltatore.

Articolo 6 - Modalità di esecuzione

Il servizio oggetto del presente Accordo dovrà essere eseguito in conformità alle prescrizioni contenute nel Capitolato Tecnico, **[eventuale se in gara era prevista l'offerta tecnica aggiungere anche:** *nell'offerta tecnica***]** e nei singoli Ordini applicativi.

[eventuale Articolo 8 – Catalogo Elettronico Ariba]

Il Committente si avvale di un sistema di e-Procurement basato su tecnologia SAP Ariba Cloud denominato Ariba per la gestione delle transazioni con i clienti, dei cataloghi on-line, dei prodotti, degli ordini di acquisto.

Attraverso un'unica piattaforma operatori autorizzati, di tutte le Società del Gruppo Ferrovie dello Stato Italiane, possono effettuare ordini on-line su un panel precostituito di cataloghi di prodotti e fornitori.

Ai fini della gestione del presente atto e della veicolazione dei relativi Ordini

applicativi attraverso la suddetta piattaforma, l'Appaltatore dovrà pertanto iscriversi ad Ariba Network (AN).

Per informazioni utili riguardo alla Piattaforma è possibile prendere visione delle FAQ del sito accedendo all'indirizzo internet: https://service.ariba.com/Supplier.aw/.

Per Ordini applicativi trasmessi tramite la Piattaforma Ariba il termine entro il quale la fornitura oggetto del presente atto dovrà essere consegnata decorre dal giorno lavorativo successivo alla data di ricezione dell'ordine nella Piattaforma stessa.

Ai fini di quanto sopra l'Appaltatore dovrà necessariamente e preventivamente dotarsi di uno dei sottostanti browser:

- Microsoft Edge 32-bit
- Chrome 54+ 64-bit
- Mozilla Firefox 49+ 64-bit
- Safari 9+ 64-bit
- Mozilla Firefox 17+
- Safari 5
- Mobile Safari on iPad (iOS 6 or above)
- Microsoft Edge Chromium 79+a 32 e 64 bit
- una linea per il collegamento ad Internet
- una casella di posta elettronica.

Entro 5 giorni lavorativi dalla data di stipula del presente atto, l'Appaltatore deve fornire, in versione definitiva alla struttura Sistemi e Automation per gli Acquisti di Ferservizi S.p.A., di Ferservizi S.p.A., il proprio catalogo in formato elettronico. L'Appaltatore è responsabile della creazione, gestione, aggiornamento e manutenzione del proprio catalogo e della completezza/correttezza delle informazioni in esso contenute.

Il Committente, in corso di vigenza contrattuale, può richiedere aggiornamenti del catalogo che l'Appaltatore dovrà apportare, secondo le modalità indicate, entro 7 giorni lavorativi dalla richiesta di modifica.

Articolo 9 – Emissione Ordini applicativi

Al presente Accordo sarà data esecuzione mediante l'emissione di Ordini applicativi.

[In caso di Catalogo Ariba: Gli Ordini applicativi saranno emessi dalla Società emittente ai termini ed alle condizioni contenuti nel presente Accordo.

Essi si intendono conclusi all'atto del loro ricevimento da parte dell'Appaltatore.

Gli Ordini applicativi saranno trasmessi all'Appaltatore mediante l'utilizzo del sistema di *e-Requisitioning*, in uso presso il Committente, come sopra riportato.

Eventuali Ordini applicativi inviati in modalità diversa dovranno essere preventivamente autorizzati dal RFE.]

[In alternativa qualora Non sia previsto Ariba

Gli Ordini applicativi potranno essere inviati in formato .pdf tramite email o PEC. Il RFE si riserva di indicare all'Appaltatore la modalità autorizzata di trasmissione degli Ordinativi.**]**

L'Appaltatore dovrà avere cura di controllare, in ogni caso, che l'ordinativo inoltrato attraverso email/PEC sia inviato anche "per conoscenza" al RFE.

Diversamente dovrà avere cura di informare entro 3 (tre) giorni lavorativi il RFE, e attendere un riscontro prima di dare esecuzione all'Ordine applicativo.

[In caso di Catalogo Ariba: Le richieste relative ad eventuali problemi di natura tecnica circa l'emissione degli Ordini applicativi potranno essere inoltrate dai richiedenti al seguente indirizzo e-mail: contactcenterferservizi@ferservizi.it.**]**

Negli Ordini applicativi saranno dettagliate le attività di volta in volta richieste, le modalità ed i tempi di esecuzione, il corrispettivo previsto nonché tutti gli altri dati necessari alla corretta esecuzione della prestazione.

La Società emittente è in facoltà, a suo insindacabile giudizio e senza necessità di motivazione, di recedere unilateralmente dall'Ordine applicativo, in qualsiasi momento, indipendentemente dallo stato di esecuzione dello stesso.

Il recesso ha effetto dalla data indicata e comunque non prima di 15 giorni dalla data di ricevimento da parte dell'Appaltatore della lettera raccomandata A/R o comunicazione PEC con la quale la Società emittente comunica di avvalersi di tale facoltà. È escluso il diritto dell'Appaltatore ad ogni eventuale pretesa, anche di natura risarcitoria, nonché ad ogni compenso indennizzo e/o rimborso, anche in deroga a quanto previsto dall'art. 1671 c.c..

Resta fermo il pagamento delle prestazioni già rese alla data del recesso.

Articolo 10 – Corrispettivi e Revisioni prezzi

I corrispettivi, IVA esclusa, pattuiti per quanto oggetto del presente Accordo, sono quelli di seguito riportati come risultanti dall' Offerta economica presentata dall'Appaltatore e allegata al presente Accordo [**All.** (•)]**.**

[**In caso di offerta con sconto/i percentuale/percentuali**: I corrispettivi, IVA esclusa, pattuiti per quanto oggetto del presente Accordo, sono quelli di seguito indicati derivanti dall'applicazione ai prezzi a base di gara dello sconto/i offerto/i dall'Appaltatore e riportato/i nella propria Offerta economica presentata dall'Appaltatore e allegata al presente Accordo All. (•)].

Di seguito si riporta quanto offerto dall'Appaltatore:

Descrizione del servizio	***Prezzo in € (IVA esclusa)***
[•]	**[•]**
[•]	**[•]**

[•]	**[•]**
[•]	**[•]**

Tutti i compensi si intendono comprensivi e compensativi di ogni eventuale onere, diretto ed indiretto, nessuno eccettuato, che l'Appaltatore dovrà sostenere per eseguire le prestazioni, 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.

Ai sensi dell'art. 60 e dell'Allegato II.2 bis del d.lgs. n. 36/2023, il corrispettivo dovuto all'Appaltatore a norma del presente articolo potrà essere oggetto di revisione nel rispetto di quanto di seguito previsto.

La revisione del corrispettivo, in aumento o in diminuzione, si attiverà al verificarsi di particolari condizioni di natura oggettiva che determineranno una variazione del costo del servizio/della fornitura, in aumento o in diminuzione, superiore al 5% dell'importo complessivo del contratto quale risultante dalla comunicazione di aggiudicazione/affidamento e opererà nella misura dell'80% del valore eccedente la variazione del 5% applicata alle prestazioni da eseguire.

Il valore iniziale di riferimento per il calcolo della variazione è quello dell'indice revisionale relativo al mese in cui ricade la comunicazione di aggiudicazione/affidamento (e cioè il mese di [____] dell'anno [____]) e la variazione è calcolata come differenza tra il valore dell'indice revisionale o del sistema ponderato di indici al momento della rilevazione e il corrispondente valore al mese di adozione dell'aggiudicazione. In caso di sospensione o proroga dei termini di aggiudicazione, il valore di riferimento è quello dell'indice revisionale relativo alla scadenza del termine massimo per l'aggiudicazione ex art. 1, co. 1 e 2, dell'Allegato I.3 del d.lgs. n. 36/2023.

Si procederà al calcolo utilizzando le pertinenti formule indicate all'Allegato II.2 bis e ai fini della determinazione della variazione, ai sensi dell'art. 60, comma 3, lett. b), del d.lgs. n. 36/2023 si farà riferimento _____ [indicare l'indice/gli indici tra quello/i riportato/i agli artt. 10, 11 e 13 dell'allegato II bis del Codice, tenendo conto delle regole ivi riportate per la relativa individuazione]

Il Responsabile della fase di esecuzione dell'Accordo Quadro monitorerà l'andamento dell'indice revisionale/degli indici revisionali, coerentemente con l'aggiornamento periodico del/dei medesimo/i indice/i revisionale/i.

Ove sussistano le condizioni per la revisione sopra richiamate, ne verrà data comunicazione all'Appaltatore.

Resta fermo che la revisione troverà applicazione limitatamente agli ordini applicativi ancora da emettere; per quanto riguarda gli ordini applicativi già emessi – ferma la non applicabilità della revisione nel caso di ordini che consistano in una prestazione ad esecuzione istantanea – l'eventuale monitoraggio delle variazioni in fase esecutiva, nonché l'eventuale riconoscimento di importi revisionali, è rimesso al Committente del singolo

ordine applicativo/Responsabile della fase di esecuzione del singolo ordine applicativo.

In caso di variazioni in aumento, si procederà alla liquidazione degli importi dovuti in occasione del primo pagamento utile successivo, compreso il periodo riferito alle prestazioni eventualmente già eseguite nel periodo intercorrente tra la data di rilevazione e la data del pagamento.

In caso di variazioni in diminuzione, l'importo da detrarre per le prestazioni già eseguite tra la data di rilevazione della variazione e la data di pagamento sarà trattenuto sul primo pagamento utile successivo. Qualora le suddette trattenute non fossero sufficienti, l'Appaltatore dovrà corrispondere l'importo residuo secondo le modalità prescritte dalla Società Emittente con apposita comunicazione.

Tutte le variazioni percentuali e di prezzo saranno arrotondate alla seconda cifra decimale. L'arrotondamento verrà operato in eccesso all'unità superiore qualora la terza cifra decimale sia pari o superiore a cinque.

Qualora l'Appaltatore/Fornitore esegua o consegni le prestazioni in ritardo, l'eventuale revisione opererà solo fino alla data di esecuzione/consegna contrattualmente prevista e non verranno riconosciuti eventuali maggiori oneri a titolo di revisione per il periodo corrispondente al ritardo.

Nel caso di esecuzione in anticipo rispetto ai termini contrattualmente stabiliti, l'accertamento degli eventuali maggiori oneri sopportati dall'Appaltatore dovrà essere effettuato con riferimento al momento in cui le prestazioni sono state eseguite/consegnate.

La revisione dei prezzi sarà applicata al prezzo contrattuale senza tenere conto delle eventuali revisioni riconosciute in precedenza.

Il Responsabile della fase di esecuzione dell'Accordo Quadro si riserva di richiedere l'integrazione della garanzia definitiva a fronte degli eventuali maggiori importi riconosciuti.

L'eventuale adeguamento in aumento verrà riconosciuto nei limiti di cui all'art. 60, comma 5, del d.lgs. n. 36/2023.

L'Appaltatore è in facoltà di presentare istanza motivata di rideterminazione dell'adeguamento (in aumento o in diminuzione) del corrispettivo qualora il provvedimento di revisione sia affetto da errori materiali, dandone adeguata dimostrazione. L'istanza di rideterminazione deve essere presentata, a pena di decadenza, entro trenta (30) giorni dalla data in cui l'Appaltatore ha ricevuto la comunicazione; ove, entro trenta (30) giorni dalla data di ricevimento l'istanza, essa non abbia avuto riscontro scritto, la stessa si intenderà respinta salva la facoltà dell'Appaltatore di iscrivere riserva. La presentazione dell'istanza di rideterminazione dell'adeguamento non costituisce giustificazione per la mancata o ritardata esecuzione delle prestazioni contrattuali.

Resta fermo che qualora l'applicazione della presente clausola di revisione non garantisca il principio di conservazione dell'equilibrio contrattuale e non sia

possibile garantire il medesimo principio mediante rinegoziazione secondo buona fede, è sempre fatta salva la possibilità di invocare la risoluzione per eccessiva onerosità sopravvenuta.

Articolo 10 bis – Anticipazione del prezzo

[Qualora l'anticipazione del prezzo non sia applicabile inserire la seguente formulazione: Al presente Accordo Quadro non si applica l'anticipazione del prezzo del 20% di cui all'art. 125, comma 1 del Codice, pertanto, non si darà luogo all'anticipazione del prezzo.**]**

[Qualora l'anticipazione del prezzo sia applicabile inserire la seguente formulazione: Ai sensi dell'art. 125, comma 1, del Codice, l'Appaltatore per ciascun Ordine Applicativo riceve, entro 15 giorni dall'effettivo inizio, (nel caso in cui l'anticipazione si applichi a tutte le prestazioni: della/e prestazione/i oggetto dell'Ordine Applicativo o in alternativa, nel caso in cui l'anticipazione si applichi solo ad una o più prestazioni: della/e seguente/i prestazione/i _____ oggetto dell'Ordine Applicativo (indicare espressamente le prestazioni cui si applica) un'anticipazione del prezzo pari al 20 per cento del valore dell'Ordine Applicativo stesso (o in alternativa nel caso si applichi solo ad alcune prestazioni: del valore della/e suddetta/e prestazione/i oggetto dell'Ordine Applicativo.)

[Nell'ipotesi in cui la durata dell'Ordine Applicativo sia superiore ad una annualità: L'anticipazione è calcolata sul valore delle prestazioni di ciascuna annualità contabile, stabilita nel cronoprogramma dei pagamenti, ed è corrisposta entro quindici giorni dall'effettivo inizio della prima prestazione utile relativa a ciascuna annualità, secondo il cronoprogramma delle prestazioni.]

L'erogazione dell'anticipazione è subordinata alla costituzione di una garanzia fideiussoria bancaria o assicurativa in favore della Società emittente, rilasciata dai soggetti indicati all'art. 106 comma 3 del Codice e con le modalità previste dal secondo periodo dello stesso comma, di importo pari all'anticipazione, maggiorato del tasso di interesse legale applicato al periodo necessario al recupero dell'anticipazione stessa secondo il cronoprogramma della prestazione (o altro documento equivalente, tipo SLA) indicato nel Capitolato.

L'importo della garanzia viene gradualmente ed automaticamente ridotto nel corso dello svolgimento della prestazione, in rapporto al progressivo recupero dell'anticipazione da parte della Società emittente.

L'Appaltatore decade dall'anticipazione, con obbligo di restituzione delle somme anticipate, se l'esecuzione della prestazione non procede, per ritardi a lui imputabili, secondo il cronoprogramma concordato. Sulle somme restituite sono dovuti alla Società emittente gli interessi legali con decorrenza dalla data di erogazione della anticipazione.

L'importo dell'anticipazione verrà recuperato dalla Società emittente nella misura del ____% della singola prestazione direttamente in fattura fino al raggiungimento dell'ammontare complessivo corrispondente all'importo anticipato di cui al primo capoverso.

L'Appaltatore si obbliga ad indicare nelle fatture l'importo totale delle prestazioni eseguite (pari all'importo dell'entrata merci) e in deduzione l'importo dell'anticipazione da recuperare.

[Eventuale: Articolo 10 ter – Clausola di mantenimento dell'equilibrio contrattuale

1. In caso di eventi straordinari e imprevedibili intervenuti in corso di esecuzione del presente Accordo (quali, a titolo esemplificativo e non esaustivo, guerre dichiarate o meno, ostilità militari, guerre civili, restrizioni monetarie e/o commerciali, embarghi, sanzioni, atti legittimi o illegittimi di autorità straniere o internazionali, pandemie, epidemie, calamità naturali), la Parte pregiudicata dagli stessi che non abbia volontariamente, mediante la sottoscrizione dell'Accordo, assunto i relativi rischi, può domandare all'altra Parte, la rinegoziazione secondo buona fede delle condizioni contrattuali ai sensi dell'art. 9 del D.lgs. n. 36/2023, al fine di ripristinare l'originario equilibrio dell'Accordo.
2. Resta fermo che, in conformità alla legge, la conservazione dell'equilibrio contrattuale è attuata applicando le previsioni dell'art. 10 in materia di revisione prezzi e dell'art. 5 in materia di modifiche dell'Accordo in corso di esecuzione. Ove non ricorrano i presupposti e le condizioni per l'applicazione di tali misure - ovvero le stesse risultino insufficienti a ristabilire l'originario equilibrio contrattuale - le Parti potranno procedere alla rinegoziazione delle condizioni contrattuali, nei limiti e con le modalità indicate nel presente articolo. In considerazione di quanto sopra, la rinegoziazione sarà ammessa, a titolo esemplificativo, nei seguenti casi:
    a. se gli eventi di cui al comma 1 determinano - a parità di prestazione - maggiori oneri indiretti durante la fase esecutiva;
    b. se gli eventi di cui al comma 1 determinano maggiori oneri diretti solo parzialmente rilevati dagli indici di variazione dei prezzi, perché non sono considerati nel paniere di riferimento, ovvero perché non sono adeguatamente rappresentati nel paniere rispetto alla loro effettiva incidenza sul costo complessivo dell'appalto.
3. É inammissibile la domanda di rinegoziazione promossa dall'Appaltatore la cui finalità sia quella di ristabilire l'equilibrio contrattuale rispetto ad un'offerta economica che, liberamente presentata in base a proprie valutazioni, si sia concretamente rivelata non sostenibile in seguito al verificarsi di eventi diversi da quelli di cui al precedente comma 1.
4. Non rappresentano sopravvenienze in grado di alterare in maniera rilevante l'originario equilibrio contrattuale gli eventi riconducibili alla normale alea, all'ordinaria fluttuazione economica e al rischio di mercato. In particolare, qualora la domanda di rinegoziazione sia promossa dall'Appaltatore, l'equilibrio contrattuale, ai soli fini dell'applicazione della presente clausola, non si considera alterato quando gli eventi straordinari e imprevedibili di cui al precedente comma 1 determinano un incremento degli oneri diretti e/o indiretti di esecuzione inferiore al 10% dell'importo aggiornato dell'appalto, al lordo delle variazione del corrispettivo per effetto delle modifiche contrattuali in corso di esecuzione e del riconoscimento di somme a titolo di revisione prezzi. Se gli eventi sopravvenuti elencati al comma 1

concorrono con altre cause, ai fini di cui al precedente periodo non si deve tener conto degli effetti di queste ultime sull'equilibrio contrattuale.

5. Se la rinegoziazione ha ad oggetto il riconoscimento di un maggior corrispettivo, questo può essere accordato solo per un importo pari all'ammontare dei maggiori oneri diretti e/o indiretti che eccede la percentuale di cui al precedente comma 4 ed esclusivamente nei limiti delle somme a disposizione indicate nel quadro economico dell'intervento alle voci imprevisti e accantonamenti, nonché delle economie risultanti da ribasso d'asta, nella misura risultante al momento della proposizione dell'istanza di rinegoziazione.

6. La domanda di rinegoziazione deve indicare gli specifici presupposti del disequilibrio e contenere, altresì, tutta la documentazione atta a dimostrare (i) lo scostamento percentuale in misura superiore a quella indicata al precedente comma 4 e (ii) e le cause che lo hanno determinato.

7. La domanda di rinegoziazione non sospende l'esecuzione dell'Accordo e deve essere inviata dalla Parte richiedente all'altra Parte a mezzo PEC, senza ritardo rispetto all'evento che ha alterato l'equilibrio contrattuale. Pertanto, la proposizione dell'istanza non può mai legittimare l'interruzione o la sospensione delle prestazioni contrattuali.

8. Valutata l'istanza di rinegoziazione, entro […] giorni dal suo ricevimento, la Parte destinataria della richiesta comunica all'altra Parte la sussistenza o meno dei presupposti per dar seguito alla rinegoziazione, comunque nei limiti economici di cui al precedente comma 5. Il mancato raggiungimento di un accordo sulle condizioni di riequilibrio, sia nel caso in cui la Parte destinataria dell'istanza di rinegoziazione non intenda darvi seguito, che nel caso in cui le Parti non addivengano a un accordo entro il termine di […] dal ricevimento dell'istanza, non legittima in alcun caso l'interruzione o la sospensione dell'esecuzione contrattuale. Per qualunque ipotesi di mancato accordo, restano nella disponibilità delle Parti i rimedi ordinariamente previsti dal presente Accordo, dalle C.G.C. applicabili, dal D. Lgs. n. 36/2023 per quanto applicabile al presente Contratto, nonché dall'art. 1467 e dalle altre norme del Codice civile, ad eccezione di quelle non applicabili in base alla legge o alle disposizioni contrattuali.

9. In caso di raggiungimento di un accordo, le nuove condizioni di equilibrio contrattuale vengono formalizzate dalle Parti nel contesto di un Atto Integrativo e Modificativo. In dipendenza delle sopravvenienze elencate nel precedente comma 1, l'accordo eventualmente raggiunto tra le Parti sulla rinegoziazione delle condizioni contrattuali deve comprendere, quale espressione del principio di buona fede, anche l'integrale rinuncia dell'Appaltatore alle eventuali riserve iscritte in corso di esecuzione. In mancanza di tale rinuncia, l'accordo sulla rinegoziazione non potrà ritenersi raggiunto.

10. Il quinto dell'importo dell'Accordo di cui all'art. 120, comma 9, del D. Lgs. n. 36/2023 è calcolato sull'importo contrattuale comprensivo delle eventuali maggiori somme riconosciute a titolo di rinegoziazione. Le maggiori somme riconosciute a titolo di rinegoziazione, tuttavia, non concorrono al raggiungimento del limite del quinto dell'importo contrattuale, entro il quale

la Stazione Appaltante può imporre all'Appaltatore l'esecuzione di modifiche e varianti alle condizioni originariamente previste in Accordo.

11. La rinegoziazione deve essere condotta dalle Parti secondo i principi di correttezza e buona fede e deve concludersi entro il termine di […] giorni di cui al precedente comma 7, prorogabile per una sola volta ad opera della Parte destinataria dell'istanza per un corrispondente periodo di tempo.
12. Per tutto quanto non espressamente previsto dal presente articolo, si rinvia all'art. 9 del D. Lgs. n. 36/2023 e s.m.i..**]**

Articolo 11 – Fatturazione e modalità di pagamento

Fermo restando quanto previsto all'art 11, comma 6, D.Lgs. 36/2023, i pagamenti saranno effettuati a 60 (sessanta) giorni dalla data di ricezione della fattura.

La fattura dovrà essere trasmessa con evidenza degli estremi del documento "Entrata Merci" e "Ordine applicativo" relativo attestante l'avvenuta esecuzione delle prestazioni e dovrà - ove prevista per legge - riportare la seguente annotazione: "operazione con scissione di pagamenti ex art. 17 ter DPR 633/72".

Il Documento di "Entrata Merci" o documento equivalente (Ordine di Acquisto) viene inviato a valere come verifica di ogni singola prestazione richiesta e correttamente erogata e quale verifica di conformità ai sensi dell'art. 116 del Codice.

A partire dal 1° gennaio 2019, è previsto l'obbligo di fatturazione elettronica per tutte le cessioni di beni e le prestazioni di servizi effettuate tra soggetti residenti, stabiliti o identificati nel territorio dello Stato Italiano (cfr. l'articolo 1, comma 916 e 917 della legge n. 205 del 27 dicembre 2017 cosiddetta Legge di Bilancio 2018).

Per quanto sopra, in ottemperanza agli obblighi soprarichiamati, Ferservizi SpA Società del Gruppo FS in qualità di mandataria per il Service Amministrativo, dovrà ricevere le fatture emesse dovranno essere trasmesse esclusivamente in formato elettronico attraverso il Sistema di Interscambio (SdI).

Le fatture elettroniche in formato XML dovranno riportare il Codice Destinatario "RYRNP0U" (si precisa che il penultimo carattere è uno zero) per le seguenti Società (per le quali Ferservizi SpA, Società del Gruppo FS, effettua in qualità di mandataria il Service Amministrativo):

Oltre al Codice Destinatario, le fatture elettroniche in formato XML dovranno essere alimentate nei seguenti ulteriori campi:

- 1.1.3. valorizzato con "FPR12";
- 2.1.2.2. IdDocumento: valorizzato con il numero dell'Ordine di Acquisto comunicato dalla Stazione Appaltante;
- 2.2.1.16.1. TipoDato: valorizzato con "EM"
- 2.2.1.16.2. RiferimentoTesto: valorizzato con il codice fornito dal Committente.

N.B.: nel caso di fattura elettronica riferita a più Entrate Merci aggiungere nel

campo Tipo Dato i valori da 1 a n in funzione del numero delle Entrate Merci (per esempio EM1, EM2, EM3 ecc.).

Per maggior dettaglio si riporta di seguito un esempio di compilazione dei campi relativi all'Entrata Merci nel caso di una fattura di vendita (p.es. la nr. 913 del 20/12/2018) emessa a fronte di 12 Entrate Merci come di seguito indicato: 7005295448, 7005295449, 7005295450, 7005295461, 7005295462, 7005295463, 7005295464, 7005295465, 7005295466, 7005295467, 7005295468, 7005295469. La compilazione dei campi 2.2.1.16.1. TipoDato e 2.2.1.16.2. RiferimentoTesto dovrà essere effettuata nel seguente modo:

<TipoDato>EM1</TipoDato> 7005295448

<TipoDato>EM2</TipoDato> 7005295449

<TipoDato>EM3</TipoDato> 7005295450

[…..]

<TipoDato>EM12</TipoDato> 7005295469

In caso di fornitura di beni consegnati con documenti di trasporto, è necessario indicare:

- 2.1.8.1 NumeroDDT valorizzato con il numero del Documento di Trasporto
- 2.1.8.2 DataDDT valorizzato con la Data del Documento di Trasporto.

Tutte le fatture dovranno essere intestate a:

Ragione sociale della Società Cliente: FSTechnology S.p.A.

Sede legale: Roma, Piazza della Croce Rossa 1

Cod. fiscale e P.IVA: 15032391003

CdC: [.]

Tutte le fatture ricevute nel formato sopra rappresentato saranno conservate in conformità alla vigente normativa.

In termini generali, per consentire le attività di verifica delle fatture e di pagamento entro i termini previsti contrattualmente, si evidenziano le seguenti principali regole:

- indicare sempre nella fattura XML il Codice Fornitore, il numero dell'Ordine di Acquisto e, ove presenti, gli estremi del Documento di trasporto, CUP e CIG;
- indicare sui documenti di rettifica (note debito/credito) il riferimento della fattura di origine;
- emettere sempre una fattura separata per ogni Ordine di Acquisto ricevuto.**]**

L'Appaltatore chiede che i pagamenti siano effettuati con la modalità sottoindicata, con esplicita dichiarazione che l'adempimento della modalità prescelta costituisce valore di quietanza, facendo salvo il Committente e/o la Società emittente da ogni responsabilità conseguente:

bonifico su Conto Corrente Bancario IBAN n. [.] tenuto presso [.] intestato a [.].

Articolo 12 – Tracciabilità dei flussi finanziari

I pagamenti saranno effettuati unicamente a mezzo bonifico bancario e/o postale, ovvero con altri strumenti di incasso o di pagamento idonei a consentire la piena tracciabilità delle operazioni, sul conto corrente dedicato ovvero sui conti correnti dedicati già oggetto di comunicazione da parte dell'Appaltatore ai sensi dell'art. 3, comma 7, della Legge 13 agosto 2010 n. 136 [All. •] con salvezza del Committente e della Società emittente da ogni responsabilità conseguente.

Il bonifico ovvero gli altri strumenti di pagamento di cui sopra riporteranno il Codice Identificativo di Gara (**CIG**) attribuito dall'ANAC.

L'Appaltatore assume, pertanto, espressamente tutti gli obblighi di tracciabilità dei flussi finanziari stabiliti a proprio carico dall'art. 3 della Legge 13 agosto 2010 n. 136 e dalle disposizioni interpretative, attuative e modificative di cui agli artt. 6 e 7 del Decreto Legge 12 novembre 2010 n. 187.

L'Appaltatore ha l'obbligo di inserire, nei contratti sottoscritti con i subappaltatori e i subcontraenti della filiera delle imprese a qualsiasi titolo interessate all'esecuzione dell'appalto, a pena di nullità assoluta, apposita clausola, con la quale ciascuno di essi assume gli obblighi di tracciabilità dei flussi finanziari di cui alla suddetta legge. Il Committente verificherà l'inserimento di tale clausola nei suddetti contratti. A tal fine, l'Appaltatore è obbligato a trasmettere al Committente copia dei subcontratti.

L'Appaltatore si impegna altresì a dare immediata comunicazione al Committente ed alla prefettura-ufficio territoriale del Governo della provincia competente della notizia dell'inadempimento della propria controparte (subappaltatore/subcontraente) agli obblighi di tracciabilità finanziaria.

Il mancato utilizzo del bonifico bancario o postale, ovvero degli altri strumenti idonei a consentire la piena tracciabilità delle operazioni, costituisce causa di risoluzione dell'Accordo/Ordini applicativi.

Articolo 13 – Obblighi particolari dell'Appaltatore

L'Appaltatore si obbliga, nello svolgimento delle prestazioni, ad adeguare i propri strumenti di ricezione degli Ordini applicativi predisponendo mail-box specifiche, abilitate a ricevere dai sistemi di *e-Procurement* installati presso il Committente e la Società emittente, in funzione del numero delle transazioni ricevute dalla Società emittente e della modalità di trasmissione utilizzata, con l'obiettivo di garantire la massima sicurezza e rapidità di evasione degli stessi.

L'Appaltatore provvederà ad archiviare, secondo le modalità più opportune, copia degli Ordini applicativi per il periodo minimo previsto dagli obblighi di legge.

L'Appaltatore dovrà verificare la completezza, la correttezza e la chiarezza degli Ordini applicativi ricevuti. In mancanza di uno dei predetti requisiti, sarà onere dell'Appaltatore contattare l'Unità Ordinante e chiedere l'invio di un nuovo Ordine applicativo opportunamente corretto.

L'Appaltatore si obbliga, nell'esecuzione delle prestazioni oggetto del presente Accordo, che saranno commissionate con gli Ordini applicativi ad eseguirle a regola d'arte e nel rispetto di tutte le norme di legge e di tutte le disposizioni, anche amministrative, vigenti o entrate in vigore durante l'esecuzione

dell'Accordo, nonché nel rispetto delle *best practices* di settore.

Per l'esecuzione del Servizio l'Appaltatore è tenuto a prestare - assumendone i relativi rischi - un'idonea organizzazione d'impresa avente una capacità prestazionale comunque efficacemente dimensionata a far fronte, con esattezza e regolarità, alle prestazioni affidate, nel rispetto dei risultati e requisiti, anche in materia di qualità, richiesti dal presente Accordo e relativi allegati.

L'Appaltatore è obbligato a mantenere ed adeguare in qualsiasi momento alle effettive esigenze e caratteristiche del servizio affidato la propria organizzazione produttiva, disponendo l'impiego di tutti i fattori produttivi necessari a far fronte agli obblighi di cui al presente Accordo, senza che l'eventuale maggior impiego di mezzi produttivi rispetto alle proprie stime, previsioni o dichiarazioni effettuate o rese all'atto dell'offerta possa costituire motivo di esonero dagli obblighi contrattualmente assunti, ovvero fondamento per richieste di maggiori compensi, indennizzi o risarcimenti.

L'Appaltatore riconosce che il Servizio è elemento essenziale per l'immagine delle Società del Gruppo FS e si impegna ad espletarlo con modalità organizzative, tecniche e di controllo, le più idonee per l'ottenimento del risultato richiesto, intendendosi impegnato a porre in essere tutti quegli interventi, procedure e modalità o attività che, pur se non specificati nel presente Accordo e relativi allegati, si rendessero necessari per garantire il livello quantitativo e qualitativo dei servizi.

Resta di competenza esclusiva dell'Appaltatore l'esercizio del potere organizzativo e direttivo nei confronti dei lavoratori utilizzati nel Servizio. L'Appaltatore stesso individuerà, prima dell'inizio delle attività contrattuali, il Responsabile dell'Accordo Quadro dell'Appaltatore; il personale dell'Appaltatore nonché di eventuali subappaltatori eseguirà esclusivamente gli ordini e le disposizioni impartiti da detto Responsabile e/o da altri soggetti dallo stesso delegati, e comunque individuati dall'Appaltatore medesimo.

L'Appaltatore si obbliga, altresì, a garantire la sicurezza del sistema informatico utilizzato per l'esecuzione delle prestazioni oggetto del presente Accordo, ivi comprese le relative attività di trasmissione, ricezione, conservazione e condivisione telematica di tutta la documentazione, concernente l'oggetto del presente Accordo.
A tal fine si obbliga a:

a) rispettare i seguenti controlli essenziali di sicurezza informatica:
    1. nominare un referente che sia responsabile per il coordinamento delle attività di gestione e di protezione delle informazioni e dei sistemi informatici;
    2. che siano identificate e rispettate le leggi e/o i regolamenti con rilevanza in tema di cyber-security che risultino applicabili per l'azienda;
    3. che tutti dispositivi che lo consentono siano dotati di software di protezione (antivirus, anti-malware, etc. …) regolarmente aggiornato;
    4. che le password siano diverse per ogni account, dalla complessità adeguata e con procedure di blocco automatico a seguito di reiterati tentativi. Viene valutato, inoltre, l'utilizzo dei sistemi di

autenticazione più sicuri offerti dal provider del servizio (es. autenticazione a due fattori);

5. che il personale autorizzato all'accesso, remoto o locale, ai servizi informatici disponga di utenze personali non condivise con altri; l'accesso sia opportunamente protetto; i vecchi account non più utilizzato siano disattivati;
6. che il personale sia adeguatamente sensibilizzato e formato sui rischi di cyber-security e sulle pratiche da adottare per l'impiego sicuro degli strumenti aziendali (es. riconoscere allegati e-mail, utilizzare solo software autorizzato, bloccare il dispositivo in caso di non utilizzo, ecc.);
7. che la configurazione iniziale di tutti i sistemi e dispositivi sia svolta da personale esperto, responsabile per la configurazione sicura degli stessi;
8. che in caso di utilizzo di applicazioni web con accesso da rete pubblica, o di gestione remota dei server e dei dispositivi di rete, siano utilizzati protocolli di rete cifrati (es. SSH, SSL);
9. che siano eseguiti periodicamente back up delle informazioni e dei dati. I backup siano conservati in modo sicuro e verificati periodicamente. I dati inoltre dovranno essere resi tempestivamente disponibili ove richiesti;
10. che le reti e i sistemi siano protetti da accessi non autorizzati attraverso strumenti specifici (es. Firewall e altri dispositivi/software anti-intrusione);
11. che tutti i software in uso (inclusi i firmware) siano aggiornati all'ultima versione consigliata dal produttore;

b) L'Appaltatore si obbliga a segnalare con la massima tempestività al Committente qualunque violazione o potenziale violazione della sicurezza informatica che possa avere un impatto sulle informazioni, sui sistemi e/o sulle infrastrutture del Committente contattando il Cyber-Security Operation Center (C-SOC) di Gruppo ai numeri 0644106332; 0644102620 ; 0644103052, ovvero scrivendo all'indirizzo mail securityincident@fsitaliane.it.
L'Appaltatore deve cooperare con il Committente per la gestione dell'eventuale incidente informatico e adottare misure adeguate a proprie spese per contenere e mitigarne gli effetti e prevenirne il ripetersi.

c) L'Appaltatore si obbliga, inoltre, a consentire l'accesso del personale incaricato dal Committente per la verifica delle misure minime di sicurezza informatica di cui al presente articolo, nel rispetto delle normative in materia di trattamento dei dati personali e di sicurezza cibernetica.effettuare un back-up della documentazione informatica di cui sopra su un sistema offline al fine di evitare, quantomeno, la perdita degli atti e, in caso di adempimenti con scadenza imposta da contratto o norma di legge, a produrre la documentazione secondo una tempistica che consenta il rispetto dei termini di legge e di contratto, anche in caso di attacco informatico;

d) L'Appaltatore può accedere ai sistemi informatici del Committente solo previa autorizzazione esplicita del Committente, impegnandosi - anche per il proprio personale, i propri eventuali subappaltatori ed eventuali

terzi che tratteranno, elaboreranno o accederanno alle informazioni del Committente durante l'esecuzione del Contratto - a rispettare le istruzioni di accesso fornite dal Committente. Pertanto, l'Appaltatore rimane pienamente e direttamente responsabile nei confronti del Committente di qualsiasi violazione degli obblighi di cui al presente articolo da parte del proprio personale, di eventuali subappaltatori e di terzi coinvolti nell'esecuzione del Contratto.

e) L'Appaltatore si impegna, inoltre, ad utilizzare gli strumenti, i servizi e le infrastrutture eventualmente messi a disposizione dal Committente per garantire la sicurezza delle informazioni. In ogni caso, il ricorso agli strumenti, ai servizi e alle infrastrutture messi a disposizione dal Committente non esonera l'Appaltatore dal garantire l'implementazione e la corretta adozione di misure di sicurezza interne. Nel caso vi siano impianti di fornitura relativi a circolazione ferroviaria, o afferenti ad ambiti prettamente industriali dove insistono sistemi informativi di natura Operational Technology l'Appaltatore si impegna ad adeguare le proprie metodologie operative e procedure alle raccomandazioni di standard internazionali riconosciuti nel settore della Sicurezza delle Informazioni in ambito OT.

f) L'Appaltatore garantisce la sicurezza del sistema informatico utilizzato per l'esecuzione delle prestazioni oggetto del Contratto, ivi comprese le relative attività di trasmissione, ricezione, conservazione e condivisione telematica di tutta la documentazione concernente l'oggetto del Contratto.

   A tal fine, si impegna a rispettare:

   1. le misure di sicurezza stabilite all'allegato B del Decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81, di cui all'articolo 1, comma 2, lettera b), del Decreto-Legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla Legge 18 novembre 2019, n. 133;
   2. le misure di sicurezza di base previste negli Allegati 1 e 2 della Determinazione dell'Agenzia per la Cybersicurezza Nazionale n. 164179 del 14 aprile 2025, attuativa del Decreto Legislativo 4 settembre 2024, n. 138 (cd. "Decreto NIS");
   3. gli elementi essenziali di cybersicurezza dei beni e dei servizi informatici di cui all'Allegato 1 del Decreto del Presidente del Consiglio dei Ministri 30 aprile 2025, attuativo della Legge 28 giugno 2024, n. 90.

   A tal fine, l'Appaltatore si impegna ad implementare e mantenere misure tecniche, operative e organizzative adeguate e proporzionate a garantire la massima sicurezza delle informazioni digitali gestite e trattate per l'esecuzione del Contratto. Tali misure comprendono, ma non sono limitate a: protezioni contro distruzioni, perdite, danni, alterazioni,

divulgazioni, accessi non autorizzati, violazioni della sicurezza e altre minacce informatiche.

Pertanto, fermi gli eventuali ulteriori obblighi previsti nel Contratto, l'Appaltatore si obbliga a conformarsi alle seguenti misure di sicurezza:

GOVERN

- designare e mantenere responsabili, adeguatamente formati e preparati, incaricati di gestire i sistemi informatici e rispondere prontamente a errori, incidenti o violazioni della sicurezza delle informazioni nell'ambito dell'esecuzione del Contratto;
- rispettare la normativa vigente e sopravvenuta in materia di cybersecurity, incluse le disposizioni attuative, le modifiche e integrazioni successive, nonché qualsiasi altra normativa pertinente, adeguando le proprie metodologie operative e procedure alle raccomandazioni di standard internazionali riconosciuti nel settore della sicurezza delle informazioni, per l'intera durata del Contratto;
- garantire l'attuazione di programmi di formazione dei propri dipendenti, con cadenza almeno annuale, sulle materie della cybersecurity e della data protection;
- adottare politiche di analisi dei rischi e di sicurezza dei sistemi informatici nonché strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza, che includano attività di trattamento del rischio cyber nonché aggiornarle e revisionarle periodicamente;
- mantenere un elenco aggiornato dei sistemi informativi e di rete rilevanti;
- adottare misure volte a garantire la sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra il Committente e i suoi diretti fornitori o fornitori di servizi;
- adottare processi di gestione del rischio di cybersecurity della catena di approvvigionamento;
- mantenere un inventario aggiornato dei fornitori, le cui forniture hanno un potenziale impatto sulla sicurezza dei sistemi informativi e di rete;
- formalizzare la valutazione del rischio per ogni fornitura con potenziali impatti sulla sicurezza dei sistemi informativi e di rete, con la definizione di requisiti di sicurezza sulla fornitura coerenti con le misure di sicurezza applicate ai sistemi informativi e di rete ed inserire tali requisiti nelle richieste di offerta, bandi di gara, contratti, accordi e convenzioni relativi a tali forniture;
- adottare inventari completi e aggiornati degli asset (ad esempio, dati, hardware, software, sistemi, infrastrutture, servizi informatici anche erogati dai fornitori, persone).

IDENTIFY

- identificare e documentare le vulnerabilità e i componenti contenuti nel bene o servizio informatico, e redigere una distinta base del software in un formato di uso comune e leggibile da un dispositivo automatico, che includa almeno le dipendenze di primo livello del bene o servizio;
- condurre regolari security assessment per identificare, mitigare e notificare tempestivamente eventuali vulnerabilità riscontrate.

PROTECT

- adottare misure di protezione e sicurezza dei dati e delle informazioni adeguate rispetto al rischio derivante dalle attività erogate nei confronti del Committente (a titolo esemplificativo: utilizzo di protocolli di rete cifrati, antivirus, antimalware, software anti-intrusione e firewall, tutti regolarmente aggiornati);
- adottare misure di sicurezza per la gestione delle identità, per l'autenticazione multifattoriale e per il controllo degli accessi;
- garantire sistemi di aggiornamento e manutenzione delle reti, dei sistemi e dei servizi utilizzati per le attività erogate nei confronti del Committente;
- implementare politiche e procedure relative all'uso della crittografia e della cifratura;
- adottare procedure per la generazione, conservazione sicura e consultazione centralizzata dei log (PR.PS-04), in particolare quelli relativi ad accessi remoti e privilegiati, definendo tempi di conservazione in base alla valutazione del rischio;
- adottare pratiche di sviluppo sicuro del software e gestione dell'intero ciclo di vita del software, garantendo la sicurezza durante l'acquisizione, lo sviluppo e la manutenzione dei sistemi informatici e di rete (Secure Software Development Lifecycle);
- fornire, sulla base della valutazione del rischio cyber, beni e i servizi informatici senza vulnerabilità sfruttabili note e con la garanzia che tali vulnerabilità possano essere trattate mediante aggiornamenti di sicurezza, anche, se del caso, mediante aggiornamenti di sicurezza automatici installati entro e per un periodo di tempo adeguato, abilitato come impostazione predefinita, con un meccanismo di disattivazione chiaro e di facile utilizzo, attraverso la notifica agli utilizzatori degli aggiornamenti disponibili e la possibilità di rinviarli temporaneamente;
- fornire, sulla base della valutazione del rischio cyber, beni e i servizi informatici con una configurazione sicura per impostazione predefinita, garantendo la possibilità di ripristinarli allo stato iniziale;
- garantire che i beni e servizi informatici forniti, trattino solo dati, personali o di altro tipo, adeguati, pertinenti e limitati a quanto necessario in relazione alla finalità prevista («minimizzazione dei dati»);

- garantire che i beni e servizi informatici forniti, siano progettati, sviluppati, prodotti e forniti per limitare le superfici di attacco, comprese le interfacce esterne e che riducano al minimo il loro impatto negativo sulla disponibilità dei servizi forniti da altri dispositivi o reti;
- garantire che i beni e servizi informatici forniti offrano agli utenti la possibilità di rimuovere in modo sicuro e agevole, su base permanente, tutti i dati e le impostazioni. Qualora tali dati possano essere trasferiti ad altri beni o servizi informatici, assicurare che tale trasferimento avvenga in modo sicuro;
- adottare meccanismi per garantire che, qualora disponibili, siano diffusi tempestivamente e gratuitamente, aggiornamenti di sicurezza al fine di risolvere i problemi di sicurezza individuati, accompagnati da messaggi di avviso che forniscano agli utilizzatori le informazioni pertinenti, comprese le potenziali misure da adottare;
- correggere tempestivamente le vulnerabilità, anche fornendo aggiornamenti di sicurezza; ove tecnicamente fattibile, fornire separatamente nuovi aggiornamenti di sicurezza separatamente dagli aggiornamenti della funzionalità;
- adottare meccanismi per distribuire in modo sicuro gli aggiornamenti dei beni e servizi informatici al fine di garantire che le vulnerabilità siano corrette o mitigate in modo tempestivo e, ove applicabile per gli aggiornamenti di sicurezza, in modo automatico;

DETECT

- utilizzare sistemi di monitoraggio e rilevamento delle anomalie e violazioni della sicurezza, oltre che processi per la comunicazione delle stesse al Committente come per legge;

RESPOND

g) definire, documentare e aggiornare un piano per la gestione degli incidenti di sicurezza informatica, che includa le fasi di rilevazione, contenimento, analisi, risoluzione e notifica al CSIRT Italia, nonché l'individuazione dei ruoli e delle responsabilità coinvolti e la predisposizione della relativa reportistica;

h) definire e documentare, se ritenuto opportuno e qualora intimato dall'ACN, procedure per garantire la tempestiva comunicazione degli incidenti di sicurezza informatica ai destinatari dei propri servizi che siano potenzialmente interessati da una minaccia informatica significativa, fornendo anche informazioni sulle misure o azioni correttive o di mitigazione adottabili e sulla natura della minaccia rilevata;

i) una volta reso disponibile un aggiornamento di sicurezza, condividere e divulgare agli utilizzatori delle informazioni sulle vulnerabilità risolte, comprendenti una descrizione delle vulnerabilità, informazioni che consentano agli utilizzatori di identificare il bene o servizio informatico

interessato, l'impatto delle vulnerabilità, la loro gravità e informazioni chiare e accessibili che aiutino gli utilizzatori a correggere le vulnerabilità; in casi debitamente giustificati, qualora ritenuto che i rischi di sicurezza legati alla divulgazione siano superiori ai benefici in termini di sicurezza, è possibile ritardare la divulgazione di informazioni su una vulnerabilità risolta fino a quando gli utilizzatori non abbiano avuto la possibilità di applicare la pertinente patch, in coerenza con quanto previsto dall'art. 16 del decreto legislativo 4 settembre 2024, n. 138;

j) adottare misure per facilitare la condivisione di informazioni sulle potenziali vulnerabilità del bene o servizio informatico e dei componenti di terzi ivi contenuti, fornendo anche un indirizzo di contatto per la segnalazione delle vulnerabilità individuate;

RECOVER

k) adottare misure volte a garantire la continuità operativa, come la gestione del backup e il ripristino in caso di disastro e a proteggere la disponibilità delle funzioni essenziali e di base, anche dopo un incidente, anche attraverso misure di resilienza e di mitigazione anche contro gli attacchi di negazione del servizio (denial of service);

Con riferimento al Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale (AI ACT), l'Appaltatore dichiara e garantisce che non vi sono sistemi di intelligenza artificiali implementati sulla fornitura oggetto del presente Contratto.

[FORMULAZIONE ALTERNATIVA IN CASO DI UTILIZZO DELL'AI

Con riferimento al Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale (AI ACT), l'Appaltatore dichiara e garantisce che i sistemi di intelligenza artificiali implementati sulla fornitura oggetto del presente Contratto sono conformi:

i. a quanto previsto dal Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale (AI ACT) e non integrano alcuna delle pratiche di intelligenza artificiale vietate dagli articoli 3 e 5 di tale Regolamento;

ii. a quanto previsto dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GDPR), qualora i richiamati sistemi di intelligenza artificiale dovessero comportare il trattamento.**]**

L'Appaltatore si impegna a compilare il questionario per la valutazione delle proprie performance di sostenibilità, disponibile su una piattaforma informatica

dedicata raggiungibile al link https://esgrating.gruppofs.it, entro 15 (quindici) giorni dalla data di sottoscrizione dell'Accordo Quadro (qualora non avesse già provveduto) e ad aggiornarlo annualmente sino alla scadenza dell'Accordo Quadro stesso. La Metodologia applicata e i questionari sono visionabili sul Portale Acquisti di Gruppo raggiungibile al link https://eprocurement.gruppofs.it.

N.B.: Ai sensi dell'art. 57 del D. lgs. n. 36/2023 e s.m.i., qualora per lo specifico appalto trovino applicazione Criteri Ambientali Minimi (cd. "CAM") indicare le clausole contrattuali previste per la relativa categoria merceologica nell'ambito dello specifico decreto emanato dal Ministero dell'Ambiente e della Sicurezza Energetica. Si riporta il link dove verificare in tempo reale, i CAM in vigore https://gpp.mase.gov.it/CAM-vigenti: *Per l'espletamento delle prestazioni oggetto del presente Accordo Quadro, l'appaltatore si obbliga a rispettare* _____.**]**

In caso di inadempimento parziale o integrale anche di uno soltanto degli obblighi sopra elencati, il Committente avrà la facoltà di risolvere il presente Accordo e/o i singoli Ordini applicativi ai sensi dell'art. 1456 c.c. e, indipendentemente dall'esercizio di tale facoltà, avrà diritto all'integrale risarcimento dei danni subiti in conseguenza all'inadempimento dell'Appaltatore.

[se del caso: *L'appaltatore si obbliga, infine, al rispetto dei seguenti obblighi in materia di:*

- **(da inserire laddove sia stato previsto nella documentazione della procedura di selezione: *Promozione dell'occupazione giovanile e femminile:*** *l'Appaltatore si impegna, altresì, ad assicurare una quota pari almeno al __%* (inserire la quota stabilita nella documentazione della procedura di selezione) *delle assunzioni necessarie per l'esecuzione dell'Accordo Quadro o per la realizzazione di attività a esso connesse o strumentali, sia all'occupazione giovanile sia all'occupazione femminile. A tal fine, l'Appaltatore dovrà produrre, 6 mesi prima della scadenza dell'ultimo Ordine applicativo, apposita dichiarazione, con l'eventuale documentazione a supporto, contenente le informazioni relative alle eventuali assunzioni effettuate durante il periodo di vigenza dell'Accordo Quadro con indicazione del numero di persone assunte e relativa indicazione di età e genere o le eventuali motivazioni che non hanno reso possibile l'adempimento dei suddetti impegni così come assunti.***)**
- **(da inserire laddove sia stato previsto nella documentazione della procedura di selezione*: Relazione di genere sulla situazione del personale maschile e femminile:*** *l'Appaltatore,* (nel caso di RTI o Consorzi aggiungere: *in relazione a ciascuna impresa e/o consorziata*), *che occupa un numero pari o superiore a quindici dipendenti e che non rientra nella classificazione di cui all'art. 46 comma 1 del d.lgs. n. 198/2006, è tenuto a consegnare al Committente, entro sei mesi dalla stipula dell'Accordo Quadro, una relazione di genere sulla situazione del personale maschile e femminile in ognuna delle professioni e in relazione allo stato di assunzioni, della formazione, della promozione professionale, dei livelli, dei passaggi di categoria o di qualifica, di altri fenomeni di mobilità, dell'intervento della Cassa integrazione guadagni, dei licenziamenti, dei prepensionamenti e pensionamenti, della retribuzione effettivamente corrisposta. La relazione di cui sopra dovrà essere corredata dall'attestazione dell'avvenuta*

*trasmissione della stessa alle rappresentanze sindacali aziendali e alla consigliera e al consigliere regionale di parità.***)**

- **(da inserire laddove sia stato previsto nella documentazione della procedura di selezione*: Dichiarazione e relazione sull'assolvimento delle norme sul diritto al lavoro delle persone con disabilità:* *l'Appaltatore,* (nel caso di RTI o Consorzi aggiungere: *in relazione a ciascuna impresa e/o consorziata*), *che occupa un numero pari o superiore a quindici dipendenti e che non rientra nella classificazione di cui all'art. 46 comma 1 del d.lgs. n. 198/2006, è tenuto a consegnare al Committente, entro sei mesi dalla stipula dell'Accordo Quadro, la certificazione di cui all'articolo 17 della legge 12 marzo 1999, n. 68, e una relazione relativa all'assolvimento degli obblighi di cui alla medesima legge e alle eventuali sanzioni e provvedimenti disposti a loro carico nel triennio antecedente la data di scadenza di presentazione delle offerte. La relazione di cui sopra dovrà essere corredata dall'attestazione dell'avvenuta trasmissione della stessa alle rappresentanze sindacali aziendali***)**
- **_____ (se del caso, inserire eventuali ulteriori obblighi derivanti da criteri premiali dell'offerta previsti in procedura ai sensi dell'allegato II.3 del Codice o ai sensi della normativa relativa agli appalti finanziati in tutto o in parte da fondi PNRR o PNC)**

Articolo 13 bis – Segregazione

Al fine di svolgere i Servizi di cui al presente Accordo Quadro, in conformità a quanto previsto dall'art. 11 comma 10 del D.Lgs. 112/2015, per come novellato dal D. Lgs. 139/2018 che recepisce l'art.1, comma 4 della Direttiva 2016/2370/UE (cd. Quarto Pacchetto Ferroviario), l'Appaltatore si impegna ad adottare le seguenti misure atte a garantire la segregazione della gestione dei sistemi informativi della società [inserire Società Beneficiaria] (di seguito, "Segregation of duty dell'ICT dedicato a [Inserire Società Beneficiaria]").

L'Appaltatore si impegna a mantenere al proprio interno una o più strutture operative deputate in via esclusiva alla gestione tecnico-operativa dei servizi di information communication technology (di seguito "Servizi ICT") per [inserire Società Beneficiaria], per le società da essa controllate.

A prescindere dall'adozione di eventuali misure tecniche di segregazione dei dati (es. criptazione), l'Appaltatore provvederà, all'interno delle suddette Strutture, a far sottoscrivere al personale che ha accesso applicativo alle informazioni di [inserire Società Beneficiaria] specifici accordi di riservatezza redatti secondo il template allegato al presente Accordo Quadro (Allegato …). Tali accordi di riservatezza prevederanno il divieto di diffondere o condividere in ogni modo con terzi, e anche internamente all'Appaltatore, qualsiasi informazione rilevante ai sensi del D.Lgs. 112/2015 s.m.i.

In aggiunta a quanto sopra, le informazioni sensibili relative alle funzioni essenziali, così come definite dall'art. 3, comma 1, lett. b-septies) D.lgs. 112/15 s.m.i., saranno accessibili solo al personale dell'Appaltatore debitamente autorizzato da FS Technology S.p.A., previa espressa autorizzazione da parte di [inserire Società Beneficiaria].

Resta fin d'ora inteso che, qualora l'Appaltatore ricorra a fornitori, dovranno essere previsti a carico di tali ultimi analoghi obblighi, con riferimento alla separazione della Struttura e delle infrastrutture fisiche, agli obblighi di riservatezza a carico del personale, ai processi e agli strumenti dedicati alla gestione dei Servizi ICT destinati a [inserire Società Beneficiaria].

L'Appaltatore si impegna sin d'ora ad ottemperare alle eventuali ulteriori misure tecnico-organizzative che dovessero essere imposte dall'Autorità competente ad FSTechnology S.p.A. (anche per il tramite di [inserire Società Beneficiaria]), al fine di garantire la Segregation of Duty dell'ICT dedicato a [inserire Società Beneficiaria].

Nel caso in cui [inserire Società Beneficiaria] contesti ad FS Technology S.p.A. la mancata ottemperanza alle previsioni del presente articolo, FS Technology S.p.A. invierà all'Appaltatore specifica diffida, ai sensi e per gli effetti dell'art.1454 c.c., intimandogli di adempiere entro un termine non inferiore a 30 (trenta) giorni per avviare le attività necessarie all'adeguamento; decorso inutilmente il suddetto termine l'Accordo Quadro si intenderà risolto di diritto.

Articolo 14 – Cessione dei Crediti

I crediti derivanti dai contratti stipulati con le Società del Gruppo FS possono formare oggetto di cessione o di delegazione o di mandato all'incasso o di qualsiasi altro atto di disposizione ("Cessione") a favore di Fercredit Servizi Finanziari SpA – Società del Gruppo FS o di intermediari bancari e finanziari autorizzati e vigilati dalla Banca d'Italia.

Entro 20 (venti) giorni dal ricevimento della notifica della Cessione, la Società del Gruppo FS interessata può opporre diniego espressamente motivato.

In ogni caso, la Società del Gruppo FS cui è stata notificata la Cessione può opporre al cessionario tutte le eccezioni opponibili al cedente in base al contratto con questo stipulato.

La Cessione dovrà essere notificata al Responsabile Amministrativo della Società emittente.

Articolo 15 – Penali

Per le penali si rinvia agli artt. 54 e 55 delle CGC, che qui devono ritenersi integralmente richiamati.

Ad integrazione di quanto sopra, sarà facoltà del Committente applicare le seguenti penali relative al presente Accordo:

[Con riferimento ai termini previsti per il Catalogo elettronico di cui all'articolo "Catalogo Elettronico Ariba":

- ritardo nella tempistica indicata per la produzione della versione definitiva del Catalogo Ariba: € 150,00 per ogni giorno lavorativo di ritardo, fermo restando che in caso di ritardo pari o superiore a 10 giorni il Committente si riserva la facoltà di risolvere il presente Accordo;
- raggiunto tale limite il Committente si riserva la facoltà di risolvere il presente Accordo;

- ritardo nella tempistica indicata per l'aggiornamento del Catalogo Ariba: € 100,00 per ogni giorno lavorativo di ritardo.**]**

[N.B. nel caso in cui al precedente articolo "Obblighi particolari dell'Appaltatore" siano stati previsti gli obblighi per garantire le pari opportunità generazionali e di genere e per promuovere l'inclusione lavorativa delle persone con disabilità, ai sensi dell'art. 1 comma 6 dell'allegato II.3 del d.lgs. n. 36/2023 e dell'articolo 47, comma 6, decreto legge n. 77/2021, occorrerà prevedere anche delle penali da applicare in caso di inadempimento di tali obblighi. Dette penali, in accordo con la SR, dovranno essere commisurate alla gravità della violazione e proporzionali rispetto all'importo dell'Accordo o alle prestazioni dell'Accordo ma nella logica di non vanificare la previsione. A tal fine si riportano degli esempi di penali da poter inserire nel testo, previe eventuali necessarie personalizzazioni che si dovessero ritenere necessarie:

- (inserire nel caso siano stati previsti, al precedente articolo "Obblighi particolari dell'Appaltatore", obblighi in materia di "Promozione dell'occupazione giovanile e femminile": ***Penali per inadempimento degli obblighi in materia di "Promozione dell'occupazione giovanile e femminile" di cui al precedente art. "Obblighi particolari dell'Appaltatore"***

  In caso di mancato o parziale invio di quanto richiesto al precedente art. 13 (verificare correttezza riferimento), *nel termine ivi indicato: € _____ [*es. 0,2 per mille dell'ammontare netto contrattuale*].*

  *Il mancato adempimento dell'invio dei documenti richiesti entro 30 giorni dal termine può comportare l'applicazione di una ulteriore penale di € _____ [*es. 0,5 per mille dell'ammontare netto contrattuale*], ogni trenta giorni di ritardo, fino all'avvenuto adempimento e comunque, a parziale deroga di quanto previsto all'ultimo periodo del presente articolo, per un importo complessivo non superiore al 20% del valore dell'Accordo Quadro.*

  Ove dalla documentazione prodotta risulti che l'Appaltatore non abbia rispettato la quota di assunzione di cui al precedente 13 (verificare correttezza riferimento)*, né abbia dato adeguata motivazione dell'inadempimento, il Committente si riserva di adottare i provvedimenti che riterrà più opportuni nonché di segnalare l'inadempimento alle Autorità competenti.*)

- (inserire nel caso siano stati previsti, al precedente articolo "Obblighi particolari dell'Appaltatore", obblighi in materia di "Relazione di genere sulla situazione del personale maschile e femminile": ***Penali per inadempimento degli obblighi in materia di "Relazione di genere sulla situazione del personale maschile e femminile" di cui al precedente art. "Obblighi particolari dell'Appaltatore"*** *In caso di mancato o parziale invio della documentazione richiesta entro il termine di sei mesi dalla stipula dell'Accordo Quadro: € _____[*es. 0,2 per mille dell'ammontare netto contrattuale*].*

  *Il mancato adempimento dell'invio dei documenti richiesti entro 30 giorni dal termine fissato può comportare l'applicazione di una ulteriore penale di € _____ [*es. 0,5 per mille dell'ammontare netto contrattuale*], ogni trenta giorni di ritardo, fino all'avvenuto adempimento e comunque, a parziale deroga di quanto previsto*

all'ultimo periodo del presente articolo, per un importo complessivo non superiore al 20% del valore dell'Accordo Quadro.)

- (inserire nel caso siano stati previsti, al precedente articolo "Obblighi particolari dell'Appaltatore", obblighi in materia di "Dichiarazione e relazione sull'assolvimento delle norme sul diritto al lavoro delle persone con disabilità": ***Penali per inadempimento degli obblighi in materia di "Dichiarazione e relazione sull'assolvimento delle norme sul diritto al lavoro delle persone con disabilità" di cui al precedente art. "Obblighi particolari dell'Appaltatore"*** *In caso di mancato o parziale invio della documentazione richiesta entro il termine di sei mesi dalla stipula dell'Accordo Quadro: € _____[*es. 0,2 per mille dell'ammontare netto contrattuale*].*

  *Il mancato adempimento dell'invio dei documenti richiesti entro 30 giorni dal termine fissato può comportare l'applicazione di una ulteriore penale di € _____ [*es. 0,5 per mille dell'ammontare netto contrattuale*], ogni trenta giorni di ritardo, fino all'avvenuto adempimento e comunque, a parziale deroga di quanto previsto all'ultimo periodo del presente articolo, per un importo complessivo non superiore al 20% del valore dell'Accordo Quadro.*)

- _____ (se del caso, inserire eventuali penali per inadempimento degli ulteriori obblighi di cui al precedente art. 13, derivanti da criteri premiali dell'offerta previsti in procedura ai sensi dell'allegato II.3 del Codice o ai sensi della normativa relativa agli appalti finanziati in tutto o in parte da fondi PNRR o PNC)**]**

Fermo quanto sopra, l'ammontare delle penali maturate sarà trattenuto sull'importo dei corrispettivi contrattuali in sede di liquidazione delle fatture ovvero, quando occorra, sarà recuperato mediante corrispondente incameramento della Garanzia di cui al successivo art. 16 senza bisogno di diffida o procedimento giudiziario.

L'applicazione delle penali non pregiudica il risarcimento di eventuali danni/ ulteriori oneri sostenuti dal Committente e/o dalla Società emittente a causa degli inadempimenti / ritardi dell'Appaltatore nell'esecuzione delle prestazioni oggetto del presente Accordo.

Qualora il valore complessivo delle penali applicate sull'Accordo superi il 10% del valore dello stesso così come qualora il valore complessivo delle penali applicate sul singolo Ordine applicativo superi il 20% del valore dell'Ordine applicativo al quale si riferiscono, il Committente e la Società emittente si riservano di procedere alla risoluzione, rispettivamente, dell'Accordo e degli Ordini applicativi.

Articolo 16 – Garanzia definitiva

A garanzia dell'esatto adempimento degli obblighi contrattuali, l'Appaltatore ha costituito la garanzia definitiva ("Garanzia" o "Garanzia definitiva") di importo pari a € [•] (Euro ____/_) mediante fideiussione emessa da [•] (di seguito "Garante") – (**All.** [•])[o mediante cauzione mediante accredito, con bonifico di importo pari a € [•] (Euro ____/_– (All. [•])]

La Garanzia definitiva sarà progressivamente svincolata a misura dell'avanzamento dell'esecuzione dell'Accordo Quadro, nel limite massimo dell'80% dell'iniziale importo garantito. Lo svincolo, nei termini e per gli importi

anzidetti, è automatico, senza necessità di benestare del Committente e/o della Società emittente, previa deduzione di crediti del Committente e/o della Società emittente verso l'Appaltatore e con la sola condizione della preventiva consegna al Garante, da parte dell'Appaltatore, dei documenti di "entrata merci" di cui all'art. 57 delle CGC, in originale o in copia autentica, attestanti l'avvenuta esecuzione.

L'ammontare residuo, pari al 20% dell'iniziale importo garantito, sarà svincolato a partire dalla data di approvazione da parte del Committente certificato di regolare esecuzione.

L'Appaltatore dovrà inviare per conoscenza al Committente, in persona del RFE, la comunicazione che invia al Garante ai fini dello svincolo. Il Garante dovrà comunicare al Committente il valore dello svincolo. Il Committente si riserva di verificare la correttezza degli importi svincolati e di chiedere all'Appaltatore e al Garante, in caso di errore, un'integrazione.

La Garanzia definitiva è prestata a garanzia dell'esatto adempimento di tutte le obbligazioni assunte dall'Appaltatore in dipendenza dell'esecuzione dell'appalto e copre il risarcimento dei danni derivanti dall'eventuale inadempimento delle stesse obbligazioni, nonché il rimborso delle somme pagate in più all'esecutore rispetto alle risultanze della liquidazione finale, salva comunque la risarcibilità del maggior danno verso l'Appaltatore.

Il Committente e/o la Società emittente ha, inoltre, diritto di avvalersi in tutto o in parte della Garanzia suddetta, nei limiti dell'importo massimo garantito: *i)* per l'eventuale maggiore spesa sostenuta per il completamento delle prestazioni nel caso di risoluzione del contratto disposta in danno dell'esecutore; *ii*) per provvedere al pagamento di quanto dovuto dall'Appaltatore per le inadempienze derivanti dalla inosservanza di norme e prescrizioni dei contratti collettivi, delle leggi e dei regolamenti sulla tutela, protezione, assicurazione, assistenza e sicurezza fisica dei lavoratori comunque presenti nei luoghi dove viene eseguito il contratto ed addetti all'esecuzione dell'appalto.

In particolare, il Committente e/o la Società emittente potrà altresì avvalersi della Garanzia definitiva anche per la riscossione di penali.

Il Committente e/o la Società emittente ha diritto di incamerare la garanzia, in tutto o in parte, per i danni che essa affermi di aver subito, senza pregiudizio dei suoi diritti nei confronti dell'Appaltatore per la rifusione dell'ulteriore danno eventualmente eccedente la somma incamerata.

La Garanzia prevede, espressamente, la rinuncia della preventiva escussione del debitore principale, di cui all'art. 1944 del cc, la rinuncia all'eccezione di cui all'art. 1957, comma 2 del codice civile, nonché l'operatività della stessa entro 15 giorni, a semplice richiesta scritta.

L'Appaltatore è obbligato a reintegrare la Garanzia suddetta qualora il Committente e/o la Società emittente se ne sia avvalsa – in tutto o in parte – nel corso dell'esecuzione del presente Accordo Quadro.

In caso di mancato reintegro della Garanzia definitiva, il Committente e/o la Società emittente potrà trattenere i ratei di prezzi fino alla concorrenza di un importo che, sommato all'eventuale residuo del massimale della garanzia, ripristini l'ammontare della Garanzia medesima.

[Da inserire qualora sia prevista al precedente articolo 5 una o più opzioni che comportino un aumento dell'importo contrattuale: *Nel caso di esercizio* _____ (inserire la denominazione della/e opzione/i il cui esercizio comporta un aumento di importo, es. opzione di importo e c.d. sesto quinto) *di cui al precedente art. 5, l'Appaltatore sarà tenuto ad estendere la Garanzia definitiva allegata al presente Accordo Quadro al fine di ricomprendere, oltre a tutte le obbligazioni ancora in essere in virtù dell'Accordo Quadro stesso, anche le obbligazioni nascenti dalle predette opzioni, per tutto il periodo di validità di quest'ultimo. In alternativa, ai fini delle opzioni di cui al precedente art. 5, l'Appaltatore potrà produrre una nuova Garanzia definitiva.***]**

L'Appaltatore si obbliga fin da ora, qualora il Committente si avvalga della facoltà di cedere il presente Accordo Quadro, ai sensi del successivo art. 19, a sostituire la Garanzia prodotta a garanzia degli obblighi assunti in forza del presente Contratto con tante garanzie quante saranno le Società destinatarie della fornitura.

Articolo 17 – Recesso

Il Committente, e/o la Società emittente, ovvero la/e Società cessionaria/e, qualora venga esercitata la facoltà di cedere il presente Accordo ai sensi del successivo art. 19 - è in facoltà di recedere unilateralmente dall'Accordo, e/o dal singolo Ordine applicativo, in qualsiasi momento, indipendentemente dallo stato di esecuzione dello stesso.

Il recesso del Committente e/o della Società emittente e/o della/e Società cessionaria/e ha effetto dal giorno in cui viene comunicato all'Appaltatore con lettera raccomandata A.R./PEC, ovvero dalla diversa data indicata nella comunicazione di recesso; a partire dalla suindicata data di efficacia del recesso, l'Appaltatore è tenuto a cessare l'esecuzione delle prestazioni contrattuali.

Nell'ipotesi di cui al primo capoverso del presente articolo, il Committente è tenuto a ritirare e pagare ai prezzi contrattuali per le prestazioni eseguite dall'Appaltatore fino alla data di efficacia del recesso.

È escluso il diritto dell'Appaltatore ad ogni eventuale pretesa, anche di natura risarcitoria, nonché ad ogni compenso indennizzo e/o rimborso, anche in deroga a quanto previsto dall'art. 1671 c.c..

Articolo 18 – Clausola risolutiva espressa

Il presente Accordo e/o i singoli Ordini applicativi potranno essere risolti nei casi previsti dall'art. 122 D.Lgs. 36/2023 e dalle Condizioni Generali.

Il presente Accordo e/o i singoli Ordini applicativi potranno, inoltre, essere risolti dal Committente e/o dalla Società emittente, ai sensi dell'art. 1456 c.c., nei seguenti casi:

- intervenuta sentenza di condanna passata in giudicato ovvero sentenza di applicazione della pena su richiesta delle parti per reati tali da incidere sulla moralità professionale o per delitti finanziari, nonché per frodi nei riguardi di Ferservizi o delle Società del Gruppo FS, di subappaltatori, di fornitori, di lavoratori o di altri soggetti comunque interessati ai lavori;
- inosservanza degli obblighi che la normativa vigente pone a carico dei datori di lavoro in materia di sicurezza sul lavoro;

- qualora l'Appaltatore contravvenga alle disposizioni dei seguenti articoli dell'Accordo: "Tracciabilità dei Flussi Finanziari", "Obblighi particolari dell'Appaltatore", "Cessione del Contratto e subappalto", "Trasparenza prezzi", "Contratto di di lavoro, previdenza e assicurazioni", "Clausola Integrità e Conflitto di interessi ", "Tutela della riservatezza", "Divieto di utilizzo di marchi e/o altri segni distintivi di Ferservizi/Gruppo FS" "Proprietà intellettuale e garanzie dell'Appaltatore", **[**eventuale: *"Clausola di non gradimento"***]**, "Sicurezza sui luoghi di lavoro e igiene del lavoro", **[***"Auditing"***]**, "Rispetto di Misure Restrittive";
- nelle ipotesi espressamente previste nell'articolo "Penali";
- **[**risoluzione di n. _____ Ordini applicativi (anche non consecutivi).**]**

Nei casi sopra richiamati, la risoluzione si verifica di diritto mediante unilaterale dichiarazione del Committente a mezzo di lettera raccomandata A/R o PEC e comporta l'eventuale incameramento della cauzione ed il risarcimento di eventuali ulteriori danni.

Salva diversa indicazione, la risoluzione dell'Accordo Quadro comporta anche la risoluzione degli ordini applicativi. Ove sia specificato che la risoluzione dell'Accordo Quadro non si estende anche agli Ordini applicativi, o ad alcuni di tali Ordini, l'Appaltatore sarà tenuto all'esecuzione delle prestazioni dedotte negli Ordini medesimi.

Qualora il Committente si avvalga della facoltà di cedere il presente Accordo ai sensi dell'art. 19, la facoltà di risoluzione dell'Accordo potrà essere esercitata anche dalla/e Società/e cessionaria/e.

Resta convenuto che le prestazioni oggetto del presente Accordo dovranno essere eseguite, sempre ed in ogni caso, nell'ottica di salvaguardare l'immagine ed il prestigio del Committente e del Gruppo FS nel suo complesso, privilegiando sempre tali indicazioni rispetto al successo dell'attività affidata. A tal fine, l'Appaltatore espressamente dichiara di ben conoscere le prescrizioni contenute nel Codice Etico di cui al successivo art. 27 e di informare il proprio comportamento ai criteri in esso previsti.

L'Accordo si considererà automaticamente risolto in caso di violazione della normativa in materia di responsabilità delle persone giuridiche di cui al D.Lgs. 231/2001 da parte degli amministratori, dipendenti o collaboratori dell'Appaltatore, attestata con sentenza definitiva passata in giudicato. In questo senso, l'Appaltatore dà atto di aver visionato il Modello Organizzativo del Committente di cui al successivo art. 27 e di aver sensibilizzato i propri dipendenti e collaboratori alle problematiche ed ai comportamenti sanzionati dal D.Lgs. 231/2001.

Con riferimento agli obblighi di tracciabilità finanziaria di cui alla Legge n. 136/2010, l'Accordo si considererà, altresì, automaticamente risolto, in caso di transazioni eseguite senza avvalersi di banche o della società Poste Italiane S.p.A. ovvero eseguite con strumenti diversi dal bonifico bancario o postale che non siano idonei a garantire la piena tracciabilità delle operazioni in relazione al Corrispettivo dovuto per il presente Accordo.

Articolo 19 – Cessione dell'Accordo Quadro e subappalto

È fatto assoluto divieto all'Appaltatore di cedere totalmente o parzialmente il presente Accordo o i singoli Ordini applicativi.

L'Appaltatore ha dichiarato che non intende avvalersi del Subappalto.

In alternativa

Il ricorso al subappalto è consentito, in conformità a quanto previsto dall'art. 119 del D.Lgs n. 36/2023, nei limiti di quanto dichiarato dall'Appaltatore in sede di presentazione della propria offerta.

A tal proposito l'Appaltatore ha presentato, contestualmente all'offerta, apposita dichiarazione ove ha indicato che intende subappaltare le seguenti prestazioni:

- [•],

- [•];

Pertanto, nessuna prestazione diversa da quelle indicate dall'Appaltatore in sede di offerta affidata in subappalto. Nel contratto di subappalto dovrà essere espressamente previsto che il subappaltatore è tenuto al rispetto e alla completa osservanza di tutte le disposizioni vigenti in materia di assunzione della manodopera e di contribuzione previdenziale, assicurativa ed antinfortunistica**.]**

[IN CASO DI DIVIETO DI "SUBAPPALTO A CASCATA", ove, in ragione delle specifiche caratteristiche dell'appalto, dell'esigenza di rafforzare i controllo dei luoghi di lavoro, di garantire una più intensa tutela delle condizioni di lavoro e della salute e sicurezza sul lavoro ovvero di prevenire il rischio di infiltrazioni mafiose, nella documentazione di gara sia stato previsto tale divieto inserire la seguente clausola in coerenza con quanto previsto nella documentazione di gara medesima: *Le seguenti prestazioni possono essere subappaltate ma non possono, a loro volta, essere oggetto di ulteriore subappalto:* ___ (indicare le prestazioni). *Ciò in ragione dell'esigenza di garantire* ___ (indicare le motivazioni).**]**

Ai sensi dell'art. 119 comma 2-bis del Codice, [se previsto subappalto: *nei contratti di subappalto o*] nei subcontratti è obbligatorio l'inserimento di clausole di revisione prezzi riferite alle prestazioni oggetto [se previsto subappalto: *del subappalto o*] del subcontratto, che si attivano al verificarsi delle particolari condizioni di natura oggettiva di cui al precedente art. 10**.**

In caso di violazione delle disposizioni di cui sopra la Società emittente procederà ai sensi delle Condizioni Generali.

Nel caso di ricorso a subcontratti, si applica l'art. 15.5 delle Condizioni Generali.

Il Committente si riserva, fin da ora, la facoltà di cedere totalmente o parzialmente il presente Accordo in favore di una, alcune o tutte delle Società del Gruppo FS.

A tal fine l'Appaltatore, con la sottoscrizione del presente Accordo espressamente acconsente alla cessione suddetta.

Tale cessione diverrà efficace e produrrà i suoi effetti dal momento della ricezione, da parte dell'Appaltatore ceduto, della notifica di cessione.

Articolo 20 – Trasparenza prezzi

L'Appaltatore espressamente ed irrevocabilmente:

- dichiara che non vi è stata mediazione od altra opera di terzi per la conclusione del presente Accordo;
- dichiara di non aver corrisposto né promesso di corrispondere ad alcuno, direttamente o attraverso imprese collegate o controllate, somme e/o altri corrispettivi a titolo di intermediazione o simili e comunque volte a facilitare la conclusione del presente Accordo;
- si obbliga a non versare ad alcuno, a nessun titolo, somme finalizzate a facilitare e/o a rendere meno onerosa l'esecuzione e/o la gestione del presente Accordo rispetto agli obblighi con esso assunti né a compiere azioni comunque volte agli stessi fini.

Nel caso in cui risultasse non conforme al vero anche una sola delle dichiarazioni rese ai sensi del comma precedente, ovvero l'Appaltatore non rispettasse gli impegni e gli obblighi ivi assunti per tutta la durata del presente Accordo, lo stesso si intenderà automaticamente risolto, ai sensi e per gli effetti dell'articolo 1456 del codice civile, per fatto e colpa dell'Appaltatore, che sarà conseguentemente tenuto al risarcimento di tutti i danni derivanti dalla risoluzione.

Articolo 21 – Contratto di lavoro, previdenza e assicurazioni

Nella qualità di datore di lavoro, l'Appaltatore deve, a propria cura e spese, provvedere alla completa osservanza delle norme e prescrizioni legislative e regolamentari relative agli infortuni sul lavoro, alle malattie professionali, all'assistenza sanitaria dei dipendenti e dei loro familiari ed alle altre forme di previdenza in favore dei lavoratori.

L'Appaltatore è tenuto ad osservare, indipendentemente dalla propria struttura industriale o cooperativa, con riferimento ai lavoratori subordinati o ai soci, soci/lavoratori subordinati impiegati nell'esecuzione delle prestazioni oggetto del presente Accordo e relativi Ordini applicativi, le norme vigenti in materia di pagamento dei contributi previdenziali ed assicurativi.

L'Appaltatore è tenuto, per tutta la durata dell'appalto, sempre con riferimento ai lavoratori impiegati nell'esecuzioni delle prestazioni oggetto del presente Accordo e relativi Ordini applicativi, a rispettare la disciplina vigente in materia di Trattamento di Fine Rapporto, compresa la normativa in materia di previdenza complementare e devoluzione del TFR di cui al D. Lgs. 5 dicembre 2005 n. 252 e successive modifiche ed integrazioni.

Articolo 22 – Responsabilità dell'Appaltatore

L'Appaltatore manleva e assume su di sé la piena responsabilità di qualunque evento dannoso possa derivare, al Committente, alla Società emittente, alle società del Gruppo FS beneficiarie dei servizi resi, ovvero a terzi, che sia conseguenza dell'inadempimento delle obbligazioni previste dal Contratto e dagli Ordini applicativi e dell'ADP qualora previsto.

L'Appaltatore assume su di sé la piena responsabilità di qualunque evento dannoso possa derivare, al Committente, alla Società emittente o a terzi, anche come mera conseguenza dell'attività connessa all'Accordo, imputabile a fatto e colpa dell'Appaltatore medesimo o degli addetti.

L'Appaltatore si obbliga ad osservare, nella esecuzione delle prestazioni oggetto del presente Accordo, tutte le prescrizioni imposte dalla legge, esonerando il Committente e/o la Società emittente da ogni responsabilità conseguente.

L'Appaltatore, inoltre, inoltre esonera espressamente il Committente e/o la Società emittente da ogni responsabilità in ordine a pretese e/o richieste degli addetti utilizzati avanzate in relazione all'esecuzione delle prestazioni oggetto del presente Accordo.

Resta inteso che FSTechnology S.p.A., in qualità di mandataria delle Società del Gruppo Ferrovie dello Stato Italiane beneficiarie dei servizi, e/o la Società emittente, sono pienamente legittimate ad intraprendere ogni opportuna azione volta ad ottenere il risarcimento di qualsiasi danno, perdita, pretesa o pregiudizio, sia diretto che indiretto, subito dalle società beneficiarie in conseguenza dell'inadempimento o dell'inesatta esecuzione delle prestazioni disciplinate dal presente Contratto e dai relativi Ordini applicativi e dell'ADP qualora previsto.

Le Parti convengono altresì espressamente che qualsiasi sanzione amministrativa, pecuniaria o di altra natura, irrogata dal Garante per la protezione dei dati personali o da altra Autorità competente a seguito di inadempimenti attribuibili all'Appaltatore a qualsiasi Società del Gruppo FS, sarà integralmente a carico dell'Appaltatore, sollevando la parte destinataria da ogni correlato onere economico.

Articolo 23 – Diritto di rivalsa

Nell'ipotesi in cui, per fatto e colpa dell'Appaltatore, il Committente e/o la Società emittente fossero tenuti al pagamento di somme per l'esecuzione delle prestazioni di cui al presente Accordo a favore di soggetti diversi dall'Appaltatore, le stesse avranno diritto a rivalersi direttamente sull'Appaltatore dietro esibizione delle relative fatture quietanzate anche incamerando a titolo compensativo parte della Garanzia definitiva.

Articolo 24 – Durc e Manleve

L'Appaltatore si obbliga a mantenere e verificare, per tutta la durata dell'Accordo, la situazione di regolarità ai fini retributivi, contributivi, assistenziali e assicurativi nel rispetto di quanto previsto dalla normativa vigente e dalle Condizioni Generali.

La regolarità contributiva è accertata tramite DURC in corso di validità..

Nel caso in cui il DURC dell'Appaltatore risulti irregolare, la Società emittente si riserva di esercitare la facoltà di sospendere completamente - fino all'accertato ripristino della posizione di regolarità contributiva dell'Appaltatore - l'emissione di nuovi Ordini applicativi e, di norma, non procederà alla validazione delle Entrate Merci, né ai pagamenti relativi agli applicativi emessi in attuazione dell'Accordo.

In relazione all'irregolarità del DURC, la Società emittente attiverà presso gli Enti

preposti l'intervento sostitutivo.

La Società emittente effettuerà l'intervento sostitutivo sulla base e nei limiti dell'importo netto dell'intero debito scaduto relativo alle prestazioni eseguite in attuazione dell'Accordo liquidabile all'Appaltatore.

La Società emittente si riserva di indicare, nell'apposita comunicazione preventiva all'Ente, oltre all'ammontare complessivo del proprio debito "scaduto" liquidabile nei confronti dell'Appaltatore in relazione all'Accordo, anche il dettaglio del predetto debito complessivo riferito ai corrispettivi dei singoli Ordini applicativi.

Quanto sopra non darà diritto all'Appaltatore di disporre autonomamente la sospensione del servizio, né lo stesso potrà pretendere altro a titolo di interessi o di risarcimento danni.

L'Appaltatore si assume, inoltre, ogni responsabilità per danni che possano derivare al proprio personale, a persone o cose di proprietà della Società emittente e/o di altre Società del Gruppo FS e/o di terzi per fatto proprio o dei propri dipendenti, collaboratori o a questi direttamente o indirettamente ricollegabili e si impegna a tenere manlevati e indenni la Società emittente e/o le altre Società del Gruppo FS da qualsiasi pretesa risarcitoria e/o indennitaria avanzata al riguardo dai terzi in genere.

L'Appaltatore si obbliga a manlevare e tenere comunque indenne – sostanzialmente e processualmente, a semplice richiesta e senza facoltà di opporre eccezioni - la Società emittente e/o le altre Società del Gruppo FS da ogni eventuale onere, richiesta o pretesa, anche derivante da sentenze, avanzata da soggetti terzi nei confronti della Società emittente o di altra Società del Gruppo FS a qualsiasi titolo o ragione connessa al rapporto contrattuale derivante dal presente Accordo, quale, a titolo meramente esemplificativo e non esaustivo, richieste avanzate da dipendenti, collaboratori, subappaltatori, subcontraenti, sub affidatari, fornitori dell'Appaltatore, nonché Pubbliche Amministrazioni, Istituti ed Enti Pubblici e soggetti terzi in genere, in ragione di qualsiasi forma di responsabilità anche solidale che dovesse risultare riferibile alla Società emittente o altra Società del Gruppo FS anche in virtù di normativa sopravvenuta alla stipula del presente Atto.

Fermo restando quanto sopra pattuito, resta inteso che la Società emittente sarà legittimata a sospendere le procedure di pagamento finalizzate alla liquidazione dei compensi dovuti all'Appaltatore e, in subordine, eventualmente ad escutere in tutto o in parte, anche solo in via cautelativa, la Garanzia prestata in tutti i casi in cui la Società emittente stessa intenderà tutelare la propria posizione a fronte di iniziative poste in essere nei suoi confronti, anche solo in sede stragiudiziale, da parte di soggetti terzi, pubblici o privati, di qualunque natura, che affermino di avere diritto a rivalersi nei confronti della stessa per richieste di natura economica vantate a qualsiasi titolo nei confronti dell'Appaltatore.

Articolo 25 – Responsabile dell'Accordo Quadro dell'Appaltatore

L'Appaltatore ha nominato e comunicato le generalità del Responsabile dell'Accordo, deputato al coordinamento di tutte le attività volte all'adempimento degli obblighi contrattuali, nella persona di [•], tel. [•] e-mail [•] pec. [•].

L'Appaltatore garantirà, tra l'altro, la continuità in caso di assenza del Responsabile dell'Accordo, attraverso un sostituto autorizzato a tutti gli effetti a farne le veci.

Il Responsabile dell'Accordo ed il suo sostituto rivestiranno l'incarico di rappresentanti dell'Appaltatore ed avranno i poteri decisionali per trattare e concordare con il RFE, secondo le rispettive competenze, ogni azione tecnica, contrattuale e amministrativa inerente allo svolgimento delle attività oggetto del presente incarico.

Il Responsabile dell'Accordo si interfaccerà direttamente con il RFE per quanto riguarda le indicazioni necessarie per assicurare il regolare svolgimento delle attività entro i termini e secondo le prescrizioni del presente Accordo.

Articolo 26 – Soggetto Responsabile per la fase esecutiva dell'Accordo Quadro

Il soggetto Responsabile per la fase esecutiva dell'Accordo ("RFE"), deputato alla gestione ed al controllo sull'esatta esecuzione del presente Accordo, è individuato nel Responsabile *pro tempore* della Struttura **[.]**.

Il RFE si riserva il diritto di controllare e verificare durante il corso di esecuzione delle prestazioni la perfetta osservanza da parte dell'Appaltatore di tutte le pattuizioni contrattuali, nonché il corretto e tempestivo svolgimento da parte dello stesso di tutte le attività necessarie per l'espletamento delle prestazioni.

Al RFE spetterà il compito di indirizzare e monitorare l'operato della Società emittente.

Al RFE spetterà infine il compito di determinare i nuovi prezzi relativi a variazioni delle prestazioni contrattuali.

Qualora il Committente si avvalga della facoltà di cedere il presente Accordo, le attività di gestione e controllo attribuite al RFE faranno capo alla/e Società/e destinataria/e dei servizi/forniture in ragione della cessione.

Articolo 27 – Clausola integrità e Conflitto interessi

Ferservizi e le Società emittenti gestiscono i rapporti e gli affari, riferendosi ai principi contenuti nel Codice Etico del Gruppo FS ("Codice Etico"), nella Policy Anti-Corruption del Gruppo FS ("Policy Anti-Corruption"), nei rispettivi Modelli di Organizzazione Gestione e Controllo ex d.lgs. n. 231/2001 ("Modello 231") e negli strumenti di compliance antitrust che costituiscono parte integrante del Programma di Compliance Antitrust del Gruppo FS ("Programma di Compliance Antitrust").

L'Appaltatore dichiara e garantisce di aver preso visione (i) del Codice Etico (ii) della Policy Anti-Corruption; (iii) dei Modelli 231 e (iv) degli strumenti di compliance antitrust che costituiscono parte integrante del Programma di Compliance Antitrust, e di aver ben compresi i principi, i contenuti e le finalità dei sopra citati documenti, pubblicati sui siti web istituzionali delle su menzionate Società e/o di Ferrovie dello Stato italiane S.p.A., che possono essere scaricati e stampati e di cui l'Appaltatore potrà chiedere in ogni momento copia cartacea.

L'Appaltatore si impegna al rispetto dei principi e delle previsioni contenuti nei documenti di cui al precedente paragrafo sia nello svolgimento della propria attività sia nella gestione dei rapporti con terzi, assicurando che questi ultimi si informino a principi equivalenti a quelli adottati dalle Società su menzionate.

L'Appaltatore prende atto che le segnalazioni di informazioni sulle violazioni, aventi ad oggetto fatti riferibili a persone del Gruppo FS o a terzi che intrattengono rapporti di lavoro, di collaborazione o d'affari con il Gruppo FS, che possono integrare:

- violazioni del Modello 231 e delle procedure che ne costituiscono attuazione e/o della Policy Anti-Corruption e del Modello di Gestione Anti-Corruption, e/o del Codice Etico, e/o in ogni caso idonee ad arrecare danno o pregiudizio, anche solo d'immagine o reputazionale, al Gruppo FS;
- illeciti amministrativi, contabili, civili o penali;
- condotte illecite rilevanti ai sensi del d.lgs. n. 231/2001;
- violazioni del diritto dell'Unione Europea richiamate dal decreto legislativo n.24/2023 e s.m.i.;

possono essere effettuate tramite i canali disponibili sui siti web istituzionali.

La violazione da parte dell'Appaltatore di uno qualsiasi dei principi e delle previsioni contenuti nel Codice Etico e/o nella Policy Anti-Corruption del Gruppo FS e/o nel Modello 231 e/o nel Programma di Compliance Antitrust, nonché il mancato rispetto degli impegni di cui al presente articolo configurano un'ipotesi di risoluzione di diritto del contratto ai sensi e per gli effetti di cui all'art. 1456 c.c. e fatto salvo, in ogni caso, il risarcimento del danno.

Ai fini dell'esecuzione dell'Accordo, l'Appaltatore dichiara l'insussistenza di situazioni soggettive od oggettive che possano comportare un conflitto di interessi che osti in qualsivoglia misura allo svolgimento del Accordo medesimo.

Parimenti, l'Appaltatore si impegna, ove nelle more dell'esecuzione dell'Accordo dovessero insorgere impreviste situazioni di conflitto di interessi, a darne immediata notizia al Committente, che procederà alle valutazioni del caso.

Nel caso in cui risultasse non conforme al vero anche una sola delle dichiarazioni rese ai sensi del presente articolo, ovvero l'Appaltatore non rispettasse gli impegni e gli obblighi assunti per tutta la durata dell'Accordo, lo stesso si intenderà automaticamente risolto, ai sensi e per gli effetti dell'art. 1456 del codice civile, per fatto e colpa dell'Appaltatore, che sarà conseguentemente tenuto al risarcimento dei danni derivanti dalla risoluzione.

Articolo 28 – Tutela della riservatezza [eventuale: e Informazioni Privilegiate]

Con la sottoscrizione del presente Accordo l'Appaltatore s'impegna a non rivelare a terzi e comunque a non utilizzare in alcun modo, per motivi che non siano attinenti all'esecuzione dello stesso, le informazioni relative a fatti, atti e programmi del Committente ovvero delle Società del Gruppo FS, che vengano messe a disposizione o di cui venisse comunque a conoscenza in conseguenza del presente Accordo.

L'obbligo alla riservatezza sarà assoluto e vincolante in via contestuale alla stipula del presente Accordo e resterà valido anche dopo la scadenza dello stesso fino al momento in cui le informazioni delle quali è venuto a conoscenza siano divenute di dominio pubblico.

L'Appaltatore è responsabile nei confronti del Committente e delle Società del Gruppo FS dell'esatta osservanza da parte dei propri dipendenti, ausiliari e collaboratori, nonché dei propri subappaltatori in genere e dei dipendenti, ausiliari e collaboratori di questi ultimi, degli obblighi di riservatezza ed è tenuto pertanto a risarcire tutti i danni che allo stesso dovessero derivare dall'inosservanza di detti obblighi.

In caso sviluppi e/o di studi di nuove progettualità richieste dalla Committente nell'ambito dei servizi ovvero della fornitura oggetto del presente Contratto, l'Appaltatore si impegna sin d'ora, a rispettare o a far rispettare gli obblighi di riservatezza assunti anche nei confronti dei potenziali partner di mercato della Committente e/o del Gruppo FS, previa comunicazione da parte della Committente degli accordi di riservatezza contenenti detti obblighi.

[Eventuale in caso di informazioni privilegiate: Le Parti sono a conoscenza degli obblighi derivanti da tutte le leggi e regolamenti in materia di abuso di mercato - ivi incluso il Regolamento UE relativo agli abusi di mercato n. 596/2014 ("Normativa sull'Abuso di Mercato") - e delle restrizioni relative all'uso o alla diffusione delle informazioni che possono essere considerate "informazioni privilegiate" ai sensi della Normativa sull'Abuso di Mercato, compresa l'istituzione di un registro delle persone che hanno accesso a tali informazioni privilegiate, e convengono di rispettare costantemente la Normativa sull'Abuso di Mercato nella misura a loro applicabile**].**

Articolo 29 – Divieto di utilizzo di marchi e/o altri segni distintivi del Committente/Gruppo FS

Il presente rapporto contrattuale non autorizza in nessun modo l'Appaltatore, o altro soggetto da questi incaricato, ad utilizzare alcun segno distintivo del Committente o di altra Società del Gruppo FS.

A titolo esemplificativo e non esaustivo, è vietato, salvo specifica autorizzazione scritta del Committente, l'uso dei marchi, loghi, *domain name*, segni grafici di proprietà del Committente e delle Società del Gruppo FS nonché l'utilizzo di qualsivoglia altro segno grafico che possa ingenerare confusione tra le attività svolte dall'Appaltatore e quelle svolte dal Committente e dalle altre Società del Gruppo FS.

L'Appaltatore si obbliga a manlevare e tenere indenne il Committente e/o la Società emittente da ogni e qualsiasi pretesa e/o richiesta di terzi, incluse quelle di eventuali danni che possano derivare dall'inosservanza e/o dalla violazione degli obblighi di cui ai commi che precedono.

In caso di inadempimento anche solo di uno degli obblighi sopra elencati, il Committente avrà la facoltà di risolvere l'Accordo ai sensi dell'art. 1456 c.c. e, indipendentemente dall'esercizio di tale facoltà, il diritto all'integrale risarcimento dei danni subiti in conseguenza dell'inadempimento.

Articolo 30 – Proprietà intellettuale e garanzie dell'Appaltatore

L'Appaltatore trasferisce integralmente alla Società emittente a titolo gratuito ed in via esclusiva, ogni diritto di proprietà intellettuale, di natura patrimoniale, che possa comunque essere riferito agli elaborati prodotti in esecuzione delle prestazioni affidate e a quant'altro realizzato nell'esecuzione del presente Accordo.

Pertanto, nel rinunciare sin d'ora a far valere ogni diritto di cui al precedente comma, l'Appaltatore riconosce incondizionatamente alla Società emittente ogni diritto di utilizzazione economica, irrevocabile e privo di royalty, su quanto comunque realizzato nell'esecuzione del presente Accordo, compresi, a titolo meramente esemplificativo, il diritto alla riproduzione, il diritto di esecuzione, di diffusione, di distribuzione, di pubblicazione, di elaborazione e sviluppo, di concedere in licenza, promuovere e creare opere derivate.

Fermo restando quanto previsto dall'art. 5 delle "Condizioni Generali" richiamate al precedente art. 3, l'Appaltatore dichiara sin da ora che ogni contributo comunque fornito nel corso dell'esecuzione del presente Accordo in qualsiasi forma presentato non viola alcun diritto di proprietà intellettuale altrui né diritti della persona comunque denominati.

Conseguentemente, l'Appaltatore fornisce espressa garanzia, senza limite di tempo, contro ogni possibile pretesa da parte di terzi che assumano essere titolari, licenziatari o comunque detentori di diritti di proprietà intellettuale su quanto comunque realizzato nell'esecuzione del presente Accordo. L'Appaltatore presta analoga garanzia anche contro ogni possibile rivendicazione di terzi che lamentino la lesione di diritti della persona quali, ad esempio, il diritto all'immagine.

Pertanto, l'Appaltatore accetta, irrevocabilmente e perpetuamente, di tenere indenne e manlevato il Committente e/o la Società emittente e/o le Società del Gruppo FS da ogni pretesa, richiesta, risarcimento, costo, onere e responsabilità, comprese le spese di gestione amministrativa o di consulenza e legali extragiudiziali ragionevoli, avanzata da terzi a causa delle attività poste in essere in esecuzione del presente Contratto o comunque da queste ultime derivanti.

[Eventuale – nel caso di realizzazione di Deliverables da parte del Fornitore

Relativamente ai Deliverables realizzati dall'Appaltatore nell'esecuzione del Contratto, lo stesso dovrà:

- specificare nell'offerta e/o nel preventivo, o in un suo allegato, anche gli organi, i mezzi, i dispositivi, i processi di lavorazione brevettati dallo stesso Appaltatore, che intenda eventualmente adottare, segnalando per ciascuno di essi gli estremi del brevetto ovvero di altri elementi di privativa;
- garantire, in ogni tempo, FS Tech contro ogni e qualsiasi pretesa da parte di titolari o concessionari di brevetti, marchi, licenze, disegni, modelli e altre opere dell'ingegno utilizzati ai fini dell'esecuzione del Contratto.

Con riferimento all'utilizzo di proprietà intellettuali di terzi ("Componenti di terzi") che lo stesso ritenga necessarie ai fini dell'esecuzione del Contratto, l'Appaltatore si obbliga altresì a specificare nell'offerta e/o nel preventivo o in

un suo allegato, l'utilizzo delle stesse, indicandone i relativi costi. L'Appaltatore dovrà richiedere preventiva autorizzazione scritta alla Committente ai fini dell'utilizzo delle Componenti di terzi. La Committente valuterà preventivamente, a suo insindacabile giudizio, di acquistare le Componenti di terzi in autonomia, per metterle a disposizione dell'Appaltatore. Laddove la Committente non voglia utilizzare le Componenti di terzi indicate dall'Appaltatore, quest'ultimo si impegna sin d'ora a proporre soluzioni alternative di gradimento della stessa Committente.

Fermo quanto sopra, FS Tech resta estranea ai rapporti tra l'Appaltatore ed i titolari dei brevetti e alle eventuali controversie che dovessero insorgere tra detti soggetti.

Salva diversa disposizione contenuta nel Contratto, l'Appaltatore si impegna a porre in essere tutto quanto necessario affinché FS Tech possa esercitare il diritto a riparare o far riparare da terzi gli organi, i pezzi o i dispositivi forniti dall'Appaltatore medesimo e di procurarsi i pezzi necessari per le eventuali riparazioni, senza che sia dovuto alcun compenso al titolare e/o licenziatario.**]**

Articolo 31 – Tutela dei dati personali
[inserire la disciplina fornita dal DPO]

Articolo 31 bis – Accordo di Data Protection
[inserire la disciplina fornita dal DPO]

Articolo 32 – Clausola di non gradimento

Omissis.

Articolo 32 bis – Clausola sociale

[Inserire se nella *lex specialis* è prevista la clausola sociale sul CCNL e/o sulla stabilità occupazionale, eliminare i passaggi non pertinenti: *L'Appaltatore è tenuto a garantire l'applicazione del contratto collettivo nazionale e territoriale (o dei contratti collettivi nazionali e territoriali di settore) indicato nella documentazione di gara, oppure il diverso contratto collettivo indicato in sede di offerta, che, in ogni caso, deve garantire ai dipendenti le stesse tutele economiche e normative del CCNL indicato nella documentazione di gara.*

L'Appaltatore si impegna ad assicurare che le medesime tutele normative ed economiche siano garantite dai propri subappaltatori ai lavoratori in subappalto.

Ferma restando la necessaria armonizzazione con l'organizzazione dell'operatore economico subentrante e con le esigenze tecnico-organizzative e di manodopera previste nel nuovo contratto, l'Appaltatore è tenuto a garantire la stabilità occupazionale del personale impiegato nel contratto, assorbendo prioritariamente nel proprio organico il personale già operante alle dipendenze dell'appaltatore uscente.

L'elenco e i dati relativi al personale attualmente impiegato dal contraente uscente per l'esecuzione del contratto sono riportati negli allegati alla documentazione di gara **(la *lex specialis* dovrà avere come allegato l'*"Elenco dei lavoratori impiegati nell'appalto"*).**

(Qualora non già previste al precedente paragrafo "Obblighi particolari dell'Appaltatore", integrare la clausola in coerenza con la *lex specialis*, prevedendo l'impegno dell'Appaltatore a garantire l'adozione di misure

orientate a garantire le pari opportunità generazionali, di genere e di inclusione lavorativa per le persone con disabilità o svantaggiate: _____).]

Articolo 33 – Sicurezza sui luoghi di lavoro e igiene del lavoro

L'Appaltatore, di cui il Committente ha verificato l'idoneità tecnico professionale ai sensi dell'art. 26 del D. Lgs. n. 81/2008, eseguirà le prestazioni oggetto del Contratto osservando scrupolosamente tutte le norme in materia di sicurezza ed igiene del lavoro vigenti al momento dell'esecuzione, incluse quelle non esplicitamente citate nell'Accordo e nei relativi allegati.

A tale fine, l'Appaltatore si impegna, in particolare, affinché gli addetti, demandati in esecuzione di ciascun Ordine applicativo ad accedere presso i siti del Gruppo FS, rispettino tutte le disposizioni impartite dal Committente e dalle altre Società del Gruppo FS in materia di sicurezza degli impianti e degli stabili di proprietà.

In particolare l'Appaltatore si impegna a prendere visione e far osservare agli addetti tutte le disposizioni in materia di salute e sicurezza sui luoghi di lavoro, emanate dal Committente e dalla Società emittente, per tutti i propri siti dislocati sul territorio italiano, in conformità con quanto disposto dal D.Lgs. 81/2008 e successive modifiche.

L'importo relativo ai costi della sicurezza è pari a zero, in quanto l'Accordo non presenta rischi di interferenza ai sensi e per gli effetti dell'art. 26 del D.Lgs. n. 81/2008. Per tale motivo non si è provveduto alla redazione del documento unico di valutazione dei rischi interferenziali (D.U.V.R.I.).

Relativamente all'individuazione e quantificazione degli oneri della sicurezza e relativi D.U.V.R.I., trattandosi di Accordo Quadro si precisa che, al verificarsi dei presupposti, gli stessi saranno quantificati in sede di emissione degli Ordini applicativi).

Articolo 34 – Auditing

[Eventuale da prevedere negli Accordi di importo superiore a € 500.000,00:

L'Appaltatore si obbliga a tenere una contabilità separata di quanto attinente al presente Atto, documentata ai sensi di legge, ed a consentire in ogni momento idonee verifiche da parte del Committente e/o della Società emittente e/o da soggetto terzo da questo incaricato.

A tal fine si obbliga a mettere a disposizione del Committente e/o della Società emittente e/o del soggetto da questo incaricato, tutte le volte che questi ne facesse richiesta, tutte le proprie scritture contabili ed a facilitare in ogni ragionevole misura l'espletamento delle verifiche di cui sopra.

Il Committente e/o la Società emittente avrà facoltà di effettuare audit, ispezioni, verifiche, monitoraggi, con proprio personale o tramite società terze da esso incaricate, per verificare la rispondenza di quanto previsto col presente Atto e suoi allegati o comunque ordinato all'Appaltatore a quanto eseguito.

Fermo restando quanto disposto dall'art. 15 delle Condizioni Generali di Contratto, l'Appaltatore, a semplice richiesta del Committente e/o delle Società

emittenti, si impegna altresì a fornire tutte le notizie relative alle sub-commesse aperte o da aprire a carico dell'Accordo con l'indicazione del soggetto responsabile designato.**]**

Articolo 35 – Rispetto di Misure restrittive

L'Appaltatore dichiara di, e si obbliga a, operare nel rispetto (*i*) delle misure restrittive vigenti, adottate, promulgate, emanate, applicate, imposte o fatte valere dall'Unione Europea, dalla Repubblica Italiana, dall'Office of Foreign Assets Control del Dipartimento del Tesoro degli Stati Uniti d'America, dal Consiglio di Sicurezza delle Nazioni Unite, dal dipartimento del Tesoro del Regno Unito; (*ii*) di ogni altra misura restrittiva di natura commerciale promulgata, emanata, applicata, imposta o fatta valere dall'Unione Europea, dalla Repubblica Italiana (es. da UAMA-Unità per le autorizzazioni dei materiali di armamento), dal Bureau of Industry and Security degli USA che vieti, limiti o sottoponga a uno specifico iter autorizzativo determinati flussi commerciali in base alle caratteristiche dei beni/tecnologie e/o dei Paesi di destinazione e/o degli usi/utilizzatori finali (ad es. misure di *export control*); nonché (*iii*) delle relative disposizioni nazionali di attuazione applicabili.

L'Appaltatore dichiara di, e si obbliga a, non porre in essere alcuna attività e a non trovarsi in alcuna situazione che possa comportare, per il Committente la violazione delle normative di cui al paragrafo precedente o l'imposizione di qualsivoglia misura restrittiva in base alle stesse, inclusa, a titolo esemplificativo, la fattispecie di cui all'art. 5 *duodecies* di cui al Reg. (UE) 833/2014 e s.m.i., anche attraverso l'inserimento, ove opportuno, nei contratti sottoscritti con i propri subappaltatori e subcontraenti apposita clausola con cui ciascuno di essi assume i medesimi obblighi di cui ai punti precedenti.

In riferimento a quanto sopra, l'Appaltatore si impegna a comunicare al Committente qualsiasi variazione successiva in merito alle dichiarazioni rese.

Le Parti dichiarano e riconoscono che il presente articolo si applica nella misura in cui non comporti la violazione del Regolamento (CE) 2271/96 o analoga normativa c.d. "*anti-boycott*" applicabile.

Nel caso di violazione da parte dell'Appaltatore delle dichiarazioni e degli impegni di cui ai precedenti punti del presente articolo, il Committente si riserva la facoltà di risolvere il presente Contratto ai sensi dell'art. 1456 cod. civ.

Articolo 36 – Domicilio delle parti e comunicazioni

Il Committente elegge il proprio domicilio, ai fini amministrativi ed a quelli legali e fiscali, in Roma, Piazza della Croce Rossa, n. 1, C.A.P. 00161; pec fstechnology@pec.fstechnology.it.

L'Appaltatore elegge il proprio domicilio in [•]**,** indirizzo [•]e-mail [•], fax n. [•] pec [•].

Tutte le comunicazioni inerenti al presente Accordo sono validamente effettuate con lettera raccomandata a/r, fax o pec agli indirizzi sopra indicati, fatta salva la comunicazione via e-mail laddove espressamente prevista.

Articolo 37 – Spese di Accordo Quadro, di registro e accessorie a carico dell'Appaltatore

Le Parti convengono espressamente che, ricorrendone i presupposti di legge e nella misura e termini previsti, resta a carico dell'Appaltatore l'assolvimento degli adempimenti fiscali - ivi compresa l'imposta di bollo e di registro - ed i relativi costi connessi alla conclusione del presente Accordo. L'Appaltatore assume, inoltre, l'obbligo di fornire al Committente - entro 5 giorni dalla data del pagamento - prova dell'assolvimento dell'imposta di registro dovuta entro i termini di legge.

L'Appaltatore ha proceduto al pagamento dell'imposta di bollo nei termini di legge (All. **[•]**).

Articolo 38 – Foro competente

Le Parti convengono che le eventuali controversie giudiziarie aventi ad oggetto qualsiasi questione attinente all'esecuzione, alla gestione e/o all'interpretazione del presente Accordo e degli Ordini applicativi saranno deferite in via esclusiva al Foro di Roma.

Il Procuratore

ALLEGATO 1

Dichiarazione dell'Appaltatore ai sensi degli artt. 1341 e 1342 del codice civile l'Appaltatore dichiara di approvare, specificatamente, le clausole contenute nei seguenti articoli dell'Accordo Quadro e delle Condizioni Generali di Contratto per gli Appalti di Forniture delle Società del Gruppo Ferrovie dello Stato Italiane.

DELL'ACCORDO QUADRO

- Articolo 3 - Disciplina applicabile
- Articolo 4 - Oggetto dell'Accordo Quadro;
- Articolo 5 - Durata, Importo e Opzioni dell'Accordo;
- Articolo 6 - Modalità di esecuzione
- **[Eventuale** Articolo 8 - Catalogo elettronico Ariba**]**;
- Articolo 9 - Emissione Ordini applicativi;
- Articolo 10 - Corrispettivi e Revisioni dei prezzi;
- Articolo 11 - Fatturazione e modalità di pagamento;
- Articolo 12 - Tracciabilità dei flussi finanziari;
- Articolo 13 - Obblighi particolari dell'Appaltatore
- Articolo 14 - Cessione dei crediti;
- Articolo 15 - Penali;
- Articolo 16 - Garanzia definitiva;
- Articolo 17 - Recesso;
- Articolo 18 - Clausola risolutiva espressa;
- Articolo 19 - Cessione dell'Accordo Quadro e subappalto;
- Articolo 20 - Trasparenza dei prezzi;
- Articolo 21 - Contratti di lavoro, previdenza e assicurazioni;
- Articolo 22 - Responsabilità dell'Appaltatore;
- Articolo 23 - Diritto di rivalsa;
- Articolo 24 - DURC e manleve;
- Articolo 27 - Clausola integrità e Conflitto interessi;
- Articolo 28 - Tutela della riservatezza;
- Articolo 29 - Divieto di utilizzo di marchi e/o altri segni distintivi di Ferservizi/Gruppo FS
- Articolo 30 - Proprietà intellettuale e garanzia dell'Appaltatore;
- Articolo 31 - Tutela dei dati personali;
- **[eventuale** Articolo 31 bis - Accordo di Data Protection;**]**
- **[eventuale** Articolo 32 - Clausola di non gradimento;**]**
- **[eventuale** Articolo 32 bis - Clausola Sociale;**]**
- Articolo 33 - Sicurezza sui luoghi di lavoro e igiene del lavoro;
- **[eventuale** Articolo 34 - Auditing;**]**
- Articolo 37 - Spese di Accordo Quadro, di registro ed accessorie a carico dell'Appaltatore;
- Articolo 38 - Foro competente.

DELLE "CONDIZIONI GENERALI"

- Articolo 6 - Impegno di riservatezza;
- Articolo 8 - Stipula del contratto e avvio dell'esecuzione della prestazione;
- Articolo 10 - Garanzie;
- Articolo 12 - Prezzi contrattuali;

- Articolo 15 - Cautele antimafia, regolarità contributiva e retributiva, cessione del contratto, subappalto e subcontratti;
- Articolo 19 - Danni per forza maggiore e responsabilità del Fornitore per danni;
- Articolo 20 - Progetti – Disegni e documentazioni tecniche del Committente;
- Articolo 26 - Custodia dei beni di proprietà del Committente;
- Articolo 29 - Divergenze nell'interpretazione e nell'applicazione delle prescrizioni tecniche;
- Articolo 30 - Accesso del fornitore e di suoi dipendenti, ausiliari o collaboratori negli impianti del Committente;
- Articolo 42 - Deposito fiduciario;
- Articolo 43 - Termini contrattuali, sospensione dell'esecuzione del contratto e proroghe;
- Articolo 44 - Illegittima durata delle sospensioni;
- Articolo 50 - Garanzia e sua durata;
- Articolo 54 - Penalità per inadempienze e modalità di computo dei ritardi;
- Articolo 55 - Penali per ritardata o mancata esecuzione e Premi di accelerazione;
- Articolo 57 - Termini e modalità di pagamento;
- Articolo 59 - Recupero di crediti - Compensazione;
- Articolo 60 - Sospensione pagamenti;
- Articolo 63 - Recesso dal contratto;
- Articolo 64 - Transazione e accordo bonario;
- Articolo 65 - Foro competente.

Letto, confermato e sottoscritto.

per l'Appaltatore

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 nome e per conto di FSTechnology S.p.A., nella persona di [●], munito dei necessari poteri per la sottoscrizione del presente Accordo di Data Protection /qui di seguito "**FST**" o "**responsabile**")

E

[*Il Contraente*], con sede legale in [*specificare l'indirizzo della sede legale del Sub Responsabile*], in persona del suo legale rappresentante [*specificare il nome completo del legale rappresentante* (qui di seguito "**altro responsabile**" o "**sub-responsabile**")

PREMESSO

- che l'art. 28 del Regolamento (UE) 2016/679 (di seguito "GDPR") stabilisce che il trattamento di dati personali effettuato per conto di un titolare da parte di un soggetto terzo responsabile del trattamento è disciplinato da un contratto o da altro atto giuridico, vincolante per il responsabile nei confronti del titolare, 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 oltre a dettagliare gli obblighi del responsabile;
- che lo stesso art, 28, al comma 4, stabilisce che *"quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3 [Art. 28], prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento."*
- che nell'ambito della prestazione effettuata da [Il Contraente], relativa allo svolgimento [----------] ("Attività") come specificato nel contratto sottoscritto dalle parti, [*specificare la data del contratto se l'ADP è firmato a posteriori*] (di seguito "Contratto"), [Il Contraente] tratta dati personali; il trattamento di tali dati personali è effettuato da [Il Contraente] per conto di FST e delle Società Titolari del trattamento con cui FST ha stipulato un contratto e un Accordo di Data Protection;
- che l'Accordo di Data Protection tra FST e la/le Società Titolare/i autorizza FST ad avvalersi di altro soggetto esterno alla propria organizzazione cui affidare talune delle attività di trattamento;
- che FST, sulla base di quanto previsto dall'art. 28 del GDPR e dell'autorizzazione della/delle Società Titolare/i, intende avvalersi di [Il Contraente] quale altro responsabile del trattamento o sub-responsabile;
- che la/le Società Titolare/i, determinano i mezzi e le finalità del trattamento dei dati che il Responsabile e il sub-Responsabile svolge per suo/loro conto nell'esecuzione delle Attività,

- che FST nell'ambito di alcune attività previste dal Contratto determina direttamente le finalità e i mezzi del trattamento; pertanto, in tali casi la medesima è qualificata come Titolare del trattamento;
- che [Il Contraente] garantisce requisiti, conoscenze specialistiche, affidabilità e risorse, per attuare misure tecniche e organizzative adeguate che soddisfino i requisiti previsti dal GDPR, compresa la sicurezza del trattamento per garantire la riservatezza e la protezione dei diritti degli interessati;
- che FST e [Il Contraente] (di seguito "le Parti") intendono stipulare un accordo che vincoli, ai sensi dell'art. 28, commi 3 e 4, del GDPR, [Il Contraente] al FST per il trattamento dei dati personali da svolgersi in esecuzione del Contratto.

Tutto ciò premesso, le Parti convengono quanto segue.

ARTICOLO 1: PREMESSE, ALLEGATI E DEFINIZIONI

1. Le premesse e gli allegati al presente accordo formano parte integrante e sostanziale dello stesso anche al fine di meglio precisare gli impegni assunti dalle Parti.
2. Le definizioni contenute nella normativa in materia di protezione dei dati personali e, in particolare, nell'art. 4 del GDPR e nell'art. 2 *quaterdecies* del d.lgs. n.196/03 e s.m.i. si intendono richiamate nel presente Accordo.

ARTICOLO 2: OGGETTO DELL'ACCORDO

1. Le Parti con il presente ADP intendono disciplinare il trattamento dei dati personali da parte di [Il Contraente] in esecuzione del Contratto [*specificare il trattamento di dati personali effettuato nell'ambito dell'oggetto del contratto*], e gli obblighi e i diritti delle Parti.
2. I dettagli del trattamento dei dati personali e le istruzioni operative rispetto alle attività del Sub Responsabile sono specificati nell'Allegato A (Istruzioni). FST si riserva la facoltà di fornire in forma scritta a [Il Contraente] ulteriori istruzioni, nel periodo di vigenza del presente ADP, che costituiranno parte integrante e sostanziale dello stesso e saranno disciplinate a norma del successivo articolo 11. Al riguardo, si evidenzia che FST definisce il livello delle Misure di sicurezza tecniche e organizzative in ottemperanza al Framework di Data Protection del Gruppo FS, anche ai fini di quanto previsto al successivo art. 4, comma 3, lett. c) ed in ottemperanza al Framework di Data Protection del Gruppo FS.

ARTICOLO 3: OBBLIGHI DI FST

1. FST conserva nei confronti della/le Società Titolare/i del trattamento, l'intera responsabilità dell'adempimento degli obblighi conferiti in via specifica al sub-responsabile [Il Contraente].

ARTICOLO 4: OBBLIGHI DEL SUB RESPONSABILE

1. [Il Contraente] effettua il trattamento dei dati personali per conto di FST in conformità alle istruzioni ricevute secondo quanto previsto dall'Art. 2.2 e per lo svolgimento delle attività necessarie per l'esecuzione del Contratto e dei servizi sopra specificati.
2. Qualora [Il Contraente] ritenga che un'istruzione fornita da FST integri una violazione della normativa vigente in materia di trattamento dei dati personali, ed in particolare del GDPR, deve informare immediatamente FST, il quale valuta le osservazioni e adotta le consequenziali determinazioni (riformulazione delle istruzioni fornite ovvero conferma delle stesse con motivazioni in ordine alla determinazione assunta).

3 Con riferimento a quanto previsto dall'art. 28 del GDPR, il [Il Contraente] assicura che:

a) darà completa attuazione delle istruzioni ricevute da FST nel rispetto degli obblighi di cui al Contratto e al presente ADP;
b) solo il personale qualificato, debitamente autorizzato e addestrato tratterà i dati personali ai sensi del presente ADP. Garantisce inoltre che le persone autorizzate all'esecuzione del trattamento dei dati si siano impegnate a garantire la riservatezza delle informazioni gestite o che siano soggette ad un obbligo legale di riservatezza, anche per un periodo ragionevole dopo la fine del rapporto di lavoro intrattenuto con [Il Contraente].

   A tal riguardo [Il Contraente] garantisce che chiunque agisca sotto la sua autorità abbia accesso esclusivamente ai dati personali la cui conoscenza è necessaria per svolgere i compiti assegnati rispetto all'esecuzione del contratto e tratti tali dati secondo specifiche istruzioni ricevute~~,~~ in conformità con la normativa vigente in materia di protezione dei dati personali e il presente ADP. Per l'attuazione dell'obbligo di cui sopra, [Il Contraente] 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.

   [Il Contraente] 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 da [Il Contraente] 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 e gli applicativi su cui opera.

   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 di FST o accertamenti da parte del Garante

   L'operato degli amministratori di sistema è oggetto, con cadenza almeno annuale, ad un'attività di verifica da parte di [Il Contraente], in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza.

   [Il Contraente] deve provvedere al tracciamento dei log degli amministratori di sistema (accessi, creazione delle utenze, assegnazione profili, interventi diretti in tabella, etc.), secondo modalità definite in comune accordo con FST.

   I log devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni

devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;

Entro il primo trimestre di ogni anno [Il Contraente] comunica a FST con apposita comunicazione scritta l'adempimento delle prescrizioni di cui ai citati provvedimenti del Garante.

c) FST fornisce al [Il Contraente], secondo quanto previsto al precedente art. 2, co. 2, le Istruzioni sul Trattamento dei dati comprensive dell'indicazione delle misure di sicurezza tecniche ed organizzative assicurando che queste ultime siano conformi all'allegato B (al livello xx e tipologia xy).

   Il [Il Contraente] garantisce l'adozione delle predette misure impartite dal FST previa verifica, anche con gli eventuali sub-Responsabili, dei livelli di misure di sicurezza previste dal sistema informativo utilizzato a supporto del trattamento.

   Resta fermo che Ciascuna Parte garantisce la sicurezza dei propri sistemi informatici utilizzati per l'esecuzione delle prestazioni oggetto del Contratto (cfr. art. xx "Sicurezza informatica").

   Ogni modifica alle predette misure di sicurezza tecnico-organizzative deve essere autorizzata per iscritto da FST. Nell'applicare il livello appropriato di sicurezza, [*il Contrente*] presta 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.

d) Nell'ambito del presente ADP, FST – quando agisce come Titolare del trattamento – autorizza i sub-Responsabili riportati in allegato al presente accordo (Allegato C); FST – quando agisce come Responsabile del trattamento – si avvale dei medesimi sub-responsabili previa autorizzazione scritta del/i Titolare/i.

   Nel periodo di vigenza del presente ADP [Il Contraente] potrà affidare attività di trattamento ad un altro Responsabile (sub-Responsabile) solo previa autorizzazione scritta – anche generale – del/i Titolare/i, per il tramite della FST, alla quale deve essere inoltrata apposita tempestiva richiesta prima della data prevista per il conferimento dell'incarico al sub-responsabile individuato; dando così al/ai Titolare del trattamento l'opportunità di opporsi a tali modifiche, ex art. 28 del GDPR .

   [Il Contraente] si impegna dunque a:

   - sottoscrivere con il terzo sub-Responsabile individuato, un contratto contenente le prescrizioni sulla protezione dei dati personali per la designazione di quest'ultimo a responsabile del trattamento con riferimento alle operazioni di trattamento,
   - imporre al terzo sub-Responsabile, in qualità di designato responsabile, gli stessi obblighi in materia di protezione dei dati personali contenuti nel presente ADP.

   In particolare, [Il Contraente] garantisce che sub-Responsabile fornisca garanzie sufficienti per attuare le misure tecniche e organizzative appropriate in modo tale che il trattamento soddisfi i requisiti del GDPR.

   Qualora il sub-Responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, [Il Contraente] conserva nei confronti di FST l'intera responsabilità dell'adempimento degli obblighi assunti dal sub-Responsabile.

[Il Contraente] si impegna a fornire l'elenco dei sub-Responsabili, fornito da (Società Responsabile xxx), aggiornato nel continuo come previsto dalle modalità indicate all'interno dell'Allegato C.

e) [Il Contraente], in caso di richieste pervenute a FST che fanno riferimento a dati personali trattati da [Il Contraente] dovrà garantire a FST di poter soddisfare i seguenti diritti degli interessati (artt. 15 e ss. del GDPR):

   i. Diritto di Accesso: [Il Contraente] dovrà collaborare con FST 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 di [Il Contraente].
   ~~ii.~~ Diritto di Cancellazione: [Il Contraente], previa precisa ed esplicita conferma di FST, nel caso in cui ricorrano i presupposti circa la sussistenza del diritto vantato dall'interessato, dovrà cancellare tutti i dati degli interessati richiedenti~~;~~
   iii. Diritto di Portabilità: [Il Contraente] dovrà consentire a FST 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 FST.
   iv. Diritto di Rettifica: [Il Contraente] dovrà garantire a FST la rettifica e/o integrazione dei Dati Personali degli interessati richiedenti.
   v. Diritto di Limitazione: [Il Contraente] dovrà garantire a FST 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.
   vi. Diritto di Opposizione: [Il Contraente] dovrà garantire a FST 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 Contraente] comunica ogni informazione utile al fine di aiutare FST a rispettare i diritti degli interessati entro 3 giorni lavorativi dal ricevimento dell'istanza da parte di FST, al fine di consentire il rispetto dei diritti degli interessati.

Nel caso in cui *[Il Contraente]* riceva direttamente richieste di esercizio dei diritti riconducibili alle operazioni di trattamento di dati effettuate per conto di FST, *[Il Contraente]* provvede a dare tempestiva comunicazione scritta a FST 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.

[Il Contraente] non risponde a richieste degli interessati a meno che non sia autorizzato per iscritto a farlo.

f) Il *[Il Contraente]*, tenendo conto della natura del trattamento e delle informazioni a sua disposizione, assiste inoltre FST nel garantire la conformità a quanto segue:

   i. l'obbligo del/i Titolare/i del trattamento di notificare la violazione dei dati personali al Garante per la Protezione dei Dati Personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le

libertà delle persone fisiche. A tal riguardo [Il Contraente] informa FST di qualsiasi violazione dei dati personali venga 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);

ii. l'obbligo del/i Titolare/i di comunicare la violazione dei dati personali all'interessato senza ingiustificato ritardo, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche; [Il Contraente] supporta FST, con le informazioni in suo possesso circa l'evento accaduto, nella elaborazione della comunicazione all'interessato;

iii. l'obbligo del/i Titolare/i del trattamento di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali; al riguardo [Il Contraente] coopera con FST 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;

iv. l'obbligo del/i Titolare/i del trattamento di consultare il Garante per la Protezione dei Dati Personali, prima del trattamento laddove una valutazione di impatto sulla protezione dei dati indichi che il trattamento comporterebbe un alto rischio in assenza di misure adottate dal titolare del trattamento per mitigare il rischio. In tal caso [Il Contraente] supporta FST nel fornire tutte le informazioni necessarie ai fini della consultazione della competente Autorità di controllo.

g) Alla cessazione del Contratto o del trattamento dei dati per qualsivoglia motivo, [Il Contraente], a scelta di FST, in accordo con il/i Titolare/i, restituisce i dati personali trattati nell'ambito della prestazione dei Servizi e le relative copie ovvero cancella/distrugge tali dati e certifica a FST che ha provveduto in tal senso, a meno che la legislazione non gli impedisca di restituire o distruggere in tutto o in parte tali dati personali. Al riguardo [Il Contraente] garantisce che non procederà più al trattamento di tali dati e assicura l'adozione di misure di sicurezza per la protezione degli stessi.

h) [Il Contraente] rende disponibili a FST tutte le informazioni necessarie a dimostrare il rispetto degli obblighi e delle istruzioni di cui al presente ADP e consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzate da FST o da un altro soggetto da questi autorizzato. In particolare, [Il Contraente], su richiesta di FST ed entro 20 giorni lavorativi dalla medesima, si impegna a presentare le proprie procedure per il trattamento dei dati personali, ivi compreso l'elenco delle persone autorizzate, e a produrre una relazione di conformità dell'operato alla normativa vigente in materia di protezione dei dati personali. [Il Contraente], inoltre, consente a FST l'accesso ai luoghi in cui viene effettuato il trattamento dei dati personali, compresi le strutture fisiche e i sistemi utilizzati e collegati al trattamento. [Il Contraente] collabora con FST nel rispetto di eventuali ordini e richieste emessi dall'Autorità di Controllo o dalle autorità giudiziarie in relazione al trattamento dei dati.

ARTICOLO 5: TRASFERIMENTO DEI DATI PERSONALI VERSO PAESI TERZI

1. È consentito al [Il Contraente] trasferire i dati personali provenienti da FST e dal/i Titolare/i al di fuori dello Spazio economico europeo (SEE) solo previa autorizzazione scritta del Titolare stesso e sulla base delle istruzioni dallo stesso fornite, al fine di garantire che il livello di protezione delle persone interessate previsto dalla normativa vigente in materia di protezione dei dati personali non sia compromesso.

2. Tuttavia, il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali può aver luogo, previa autorizzazione di FST, ai fini anche degli obblighi di informativa nei confronti degli interessati, nel caso in cui la Commissione europea abbia deciso che il Paese Terzo di destinazione garantisce un livello adeguato di protezione.
   Inoltre, a valle della Decisione di Adeguatezza EU-US Data Privacy Framework del 10 luglio 2023, è consentito il trasferimento dei dati personali dall'UE alle società statunitensi che partecipano al EU-US Data Privacy Framework, senza dover predisporre ulteriori garanzie per la protezione dei dati, per esempio senza che sia necessario effettuare un TIA Transfer Impact Assessment ovvero una valutazione dei rischi per la protezione dei dati personali una volta trasferiti al fornitore prescelto e certificato. Le aziende Europee possono verificare e monitorare le certificazioni delle aziende USA rispetto al EU-US Data Privacy Framework, la scadenza della certificazione societaria e la tipologia di dati personali coperti da tale certificazione. A tal fine, è possibile verificare la condizione di adeguatezza societaria sul sito dedicato della Federal Trade Commission degli Stati Uniti: Dataprivacyframework.gov. Pertanto, in assenza della predetta decisione di adeguatezza della Commissione, nonché della predetta certificazione di adeguatezza EU-US Data Privacy Framework, e comunque nell'arco temporale di validità della certificazione stessa, il [Il Contraente] può trasferire dati personali 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).
   Le medesime previsioni si applicano anche agli eventuali sub-responsabili stabiliti negli USA ed il TIA Transfer Impact Assessment sarà sempre effettuato anche quando il [Il Contraente] - ancorché basato in un Paese adeguato o sia certificato ai sensi EU-US Data Privacy Framework USA - utilizzi sub responsabili basati in Paesi non adeguati.

ARTICOLO 6: REGISTRO DEI TRATTAMENTI

1. [Il Contraente] si impegna a mantenere, anche in formato elettronico, un registro di tutte le categorie di attività relative al trattamento svolte ai sensi dell'art. 30 del GDPR e si impegna a produrre copia al Titolare e a FST di quanto riportato all'interno del Registro.

ARTICOLO 7: COOPERAZIONE CON L'AUTORITA' DI CONTROLLO

1. [Il Contraente], FST e il/i Titolare/i cooperano, su richiesta, con l'Autorità di controllo nell'esercizio dei suoi poteri.

ARTICOLO 8: COMUNICAZIONE DEI DATI PERSONALI

1. [Il Contraente] non comunica a terzi i dati personali trattati se non debitamente autorizzato per iscritto da FST.

ARTICOLO 9: ESCLUSIONE DEL TRATTAMENTO ECONOMICO

1. Le Parti convengono che per l'esecuzione delle attività descritte in questo ADP non viene erogato alcun compenso o rimborso, a qualunque titolo, specifico ed ulteriore a [Il Contraente] rispetto a quello previsto nel Contratto; i servizi previsti dal presente ADP, infatti, sono parte integrante del Contratto e pertanto non è dovuta alcuna remunerazione o indennità o rimborso per le attività

qui contemplate ulteriore rispetto a quanto già previsto nel Contratto, in quanto l'intera valutazione economica del rapporto tra FST e [Il Contraente] ed i relativi termini economici del rapporto sono stati debitamente definiti nel Contratto.

ARTICOLO 10: DURATA DELL'ACCORDO

1. Il presente Accordo ha validità dalla data di sottoscrizione delle Parti e per tutta la durata del Contratto stipulato, salve eventuali richieste di proroga di FST assentite per iscritto da [Il Contraente], alla cui validità ed efficacia è direttamente collegato.

ARTICOLO 11: MODIFICHE DELL'ACCORDO

1. Le variazioni dell'oggetto dell'Accordo, ivi comprese quelle conseguenti alle istruzioni previste dall'articolo 2 comma 2, saranno disciplinate dalla clausola del Contratto relativa alle varianti o, in assenza di tale clausola, dalla disciplina normativa applicabile al Contratto medesimo.

ARTICOLO 12: DISPOSIZIONI FINALI

1. Le disposizioni contenute nel Contratto, di cui il presente Accordo costituisce parte integrante e sostanziale, si intendono qui richiamate, se e in quanto applicabili.

ALLEGATI

Allegati:
Allegato A: Istruzioni sulle attività di trattamento oggetto del presente ADP
Allegato B: Misure di sicurezza tecniche ed organizzative;
Allegato C: Elenco Sub-Responsabili.

[*Firme*]

Per *FSTechnology S.p.A.*:

Nome (scritto in forma estesa):

Ruolo: Responsabile del Trattamento

Indirizzo: Roma, Piazza della Croce Rossa n° 1

Firma…….

(timbro dell'azienda)

Per *[Il Contraente]*: Nome (scritto in forma estesa):

Ruolo:

Indirizzo:

Firma…….

(timbro dell'azienda)

ALLEGATO A – ISTRUZIONI SULLE ATTIVITÀ DI TRATTAMENTO OGGETTO DEL PRESENTE ADP

Ruolo di *[Il Contraente]* nel Trattamento

Nome del trattamento	Finalità del trattamento	Descrizione e modalità del trattamento	Periodo di conservazione del trattamento e cancellazione	Presenza di Sub-Responsabili autorizzati (Sì/No)

Categorie di Interessati

I Dati Personali trattati da [Il Contraente] per conto di FST riguardano le seguenti categorie di Dati Personali:

☐ Clienti	☐ Somministrati/Tirocinanti/Stagisti
☐ Prospect	☐ Fornitori
☐ Candidati	☐ Soggetti Terzi
☐Dipendenti	☐ Altro (specificare): _____

Categorie di Dati Personali

I Dati Personali trattati dal Responsabile riguardano le seguenti categorie di Dati Personali:

☐Comuni (anagrafici; di contatto)	☐ Dati di geolocalizzazione
☐ Particolari	☐ Dati di profilazione marketing
☐ Giudiziari	☐ Dati relativi al rapporto di lavoro
☐ Dati di viaggio	☐ Altro (specificare): _____
☐ Dati di videosorveglianza	

Le istruzioni sulle modalità di trattamento sono riportate all'interno del presente documento, fornite dal Titolare di volta in volta in occasione dell'emissione degli ordini di lavoro/ordini applicativi nonché nell'ambito della (eventuale) documentazione di progetto e gestione dello stesso.

Fra le attività previste nel Contratto, le Parti concordano che quelle riportate nella tabella comportano trattamento di dati personali senza escludere che ulteriori trattamenti possano derivare anche da altri servizi, per i quali valgono le istruzioni fornite dal Titolare per come sopra. Il Responsabile è tenuto ad eseguire fedelmente ed esclusivamente le istruzioni impartite dal Titolare, evitando attività di trattamento non conformi alle predette istruzioni o volte a perseguire finalità diverse da quelle correlate all'esecuzione del Contratto.

ALLEGATO B – MISURE TECNICHE E ORGANIZZATIVE DI SICUREZZA LIVELLO xx (indicare tipologia)

[Riportare tabella misure tecniche ed organizzative]

ALLEGATO C – ELENCO SUB-RESPONSABILI

ID	Sub-Responsabile	Descrizione attività	Location

L'elenco dei sub-Responsabili è aggiornato e notificato da [Il Contraente] attraverso le modalità di cui all'art. xx del Contratto "…".

Nel caso in cui il Titolare non si opponesse entro 30 giorni dalla notifica da parte del Responsabile dell'aggiunta o sostituzione di sub responsabile/i di cui all'All. C, il/i sub-Responsabile/i si riterrà approvato/i..