Provincia di Vicenza
COMUNE DI SANDRIGO

Piazza G. Matteotti 10 – 36066 Sandrigo (VI)
P. IVA 00516260247 C.F. 95026510248
www.comune.sandrigo.vi.it PEC sandrigo.vi@cert.ip-veneto.net

Finanziato dall'Unione Europea
NextGenerationEU

SCHEDA TECNICA

GARA D'APPALTO PER LA REALIZZAZIONE DEL PROGETTO SECONDO LE INDICAZIONI DI CUI ALL'AVVISO DI INVESTIMENTO 1.2 "ABILITAZIONE AL CLOUD PER LE PA LOCALI" - FINANZIATO DALL'UNIONE EUROPEA – NEXT GENERATION EU

CUP ASSEGNATO AL PROGETTO: B51C22001500006
CIG ASSEGNATO AL PROGETTO: A01E66DA18

1.MIGRAZIONE AL CLOUD

L'appalto riguarda l'implementazione di un Piano di migrazione al cloud (comprensivo delle attività di assessment, pianificazione della migrazione, esecuzione e completamento della migrazione, formazione) delle basi dati e delle applicazioni e servizi dell'amministrazione in modalità indicati al successivo punto 2 in modalità Paas (Platform as a Service), a valere sui finanziamenti erogati dal PNRR.

L'esecuzione della fornitura si conforma necessariamente alle prescrizioni contenute:

1) Nelle "Raccomandazioni tecniche per la corretta attuazione delle strategie di cui all'Avviso Pubblico Missione 1 Componente 1 del PNRR, finanziato dall'Unione europea nel contesto dell'iniziativa NextGenerationEU, Investimento 1.2 ABILITAZIONE AL CLOUD PER LE PA LOCALI", emanate dalla Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale, che sono parte integrante e sostanziale del presente documento.

2) "Linee guida per i Soggetti attuatori individuati tramite Avvisi Pubblici a lump sum" reperibili al seguente indirizzo "https://assets.innovazione.gov.it/1694769112-zip-llgg-innovazione_20230830.zip", e successive modifiche, che sono parte integrante e sostanziale del presente documento.

L'Affidatario dovrà effettuare la migrazione avvalendosi del modello di migrazione come delineato nella Strategia Nazionale per il Cloud indicato con la dicitura "Aggiornamento in sicurezza di applicazioni in Cloud (repurchase/replatform)".

2. SERVIZI OGGETTO DI MIGRAZIONE

Si riporta di seguito la tabella contenente l'elenco dei servizi oggetto della migrazione, con il nome del servizio da migrare e la relativa tipologia di migrazione selezionata. La migrazione deve essere fatta per tutti gli applicativi, database e sistemi utilizzati per l'erogazione del/dei servizi di seguito indicati:

Servizio Applicativo	Modalità di migrazione	Servizio richiesto con la domanda per l'avviso della Misura 1.2
DEMOGRAFICI - ANAGRAFE	Attività da avviare	B - Aggiornamento in sicurezza di applicazioni in cloud
DEMOGRAFICI – STATO CIVILE	Attività da avviare	B - Aggiornamento in sicurezza di applicazioni in cloud
DEMOGRAFICI - LEVA MILITARE	Attività da avviare	B - Aggiornamento in sicurezza di applicazioni in cloud
DEMOGRAFICI - GIUDICI POPOLARI	Attività da avviare	B - Aggiornamento in sicurezza di applicazioni in cloud
DEMOGRAFICI - ELETTORALE	Attività da avviare	B - Aggiornamento in sicurezza di applicazioni in cloud
STATISTICA	Attività da avviare	B - Aggiornamento in sicurezza di applicazioni in cloud
PROTOCOLLO	Attività da avviare	B - Aggiornamento in sicurezza di applicazioni in cloud
ALBO PRETORIO	Attività da avviare	B - Aggiornamento in sicurezza di applicazioni in cloud
CONTABILITA' E RAGIONERIA	Attività da avviare	B - Aggiornamento in sicurezza di applicazioni in cloud
ECONOMATO	Attività da avviare	B - Aggiornamento in sicurezza di applicazioni in cloud
TRIBUTI MAGGIORI	Attività da avviare	B - Aggiornamento in sicurezza di applicazioni in cloud
GESTIONE ECONOMICA	Attività da avviare	B - Aggiornamento in sicurezza di applicazioni in cloud
NOTIFICHE	Attività da avviare	B - Aggiornamento in sicurezza di applicazioni in cloud
ORDINANZE	Attività da avviare	B - Aggiornamento in sicurezza di applicazioni in cloud

La soluzione proposta deve essere già qualificata da AgID e pubblicata nel cloud Marketplace della PA, quindi dovrà essere conforme a una serie di requisiti organizzativi, di sicurezza, di performance e scalabilità, interoperabilità e portabilità fissati dalle circolari Agid n. 2 e n. 3 del 9 aprile 2018.

3. REQUISITI

È richiesto che il CSP (Cloud Solution Provider) qualificato offerto fornisca sufficienti garanzie relativamente al regolamento Ue 2016/679, noto come GDPR (General Data Protection Regulation).

È fondamentale che il CSP sia compliant con la checklist DNSH (Do No Significant Harm) consultabile tramite l'allegato 4 dell'Avviso 1.2, a pena dell'irricevibilità dell'offerta tecnica proposta.

Il CSP dovrà rispettare i principi di liceità, correttezza e trasparenza, oltre che di data protection-by-design, necessità e minimizzazione. Il trattamento di dati personali da parte del CSP dovrà avvenire sulla base di un'adeguata base giuridica e dovrà prevedere un periodo di data retention coerente con la finalità del trattamento.

È opportuno che l'offerta tecnica evidenzi gli aspetti relativi:

- **all'ubicazione dei dati nel data center del CSP** evidenziando eventuali trasferimenti elaborativi extra-UE che non prevedono lo storage del dato in territori extra-UE (ad esempio, per la presenza di subappaltatori del CSP per servizi ancillari es. trouble-shooting, assistenza);
- all'esistenza di eventuali impegni del CSP alla conservazione dei dati in determinate "regional zones", onde evitare di incorrere in trasferimenti transfrontalieri di dati personali;
- alla possibilità e alle modalità, da parte del CSP, di monitorare l'utilizzo dei servizi cloud richiesti, nei casi in cui tale controllo comporti l'accesso a dati personali, il trasferimento di dati diagnostici, dati su incidenti di sicurezza e telemetria;
- **alla verifica di un processo strutturato di gestione della continuità operativa (Business Continuity)** in linea con standard internazionali come la ISO 22301;
- **alla verifica delle policy di sicurezza implementate dal CSP ed in linea con standard di sicurezza** (ad esempio, ISO 27001, 27017, 27018) o sulla base di certificazioni rilasciate da organismi indipendenti;
- alla verifica di meccanismi e soluzioni di crittografia che garantiscano la cifratura del dato a riposo (Data Encryption at rest) ed in transito (End-to-End Encryption);
- alla rilevazione e alla segnalazione di data breach;
- alla data retention da parte del CSP (in caso di cessazione del contratto, ovvero per esigenze regolatorie o di enforcement);
- alla data portability in caso di migrazione dei dati ad altro CSP. Si richiede infatti che i dati vengano resi disponibili in formati aperti alla luce della portabilità dei dati personali garantita all'interessato dal GDPR.

Con riferimento ai requisiti sopra elencati, si richiedere un rapporto dettagliato, in relazione alle garanzie e certificazioni offerte dal CSP selezionato.

4. IMPLEMENTAZIONE DEL SISTEMA

Le componenti applicative dovranno essere percepite dagli utilizzatori come parti di un sistema unico. L'interfaccia utente e la logica di funzionamento del sistema dovranno essere quindi omogenei all'intera soluzione applicativa, che pertanto dovrà presentare maschere, modalità operative, parametri, tasti funzione ecc. tra loro congruenti e consistenti, indipendentemente dalle funzionalità associate. Il termine "integrato" indica che le informazioni sono gestite una sola volta ed in un solo modo, cioè a livello sufficientemente dettagliato da poter essere utilizzate per le diverse finalità necessarie alle aree coinvolte. Si richiede di eliminare ridondanze e duplicazioni nei dati al fine di garantire unicità dei dati e delle funzioni gestite in ogni singolo insieme rispetto al sistema integrato.

5. SERVIZI PROFESSIONALI DI ASSISTENZA E SUPPORTO ORGANIZZATIVO

Al fine di supportare l'Ente nelle attività di Abilitazione al Cloud sono previsti un insieme di servizi professionali di assistenza e supporto organizzativo.

L'Affidatario sarà tenuto all'erogazione dei servizi in conformità ai processi, alle procedure ed alle responsabilità attribuite secondo le direttive dell'Amministrazione, che verranno definite e condivise nella fase di avvio della fornitura, nonché aggiornate durante il corso del contratto esecutivo in funzione delle eventuali evoluzioni.

L'Affidatario deve garantire la non regressione funzionale e il miglioramento -o almeno mantenimento- dei livelli di qualità del software/servizio nel tempo.

6. PHASE OUT

All'approssimarsi della scadenza del contratto ed in mancanza di rinnovo, o in caso di esplicita comunicazione, da parte dell'Ente, di passaggio ad altro Affidatario, o in caso di revoca della qualificazione da parte dell'AgID, l'Affidatario dovrà garantire (a titolo gratuito) il corretto svolgimento di tutte le seguenti azioni, volte ad assicurare una corretta e trasparente transizione verso il nuovo scenario:

- rilasciare, in formato aperto e tecnologicamente adeguato alle successive operazioni di import nei database del nuovo sistema, tutti i dati a qualunque titolo trattati;
- rilasciare tutti i log necessari ai fini della tracciabilità delle operazioni effettuate dagli utenti del sistema;
- rilasciare tutte le statistiche ed i report relativi al monitoraggio delle performance e dello status del sistema;
- fornire, per una durata di tempo congrua (da concordare con il Soggetto Attuatore e che potrà estendersi anche oltre la data di switch effettivo), adeguato supporto e formazione al personale del Soggetto Attuatore e/o del nuovo Affidatario in merito a tutto quanto sia necessario conoscere ed attuare per assicurare il corretto funzionamento dell'intero sistema nel nuovo scenario.

In aggiunta, qualora l'Affidatario dovesse risultare inadempiente all'esecuzione corretta e tempestiva delle attività indicate, ovvero non garantisca la prosecuzione efficace ed in continuità dei servizi, l'Amministrazione si riserva di non riconoscere i corrispettivi dei servizi erogati nel periodo di transizione in uscita.

Inoltre, al fine di prevenire e contrastare il fenomeno del vendor lock-in, l'Affidatario deve garantire il rispetto dei requisiti di interoperabilità e portabilità (RIP) contenuti nella Circolare n. 2 e nella Circolare n.3 dell'AgID del 9 Aprile 2018, di seguito riportati.

Requisiti IaaS e PaaS (Circolare n. 2):

- RIP1 - I servizi IaaS/PaaS espongono opportune Application Programming Interface (API) di tipo SOAP e/o REST associate alle funzionalità del servizio e alle procedure di gestione e configurazione del servizio;
- RIP2 - Il Fornitore Cloud rende disponibile una adeguata documentazione tecnica delle API che ne chiarisce l'utilizzo;
- RIP3 - In caso di aggiornamento delle funzionalità del servizio e/o delle relative API il Fornitore Cloud garantisce la tracciabilità delle diverse versioni delle API disponibili, allo scopo di consentire evoluzioni non distruttive (versioning). Anche la documentazione tecnica delle API dovrà essere tempestivamente aggiornata;
- RIP4 - Il Fornitore Cloud garantisce la possibilità di tracciare le richieste SOAP/REST ricevute dal servizio e il loro esito (logging e accounting), anche al fine della non ripudiabilità della comunicazione;
- RIP5 - Il Fornitore Cloud garantisce all'Acquirente la possibilità di estrarre in qualsiasi momento una copia completa dei dati e metadati memorizzati (in formato pubblico e aperto) come, a titolo esemplificativo ma non esaustivo: volumi, object e block storage, dump di DB, ecc.

7. INSTALLAZIONE SERVIZI CLOUD IN MODALITÀ PaaS

L'ammissibilità degli interventi di migrazione è disciplinata dall'art. 6 ("Interventi finanziabili") dell'avviso di Investimento 1.2 "Abilitazione al cloud per le PA Locali" e dai suoi allegati.

In caso di trasferimento di applicazioni e dati dalla situazione di on-premise strutturato verso una delle tre modalità cloud disponibili (IaaS, Paas o SaaS), le attività di installazione dovranno essere eseguite seguendo un piano di installazione/manutenzione dei servizi condiviso con l'Amministrazione, nel quale sono da tenere in considerazione:

- gli interventi effettuati in intervalli orari definiti con l'Amministrazione e coerentemente con le proprie esigenze di operatività;
- la garanzia di operatività del servizio anche durante la fase intermedia di test e collaudo;
- l'impatto delle attività di roll-out e installazione sulla normale operatività. Tale impatto dovrà essere ridotto al minimo. In caso di disservizio, l'Affidatario dovrà adoperarsi per garantire il ripristino immediato della condizione preesistente (procedura di roll-back).

Una volta eseguita l'installazione sul nuovo ambiente in cloud è necessario effettuare i test di funzionamento prima della messa in produzione così così da garantire che tutti i dati siano stati effettivamente migrati correttamente.

Al fine di verificare la corretta erogazione dei servizi e la costante adeguatezza delle soluzioni scelte si richiede l'impegno dell'Affidatario ad eseguire dei test al fine di garantire il tempestivo ripristino ove necessario.

8. MIGRAZIONE DEI SERVIZI IN AMBIENTE CLOUD

Nell'ambito dell'Avviso di Investimento 1.2 "Abilitazione al cloud per le PA Locali - Allegato 2 – Definizione dei Servizi e modalità di migrazione", per ogni servizio migrato, è necessario che il Questionario di Assessment venga compilato dall'Ente con il supporto dell'Affidatario contrattualizzato a processo di migrazione iniziato.

A tal fine l'Affidatario dovrà farsi carico di tutte le attività necessarie alla migrazione e alla progettazione del processo di migrazione per ogni servizio candidato alla migrazione in cloud. Questa è una fase ricorsiva per ogni applicazione/servizio e incrementale, di modo che si possa verificare che le applicazioni/servizio funzionino correttamente, una volta migrate.

Nel rispetto della continuità del servizio, è necessario garantire il massimo parallelismo delle attività al fine di minimizzare i tempi di migrazione/attivazione. Le operazioni di trasferimento in cloud dovranno essere completate in massimo 24 ore dal momento del fermo dell'operatività dell'Amministrazione.

9. SERVIZI DI MANUTENZIONE SISTEMISTICA SULLA PIATTAFORME DI SERVIZI

All'Affidatario è richiesto che, terminata l'implementazione del Piano di migrazione al cloud delle basi dati, delle applicazioni e dei servizi dell'amministrazione, sia effettuata l'ottimizzazione ed il fine tuning dei parametri di configurazione dell'ambiente cloud in funzione dei dati di carico a disposizione, dei test effettuati e delle prime attività d'esercizio. Lo svolgimento dell'attività di fine-tuning si rende necessaria a garantire, nell'esercizio quotidiano, le prestazioni ottimali per i servizi applicativi, le riconfigurazioni ambientali (processi, priorità ecc.) e le attività di riorganizzazione delle basi di dati, dei file system e, se necessario, di un giusto dimensionamento delle risorse computazionali anche in un'ottica di risparmio economico.

Nell'ambito dei Servizi di manutenzione sistemistica e per tutti i servizi IaaS, PaaS o SaaS previsti in fornitura, il Fornitore dovrà erogare i servizi di gestione sistemistica.

Il servizio di gestione in ambito sistemistico riguarda la gestione di tutti gli elementi/apparati/sistemi sopra descritti, mediante la disponibilità continuativa di risorse del Fornitore, durante l'orario corrispondente contrattualizzato. Il servizio include tutte le attività necessarie per prendere in carico, condurre e mantenere sempre efficiente l'infrastruttura dei sistemi server. A titolo indicativo e non esaustivo, nel seguito vengono descritte alcune delle attività minime che il Fornitore dovrà svolgere, distinte fra interventi svolti autonomamente (in maniera continuativa e proattiva) e interventi di gestione a richiesta dell'Amministrazione:

1. Attività svolte autonomamente dal Fornitore:
    a. installazione di patch, hot fix e service pack relativi a tutte le componenti software in gestione, inclusiva di: costante monitoraggio dei rilasci; verifica preventiva dell'applicabilità di tali patch nell'ambiente dell'Amministrazione e valutazione del loro impatto; richiesta delle patch/hot fix qualora non disponibili; definizione di un piano di installazione concordato con l'Amministrazione (date ed ambiti di intervento); predisposizione di apposite procedure di salvataggio;
    b. ● cambiamenti di configurazione, con particolare riferimento alle regole di sicurezza informatica, da concordare con l'Amministrazione a seguito di cambi di policy, nuove regole di sicurezza, modificazione nell'allocazione delle risorse per l'ottimizzazione delle prestazioni o altre motivazioni che dovessero emergere dall'attività di conduzione e monitoraggio, secondo le modalità previste dal processo di change management;
    c. ● amministrazione dei sistemi e settaggio di configurazioni del sistema operativo e dei servizi infrastrutturali attivi, amministrazione delle macchine virtuali;
    d. ● elaborazioni batch e schedulazione;
    e. ● amministrazione utenti a livello sistema operativo;
    f. ● monitoraggio, raccolta e storicizzazione dei valori del carico dei server della disponibilità, della capacità, dell'utilizzo e delle performance dei sistemi su base oraria, giornaliera e mensile, allo scopo di garantire l'efficienza di tutte le componenti (CPU, memorie, BUS di sistema e dispositivi di I/O), al fine di determinare possibili aree di inefficienza o colli di bottiglia dell'intera infrastruttura, definendo soglie di utilizzo delle risorse ed intervenendo prontamente a fronte di eventuali malfunzionamenti;
    g. ● monitoraggio dello scanner per la sicurezza dei sistemi e la protezione da virus;
    h. ● monitoraggio delle security policy;
    i. ● capacity planning volto alla determinazione e alla messa in esercizio di configurazioni adeguate per ogni componente dei server virtualizzati;

10. PROTEZIONE DATI PERSONALI

Il servizio/servizi dovrà prevedere, in ottemperanza di disposizioni e/o provvedimenti normativi sulla protezione dei dati personali, sistemi di gestione, configurazione, monitoraggio, meccanismi di autenticazione, autorizzazione e profilatura per l'accesso alle funzionalità previste, ai dati e ai file trattati.

Particolare attenzione dovrà essere assicurata per la gestione di informazioni di carattere sensibile, per le quali sarà garantita una soluzione che comporti il pieno rispetto della normativa sopra citata e della ulteriore normativa di settore applicabile.

All'affidatario compete la responsabilità di assicurare la sicurezza sia fisica che logica lungo tutto il ciclo di vita delle informazioni e per tutta la durata del contratto, vigilandone l'effettiva attuazione ed efficacia nel rispetto dei requisiti di sicurezza ai sensi dell'art. 28 del regolamento ue 2016/679 (gdpr), costituenti parte integrante del contratto di appalto.

11. REQUISITI MINIMI DI SICUREZZA

I servizi oggetto di migrazione dovranno rispettare i requisiti di riservatezza, autenticità, integrità, e disponibilità.

Nell'ambito dell'erogazione del servizio di sicurezza ICT, l'Affidatario è deputato all'analisi e verifica dei livelli di sicurezza complessiva dell'architettura e della valutazione di eventuali azioni di perfezionamento della security stessa.

L'Affidatario dovrà mettere in campo tutte le contromisure di tipo tecnologico volte alla difesa perimetrale e di contenuto del servizio migrato ed in particolare:

- attuare la politica per la sicurezza ai flussi di rete in termini di tipo e/o contenuto del traffico;
- monitorare e verificare l'efficacia delle misure di sicurezza adottate per i flussi di rete;
- valutare e gestire il rischio associato alle minacce di tipo informatico;
- utilizzare strumenti tecnologici e competenze per affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza;
- attuare una risoluzione reattiva o proattiva di incidenti di sicurezza;
- attività di updating e upgrading delle versioni dei prodotti di sicurezza;
- backup dei log e delle configurazioni.

Tuttavia, considerando la responsabilità generale dell'Affidatario di mantenere i sistemi in perfetta efficienza, risulta evidente che le attività di rilevazione e di bonifica delle vulnerabilità potranno essere svolte anche in modo autonomo, indipendentemente dall'attività di verifica da parte dell'Ente.

12. BACK-UP E RESTORE

L'Affidatario dovrà prevedere, per ciascuno dei servizi offerti, l'attivazione delle rispettive funzionalità di backup e restore. L'offerta tecnica dovrà prevedere al minimo: le procedure automatiche di copia e salvataggio delle configurazioni operative in un ambiente protetto mediante l'utilizzo di supporti esterni; la conseguente possibilità di ripristinarne i contenuti in caso di indisponibilità/danneggiamento dei contenuti negli ambienti operativi. L'Affidatario ha facoltà di proporre gli strumenti che ritiene più idonei per il raggiungimento degli obiettivi dichiarati.

L'Affidatario, nelle fasi iniziali (periodo di transizione iniziale), verificherà l'infrastruttura e le policy di backup e restore esistenti, concorderà con l'Ente eventuali variazioni delle policy dove queste non siano più ritenute adeguate. Si occuperà di implementare le nuove policy di backup concordate, compatibilmente con l'infrastruttura di backup messa a disposizione sul Cloud, provvedendo alla documentazione ed all'aggiornamento delle procedure di dettaglio utilizzate per il backup ed il restore dei dati.

13. DISASTER RECOVERY E BUSINESS CONTINUITY

L'Affidatario dovrà redigere un Piano di disaster recovery nel quale descriverà le strategie attuate, tra quelle previste dal paragrafo 5.3.10 "Disaster recovery" del Manuale di Abilitazione al Cloud. Le procedure di backup e restore dovranno essere accuratamente progettate e documentate e dovranno tenere conto della mole di dati da trattare e del tempo necessario per le operazioni. L'Affidatario dovrà, periodicamente, verificare e attuare le procedure, in modo tale da garantire il loro corretto funzionamento in ogni dato momento.

14. QUESTIONARIO DI ASSESSMENT

Il Questionario di Assessment, previsto dall'Avviso 1.2 di Migrazione al cloud, ha lo scopo di raccogliere le informazioni circa lo stato di avanzamento della migrazione e creare una modalità di rappresentazione sintetica dell'avanzamento delle attività. La sua corretta compilazione ed il puntuale aggiornamento fino alla conclusione delle attività rappresentano un onere che l'Affidatario assume per supportare il Soggetto Attuatore per la compilazione degli aspetti tecnici del questionario al fine di permettere di tenere traccia dello stato di esecuzione dei lavori. I Servizi identificati nel Questionario di Assessment devono corrispondere con i servizi affidati all'Affidatario. Per ogni servizio devono essere elencati tutti gli applicativi ad esso associati e oggetto di migrazione.

Deve essere compilato a processo di migrazione iniziato per ogni servizio oggetto di affidamento alla migrazione, deve essere periodicamente aggiornato ogni volta intercorre un evento significativo rispetto al contenuto tracciante del questionario. Alla conclusione del processo di migrazione il questionario conterrà lo stato "Completato" rispetto ai singoli servizi.

15. FORM DI CONFORMITA' ALLA MIGRAZIONE

Il Form di Conformità della migrazione, definito nell' "Allegato 1 - Completamento delle attività e verifiche tecniche Avvisi 1.2" alle "Linee Guida per i Soggetti attuatori individuati tramite AVVISI PUBBLICI A LUMP SUM" rappresenta il modello di form che deve essere utilizzato dal Soggetto Attuatore, ovvero la Stazione Appaltante, per fornire le informazioni richieste dall'asseveratore alla conclusione del processo di Migrazione al Cloud.

Esso consiste in un Form per l'indicazione di dati e documenti necessari all'Asseveramento della "Migrazione per "Aggiornamento in Sicurezza di applicazioni in Cloud" di tipo replatform, ovvero migrazione di un servizio applicativo ad un PaaS qualificato;

Si chiede all'Affidatario di assistere la stazione appaltante nella compilazione di tale form al fine del raggiungimento di un giudizio positivo all'Asseveramento.

16. DURATA E SCADENZE

Al fine di rispettare il suddetto cronoprogramma, tenuto conto dei tempi per l'asseverazione da parte dell'Unità di Missione del PNRR del Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei Ministri (d'ora in poi DTD) e l'eventuale richiesta di modifiche, **il termine per l'esecuzione del progetto è fissato al 30/06/2024.**

Le attività si intendono concluse al momento in cui:

- il software e gli eventuali servizi selezionati in fase di adesione risultano disponibili online, configurati, personalizzati e completi dei dati forniti dall'Amministrazione,
- è stata compilata la checklist di conformità indicata nel paragrafo "Verifica della conformità" dell'Avviso in questione.

17. CONSIDERAZIONI FINALI

Per tutto quanto non previsto nella presente scheda tecnica per il raggiungimento dell'obiettivo di finanziamento a valere sul PIANO NAZIONALE DI RIPRESA E RESILIENZA - MISSIONE 1 - COMPONENTE 1 –AVVISO DI INVESTIMENTO 1.2 "ABILITAZIONE AL CLOUD PER LE PA LOCALI" fa fede quanto previsto dall'avviso di pari oggetto e relativi allegati emanati dalla Presidenza del Consiglio dei Ministri - Dipartimento per la Trasformazione Digitale.