Proposta Tecnico Economica

SR/190471

DESTINATARIO:
Amministrazione Comunale di Cremona
Alla c.a. del Segretario Generale dr.ssa G. Di Girolamo

DATA EMISSIONE 19/08/2021- **RIFERIMENTO** SR/190471

OGGETTO
Soluzione Saas jEnte - Jpartecipate

RIFERIMENTO MUNICIPIA PER ASPETTI ECONOMICI
Cesare Rovati
e-mail cesare.rovati@eng.it
mobile 3462359608
RIFERIMENTO MUNICIPIA PER ASPETTI TECNICI
Roberto Blasioli
e-mail roberto.blasioli@eng.it
mobile 3492712085

MUNICIPIA

Municipia Spa
Il Procuratore
Firmato digitalmente da: MICHELE LANGELLA
Data: 20/08/2021 09:39:36

CAPITOLO 1

PROPOSTA ECONOMICA	
DESCRIZIONE SOLUZIONE SAAS	**IMPORTO**
JPARTECIPATE • Servizi di avviamento	€ 17.600,00
• Canone di manutenzione primo anno (durata 12 mesi) MODULO BILANCIO CONSOLIDATO	€ 3.500,00
• Canone di manutenzione primo anno (durata 12 mesi) MODULO GESTIONE PARTECIPATE •	€ 3.500,00
• Counseling bilancio consolidato	€ 5.000,00
TOTALE	**€ 29.600,00**

Gli importi sopra indicati sono da considerarsi al netto di IVA.

Ai sensi dell'art. 26 comma 6 del D. Lgs. 81/2008 Municipia Spa dichiara che i costi generali per la sicurezza del lavoro sono già inclusi nei prezzi sopra indicati e sono pari a 1,68 € giorno uomo. Inoltre i costi per la sicurezza per ridurre i rischi da interferenza sono pari a 0,00€ vista la tipologia intellettuale dell'attività oggetto della fornitura (art.26 comma 5 del D. Lgs. 81/2008).

MODULO D'ORDINE

PER VALIDARE L'ORDINE QUESTO MODULO DEVE ESSERE COMPILATO E FIRMATO IN TUTTE LE SUE PARTI

L' Ente / Azienda: Comune di Cremona

P.I. 00297960197 PEC: protocollo@comunedicremona.legalmail.it

Richiede a Municipia Spa di accedere ai servizi / soluzioni indicati nel capitolo 1 Proposta Economica (laddove presenti caselle da barrare, selezionare la scelta) e relativa/e ai contenuti tecnici descritti più avanti al Capitolo 2 Proposta Tecnica

In allegato delibera/determina	Importo al netto IVA	CIG	Codice Univoco Ufficio
N°_____ del _____			

Si specifica che in caso di mancata sottoscrizione del presente modulo che contempla anche la sottoscrizione dell'accordo per il trattamento dei dati, Municipia non potrà proseguire detto trattamento.

Luogo e Data

FIRMA QUI

Firma del Cliente per espressa accettazione di quanto sopra

Il Cliente dichiara altresì di approvare espressamente anche ai sensi degli art. 1341 e 1342 c.c. tutti gli articoli compresi nei capitoli 1. Proposta economica – 2. Proposta Tecnica - 3. Condizioni Specifiche di fornitura – 4. Condizioni Generali di Vendita della presente proposta tecnico economica inclusi gli allegati di riferimento (appendici privacy).

Luogo e Data

FIRMA QUI

Firma del Cliente per espressa accettazione di quanto sopra

CAPITOLO 2

PROPOSTA TECNICA

CARATTERISTICHE DELLA SOLUZIONE SAAS: jEnte - Jpartecipate

La descrizione delle caratteristiche del servizio viene distinta tra le peculiarità funzionali della soluzione d'interesse e quelle invece legate ai servizi accessori connessi all'avviamento degli applicativi e all'infrastruttura tecnologica.

Le **caratteristiche funzionali** del servizio sono descritte negli allegati tecnici che costituiscono parte integrante della presente proposta:

- Gestione Partecipate

Le **caratteristiche funzionali** del servizio di Counseling vengono sotto descritte:

- Individuazione dell'area di consolidamento con esame degli statuti, eventuali patti parasociali e contratti di servizio
- Predisposizione delle linee guida della Capogruppo da inviare alle Società e agli Enti compresi nell'area di consolidamento per la predisposizione del bilancio consolidato
- Identificazione delle operazioni infragruppo, elisione delle stesse e relative scritture contabili di consolidamento
- Redazione dei documenti che costituiscono il fascicolo completo del bilancio consolidato: stato patrimoniale e conto economico consolidati e nota integrativa consolidata

Le **caratteristiche dei servizi connessi all'avviamento, alla manutenzione e all'assistenza e a quelli legati dell'infrastruttura tecnologica** sono descritte qui di seguito:

SERVIZI DI ATTIVAZIONE

Comprendono tutte le attività dello staff tecnico di Municipia, erogate per via telematica per l'attivazione dei moduli della soluzione oggetto della presente fornitura. L'attività consiste nella istanziazione del tenant e della sua configurazione di base. Viene rilasciata la password di accesso in qualità di Utente Master per l'attivazione di ulteriori utenze e la configurazione delle funzionalità dell'applicazione per l'erogazione dei servizi previsti.

SERVIZI OPZIONALI CONNESSI ALL'AVVIAMENTO

Comprendono tutte le attività dello staff tecnico di Municipia, erogate per via telematica, per la configurazione, l'eventuale popolamento delle banche dati anagrafiche di riferimento e ad affiancare gli Uffici nella fase di avviamento operativo delle nuove procedure.
Tali attività hanno l'obiettivo di rendere pienamente operativo il software acquisito in tutte le sue funzionalità.
Di seguito la descrizione delle attività tipiche dei servizi opzionali di avviamento.

Recupero dati e migrazione

Nell'ambito della fornitura sono svolte le attività riferite al recupero dei dati dalla procedura in uso presso l'Ente per la successiva migrazione degli stessi nell'applicativo oggetto della presente proposta.
I dati da migrare devono essere forniti a cura dell'Ente, sulla base del tracciato standard definito da Municipia che sarà inoltrato all'Ente in caso di adesione a questa offerta.
Saranno svolte le seguenti attività:

- Esplorazione e valutazione dei dati sorgente ricevuti
- Migrazione
- Esecuzione primo test ed eventuali affinamenti
- Esecuzione secondo test per ulteriori affinamenti

Le attività di ripresa dati e migrazione dovranno essere svolte in via preventiva alla formazione in modo da poter effettuare la stessa sui dati reali dell'Ente ed essere condotta contestualmente ad una ulteriore fase di verifica e correttezza della fase di recupero dati.
Non sono ricomprese in tale attività operazioni di bonifica delle informazioni per incompletezza e/o inesattezza delle stesse, per le quali è possibile attivare, separatamente, ulteriori servizi professionali
Parte integrante dell'attività è la definitiva configurazione del software per renderlo operativo secondo le sue funzionalità standard.

Formazione

La formazione è articolata in modo tale da consentire agli operatori dell'Ente di acquisire le principali competenze necessarie all'utilizzo delle varie funzionalità presenti negli applicativi forniti.
Sarà effettuata attraverso sessioni di accompagnamento erogate da remoto e strumenti di formazione a distanza.
I formatori hanno tutti i requisiti necessari per lo svolgimento di questa attività: alta professionalità, esperienza e competenza nelle materie da trattare, approfondite competenze applicative, capacità di condurre un corso di formazione specialistico.

Supporto e Start-up
Per la messa in produzione del servizio è possibile avere il supporto a distanza di un team formato da personale qualificato con elevati skill ed esperienza nell'avviamento di servizi come quello oggetto del contratto.

SERVIZI CONNESSI ALLA MANUTENZIONE E ASSISTENZA E ALL'INFRASTRUTTURA TECNOLOGICA

MANUTENZIONE E ASSISTENZA

Per i servizi erogati in SaaS sono previste le attività di manutenzione e assistenza per le sole annualità oggetto della fornitura contemplata nella presente proposta.
Di seguito sono descritte le caratteristiche della manutenzione effettuata sugli applicativi al fine di garantirne il corretto funzionamento; sono anche indicate le modalità di rilascio degli aggiornamenti.

MANUTENZIONE CORRETTIVA

La **manutenzione correttiva** del software è in rapporto diretto con la soddisfazione dei clienti, in quanto ha l'obiettivo di assicurare la continuità e la correttezza di funzionamento dell'applicativo utilizzato nell'operatività quotidiana. La presenza di un malfunzionamento rappresenta infatti un elemento di forte criticità rispetto alla qualità e quindi, per Municipia, è di fondamentale importanza organizzare con efficienza i processi per la gestione delle segnalazioni di ogni anomalia e per la loro risoluzione, così da fornire riscontri tempestivi ed efficaci in merito alla soluzione.

La metodologia applicata da Municipia segue due approcci:

- **Reattivo:** concerne tutte le attività risolutive in risposta al verificarsi di un malfunzionamento. In questo caso si procede ad acquisire e registrare il malfunzionamento e ad avviare le attività per la risoluzione definitiva della problematica, gestendo nel contempo le interazioni con tutte le strutture dell'Ente coinvolte.
- **Proattivo:** riguarda tutte le attività di prevenzione e comprensione delle cause dei malfunzionamenti, finalizzate alla diminuzione di questi e al miglioramento dei processi risolutivi. Gli obiettivi principali perseguiti si sostanziano nel diminuire i malfunzionamenti, minimizzare l'impatto degli stessi, individuarne le cause, avviare la risoluzione strutturale dei problemi, diffondere le esperienze sulla risoluzione, definire le procedure per il governo del processo, verificare e migliorare continuamente il funzionamento del processo.

Nel servizio di manutenzione correttiva s'intendono comprese tutte le attività connesse con il processo di individuazione dell'errore e della causa che l'ha generato e i conseguenti interventi finalizzati alla rimozione dell'anomalia e al ripristino o miglioramento del funzionamento originario, operando una o più delle seguenti azioni:

- Analisi, implementazione e test di eventuali soluzioni temporanee volte all'aggiramento del problema;
- Nel caso debbano essere modificati sostanzialmente uno o più moduli, il Service Desk informerà tempestivamente le risorse utilizzatrici, specificando gli impatti sulle funzionalità e sulle performance, le specifiche delle soluzioni proposte, una valutazione di risorse e tempi necessari per le modifiche preventivate e il piano operativo proposto per l'intervento.
- Correzione del codice.
- Installazione delle versioni aggiornate del codice direttamente nell'ambiente SaaS e distribuzione per le installazioni e-Home.

Sono esplicitamente esclusi da questo servizio la correzione o il rimedio di malfunzionamenti attribuibili ad esempio a:

- non osservanza della manualistica da parte del Cliente nell'utilizzo dei prodotti;
- modifiche apportate, in modo erroneo, dal Cliente o da terzi alla configurazione del sistema;
- negligenza, incuria, dolo del Cliente o di terzi nell'utilizzo del sistema;
- cause di forza maggiore o altre cause imputabili al Cliente o a terzi.

Gli interventi eventualmente effettuati da Municipia su richiesta dell'Ente in relazione a tali ultimi casi o ad altri assimilabili sono esclusi dalla presente proposta. Pertanto saranno oggetto di specifica quotazione separata verso il Cliente sulla base delle tariffe in vigore al momento dell'intervento.

MANUTENZIONE ADEGUATIVA

La **manutenzione adeguativa** ha l'obiettivo di aggiornare le funzionalità del software in esercizio sulla base di modifiche normative. Sono da comprendersi tra le modifiche normative tutte quelle che, pur modificando le funzionalità esistenti, non comportano variazioni alla struttura base dati e non richiedono lo sviluppo di nuove funzionalità aggiuntive.

L'iter procedurale seguito per la gestione del servizio di manutenzione adeguativa è schematizzato nella seguente figura.

Una volta messo in esercizio il sistema oggetto dell'evoluzione, Municipia si occupa dell'erogazione del servizio di assistenza agli utenti per le nuove funzionalità.

In ogni caso gli aggiornamenti oggetto di questo servizio si riferiscono ai prodotti software in versione standard e non comprendono eventuali attività di predisposizione o interventi sistemistico/applicativi per la riconversione delle banche dati.

Nell'ambito delle attività di manutenzione non rientrano fra le attività a carico di Municipia quelle riferite all'installazione, *tuning*, certificazione e adattamento dei prodotti sull'impianto tecnologico del Cliente.

MANUTENZIONE MIGLIORATIVA

Comprende la fornitura a titolo gratuito di miglioramenti ed implementazioni che, per propria iniziativa e/o su suggerimento di altri Clienti, Municipia abbia ritenuto di introdurre nella versione standard del prodotto al fine di accrescerne la qualità o le prestazioni.

RILASCIO DEGLI AGGIORNAMENTI

Il software è aggiornato automaticamente; il Cliente è avvertito in merito all'aggiornamento attraverso una notifica all'interno del software o via e-mail. Contestualmente è reso disponibile il documento denominato *Nota di Rilascio* che contiene le implementazioni e le correzioni apportate alla versione.

La periodicità di rilascio di tali aggiornamenti è stabilita da Municipia.

SERVIZIO DI ASSISTENZA – SERVICE DESK

In questa sezione sono descritte le modalità con le quali operatori specializzati assistono il Cliente in una fase di primo intervento per rispondere alle richieste di supporto sull'utilizzo del software, per malfunzionamenti nell'erogazione o per correggere errori di piccola entità sui dati che non implicano modifiche a codice.

> In via preliminare alla formulazione della richiesta di assistenza, al Cliente è consigliata l'attenta lettura del documento *Nota di Rilascio* che accompagna gli aggiornamenti software.

Di seguito vengono indicate:

- le modalità di accesso al servizio di assistenza
- le modalità di erogazione del servizio
- i livelli di servizio

MODALITA' DI ACCESSO AL SERVIZIO

Per accedere al servizio di assistenza per qualsiasi area d'interesse il Cliente può in alternativa:

inviare un'e-mail all'indirizzo:	**collegarsi all' url:**	**contattare il numero**
assistenza@municipia.eng.it	https://assistenza.municipia.eng.it	0575.1696237

> Il manuale d'uso e la descrizione dettagliata del servizio di Service Desk è disponibile all'url **https://confluence.municipia.eng.it/x/pACVB**

Per accedere all'interfaccia web del **service desk** è necessario utilizzare **le credenziali** in proprio possesso, oppure registrarsi seguendo la procedura descritta nel manuale d'uso.

La richiesta di assistenza formulata attraverso l'accesso diretto al **portale service desk** consente una lavorazione più rapida delle segnalazioni in quanto è il cliente stesso a specificare il problema e a codificarlo in relazione alle casistiche previste, assegnandogli anche una priorità.

In aggiunta il cliente ha la possibilità di:

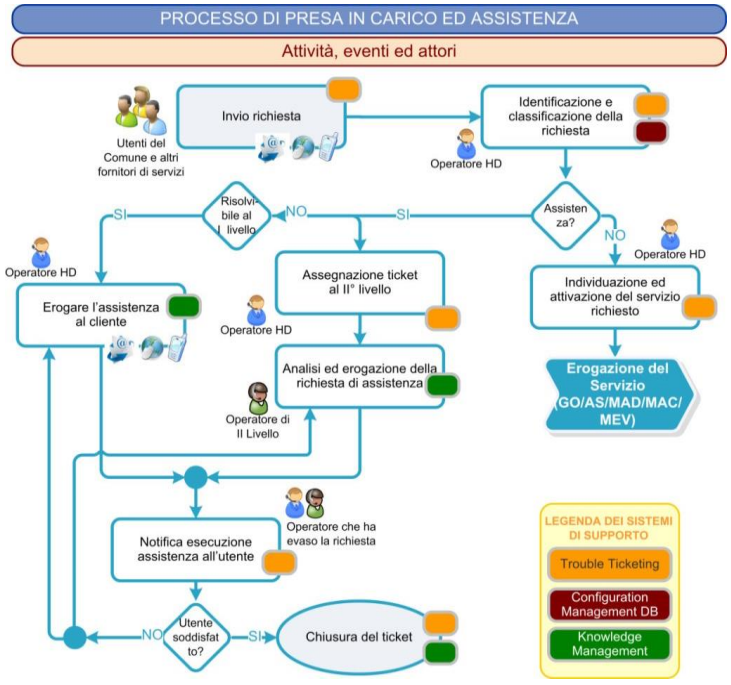
- consultare tutte le proprie segnalazioni con i dettagli della conversazione;
- caricare, visualizzare e gestire eventuali allegati inviati o ricevuti;
- usufruire di un'area per rispondere in modo semplice senza creare duplicati nelle richieste di assistenza;
- monitorare lo stato di avanzamento della segnalazione e i tempi massimi di risposta previsti.

Resta in ogni caso in carico agli operatori Municipia, addetti al servizio di assistenza, la modifica della priorità d'intervento in base alla reale criticità della segnalazione.

MODALITA' DI EROGAZIONE DEL SERVIZIO

La richiesta è processata attraverso un sistema di gestione delle segnalazioni il cui processo è illustrato nella figura che segue.
Le fasi principali sono tre:

- **Presa in carico**. Si verifica la completezza della richiesta pervenuta, richiedendo eventualmente le integrazioni necessarie. Una volta in possesso di tutti i dati necessari per la gestione della richiesta l'operatore svolge subito una ricerca per identificare eventuali correlazioni con problemi già sollevati in precedenza o con problemi aperti e in fase di risoluzione. Nel caso in cui sia individuata una segnalazione analoga, tale informazione è integrata ai dati già presenti sulla scheda intervento.
- **Esecuzione dell'intervento**. Nel caso in cui sia necessario un intervento sul sistema è svolta un'accurata analisi mediante la quale si identificano la causa dell'errore, il sistema e l'ambiente coinvolti. In base alle informazioni rilevate si individuano e attivano i profili corretti per la gestione della richiesta (sviluppatore, specialista dell'erogazione, specialista DB, etc.). Gli incaricati eseguono gli interventi e verificano che – a valle dell'esecuzione – il malfunzionamento sia effettivamente risolto.
- **Chiusura dell'intervento.** A valle della verifica della rimozione del malfunzionamento, si informa il Cliente della risoluzione dell'anomalia così da effettuare un'ulteriore verifica. L'intervento, infatti, può considerarsi effettivamente chiuso solo con la conferma del Cliente



CARATTERISTICHE DELL'EROGAZIONE DEL SERVIZIO RELATIVO AL SOFTWARE

Gli operatori addetti al servizio di assistenza assegnano la priorità ai problemi secondo le seguenti linee guida, a ciascun livello di priorità corrispondono livelli di servizi.

Di seguito i livelli di priorità che possono essere assegnati:

- **Bloccante**
  Il problema grave rende la funzione "non utilizzabile" o "non disponibile". Tutti i servizi erogati non sono disponibili
- **Maggiore**
  Il problema rende alcune funzioni non fondamentali "non utilizzabili" o "non disponibili" e non esiste una soluzione alternativa (Workaround)
- **Marginale**
  Il problema non è bloccante per i servizi erogati, ma comporta difformità rispetto alle specifiche definite o esistono soluzioni alternative

Nel sistema di Service Desk sono registrati tutti i passaggi eseguiti dal momento dell'apertura del ticket fino alla sua chiusura.

L'erogazione del servizio di Service Desk (support hours) è garantita per tutto l'anno sulla base del modello:

"5 x 8", 5 giorni alla settimana per 8 ore al giorno

dal lunedì al venerdì (nei giorni feriali) - dalle 08:30 alle 13:30 e dalle 14:30 alle 17:30

LIVELLI DI SERVIZIO

Come descritto la definizione dei livelli di servizio si riferisce al "giorno lavorativo", inteso come intervallo di tempo di 8 ore indipendente dal giorno solare. Ciò significa che, ad esempio, una segnalazione di tipo bloccante inserita nel sistema alle 16:30 di un giorno, sarà presa in carico entro le 11:30 del giorno feriale successivo.

I parametri di riferimento per il monitoraggio dei livelli di servizio sono:
1) Tempo di presa in carico della segnalazione
2) Tempo di risoluzione dell'anomalia segnalata

Di seguito gli obiettivi previsti dai SLA:

SLA	Definizione	Criticità	Contesto	Target
MFRT	Tempo di presa in carico	Bloccante	Tutti	4 ore lavorative
		Maggiore	Tutti	8 ore lavorative
		Marginale	Tutti	16 ore lavorative
TTR	Tempo di risoluzione	Bloccante	Assistenza	8 ore lavorative
		Maggiore	Assistenza	16 ore lavorative
		Marginale	Assistenza	40 ore lavorative
		Bloccante	Correttiva	16 ore lavorative
		Maggiore	Correttiva	24 ore lavorative
		Marginale	Correttiva	80 ore lavorative

PENALI

La determinazione delle penali si riferisce allo scostamento del valore determinato per gli SLA (MFRT e TTR) in termini di percentuale in un periodo di osservazione ed il valore target.
Il periodo dio osservazione è fissato in quattro mesi, durante i quali vengono determinati i ticket lavorati nei limiti temporali previsti, in relazione ai livelli di criticità, e quelli che invece non hanno soddisfatto i suddetti limiti temporali. Il rapporto numero di ticket fuori sla/Numero di ticket lavorati determina la percentuale sulla quale verificare lo scostamento rispetto al valore target.

Di seguito il valore delle penali previsto:

SLA	Definizione	Criticità	Contesto	Target	Obiettivo	Penale
MFRT	Tempo di presa in carico	Bloccante	Tutti	4 ore lavorative	90%	2 ‰ CAM del periodo
		Maggiore	Tutti	8 ore lavorative		
		Marginale	Tutti	16 ore lavorative		
TTR	Tempo di risoluzione	Bloccante	Assistenza	8 ore lavorative	90%	2 ‰ CAM del periodo
		Maggiore	Assistenza	16 ore lavorative		
		Marginale	Assistenza	40 ore lavorative		
		Bloccante	Correttiva	16 ore lavorative	90%	2 ‰ CAM del periodo
		Maggiore	Correttiva	24 ore lavorative		
		Marginale	Correttiva	80 ore lavorative		

CARATTERISTICHE DELL'EROGAZIONE DEL SERVIZIO RELATIVO ALL'INFRASTRUTTURA

EROGAZIONE DEL SERVIZIO

I servizi sono erogati da data centre di CSP qualificati sul marketplace AGID, ubicati nel territorio dell'Unione Europea e rispondenti dunque a tutte le caratteristiche di sicurezza, disponibilità e tutela del dato necessarie.

Dettagliamo di seguito alcuni aspetti di interesse.

Sicurezza dell'accesso alle applicazioni: l'accesso alle applicazioni in modalità cloud da parte degli utenti avviene attraverso accessi via Browser web o attraverso sistemi di *brokering* protetti da **cifratura TLS**. I sistemi non sono pubblici su internet ma mascherati e protetti da Firewall e Reverse Proxy. La parte applicativa e la base dati risiedono su ambienti logici separati.

Backup e sicurezza dei dati: le parti applicative sono salvate con procedure automatiche centralizzate incrementali e a rotazione. È possibile ripristinare selettivamente le basi dati, per Enti o per singolo dato. Le politiche di ritenzione del dato prevedono:
Istanze Applicative: Back-up snapshot based giornaliero incrementale con conservazione degli ultimi 7 giorni.
DataBase: Backup giornaliero con retention di 30 giorni.
Architettura Backup: il backup e il ripristino dei dati avvengono attraverso una copia consistente della banca dati del singolo Ente. L'intera area di backup è clonata al termine delle procedure di backup su altro datastore per garantire il ripristino in caso di indisponibilità dell'area di backup principale.
Casi e tempi di ripristino: nel caso di un evento distruttivo sul datastore che ospita il database, è possibile il ripristino alla sera del giorno precedente l'evento, combinando i dati salvati dai backup periodici e il backup della macchina DB. Nel caso di una modifica involontaria o di un errore applicativo che abbia reso inconsistente il database, è possibile il ripristino a un qualsiasi backup eseguito nell'ambito delle politiche di ritenzione. I tempi di ripristino sono entro le 24 ore lavorative.
Architettura Backup Macchine Applicative: le aree applicative sono salvate con sistemi di backup che, secondo i livelli di ritenzione illustrati, conservano l'intero file system e i parametri dell'ambiente. I dati sono salvati su datastore diversi da quelli sui quali risiedono le macchine stesse.
Casi e tempi di ripristino: nel caso di perdita completa dell'area applicativa, è possibile un ripristino completo entro 8 ore lavorative. Nel caso di necessità di ripristino di parti del file system in seguito a errori applicativi o umani, è possibile un ripristino entro 4 ore lavorative. In entrambi i casi è possibile ripristinare a un qualsiasi punto conservato secondo le specifiche di ritenzione del dato.
Business Continuity: L'erogazione dei servizi di connettività, alimentazione, sicurezza è garantito 24x7x365 dal Data Center. Le strutture che ospitano gli ambienti sono completamente ridondate per il *single point of failure* verso lo storage e la connettività.
Disponibilità delle Applicazioni Municipia: Le applicazioni sono accessibili agli utenti tutti i giorni dalle 5 alle 23. Dalle 23 alle 5 è prevista una finestra di manutenzione per backup, aggiornamenti e attività straordinarie.

ARCHITETTURA

L'architettura software proposta, come è stato evidenziato nel precedente paragrafo, è sicura e in linea con i più evoluti orientamenti *SaaS*. Le applicazioni e la banca dati risiedono su ambienti gestiti da Municipia ed è possibile fruirli attraverso un qualsiasi browser Internet aggiornato.
L'aggiornamento del software con l'installazione delle nuove versioni rilasciate e i salvataggi della banca dati sono demandati a Municipia.

L'architettura proposta ha diversi vantaggi che riepiloghiamo brevemente:
Sicurezza della Banca Dati. Presso il CSP sono attivi sistemi di sicurezza, back-up e protezione del dato, che assicurano che nessuna informazione delle Banche Dati custodite vada perduta.

Privacy dei Dati. Unitamente alle procedure di sicurezza, presso il CSP, sono in uso sofisticati sistemi di controllo degli accessi (questo sia dal punto di vista informatico, quindi accesso via Internet, sia dal punto di vista logistico, quindi controlli anche sulle persone che fisicamente accedono alla Server Farm).

LIVELLI DI SERVIZIO

I sistemi sono disponibili agli utilizzatori ogni giorno dalle 5 alle 23. All'interno di questo periodo di esercizio, l'**availability** è definita del 99.2%

PENALI

SLA	Definizione	Criticità	Contesto	Target	Penale
Availability	Disponibilità media dei sistemi erogati in SaaS nel periodo di esercizio da contratto. (5 - 23)	SaaS	99,2%	Quadrimestrale	1 ‰ CAM del periodo

SUPPORTO SPECIALISTICO (ON SITE O DA REMOTO)

Con questa formula il Cliente può usufruire di un servizio specialistico di assistenza da remoto o direttamente presso la propria sede. Il supporto specialistico include le attività non comprese nel contratto di assistenza e manutenzione che l'Ente può richiedere, quali: supporto di dominio, formazione, configurazione, parametrizzazione avanzata, realizzazione di modelli di stampa ecc. Per quanto riguarda questo tipo di servizio **sono stati inseriti a MEPA** dei **pacchetti di giornate** acquistabili direttamente dalla piattaforma del mercato elettronico.In relazione al numero delle giornate previste nel pacchetto diminuisce il prezzo di ogni giornata come evidenziato nel prospetto qui sotto:

GIORNATE DA REMOTO

Codici MEPA	SUGRCS01	SUGRCS03	SUGRCS05	SUGRCS10	SUGRCS20
	1 giornata	*3 giornate*	*5 giornate*	*10 giornate*	*20 giornate*
Importo pacchetto	470,00	1.350,00	2.200,00	4.300,00	8.300,00
Importo a giornata	*470,00*	*450,00*	*440,00*	*430,00*	*415,00*

GIORNATE ON SITE (PRESSO LA SEDE DELL'ENTE)

Codici MEPA	SUGSCS01	SUGSCS03	SUGSCS05	SUGSCS10	SUGSCS20
	1 giornata	*3 giornate*	*5 giornate*	*10 giornate*	*20 giornate*
Importo pacchetto	650,00	1.920,00	3.125,00	6.100,00	12.000,00
Importo a giornata	650,00	640,00	625,00	610,00	600,00

Si precisa che per ogni giornata di assistenza via web la quota minima erogabile è pari a 4 ore (1/2 giornata).

Per richiedere l'erogazione di una o più giornate di supporto specialistico, è necessario censire una richiesta attraverso uno dei seguenti canali:

- Portale WEB - **https://assistenza.municipia.eng.it** - Sezione "Supporto Specialistico"
- Posta Elettronica - **supportospecialistico@municipia.eng.it**

CAPITOLO 3

CONDIZIONI SPECIFICHE DI FORNITURA

OBBLIGO DI RISERVATEZZA

Le informazioni contenute nel presente documento devono ritenersi strettamente confidenziali. Il destinatario di questo documento è tenuto, pertanto, a: non utilizzarle per finalità diverse dalla valutazione della proposta - non divulgarle e a fare in modo che non vengano divulgate direttamente o indirettamente a soggetti diversi dal proprio personale direttamente coinvolto nella valutazione della stessa - non copiarle, riprodurle, duplicarle, senza il preventivo consenso scritto di Municipia S.p.A.

OGGETTO DELLA FORNITURA Oggetto della fornitura è l'erogazione da parte di Municipia dei servizi / soluzioni descritti nel capitolo 2 Proposta Tecnica e/o negli allegati che costituiscono parte integrante di questa proposta tecnico economica.

OBBLIGHI E RESPONSABILITÀ DI MUNICIPIA

Municipia s'impegna a:

- operare con diligenza nello svolgimento di tutte le attività connesse alla Fornitura, mettendo a disposizione personale qualificato all'esecuzione autonoma degli interventi di sua competenza, nel rispetto delle procedure specificate nel presente contratto.
- operare nel rispetto delle norme particolari di sicurezza e/o riservatezza concordate con il Cliente.
- garantire il rispetto di dette norme di sicurezza e/o riservatezza da parte di terze parti coinvolte nell'espletamento della Fornitura.
- garantire la corretta esecuzione di quanto previsto nel presente contratto, ritenendosi in ogni caso sollevato da ogni responsabilità per eventuali ritardi dovuti a cause di forza maggiore.
- farsi carico di tutti gli oneri sociali ed assicurativi per il personale impiegato nello svolgimento della Fornitura, con particolare riguardo all'assicurazione contro gli infortuni sul lavoro
- a restituire al Cliente, in caso di mancata adesione alla proposta e/o di recesso, gli archivi di propria competenza in formato CSV.
  L'eventuale supporto alla corretta lettura dei dati forniti sarà erogato previa quotazione delle giornate di lavoro necessarie a fronte delle quali sarà emessa apposita fatturazione.

Al seguente link le specifiche del processo di reversibilità seguito da Municipia:
https://confluence.municipia.eng.it/x/AgQ9BQ

OBBLIGHI E RESPONSABILITÀ DEL CLIENTE

Il Cliente s'impegna a:

- rendere disponibili tutte le informazioni necessarie per il corretto svolgimento della Fornitura
- consentire l'accesso alle proprie sedi da parte delle persone del Municipia preposte all'erogazione della Fornitura, come pure ai sistemi che devono interoperare con la soluzione SaaS.
- rendere evidente a Municipia la copertura del prodotto software standard, cui la Fornitura è connessa, con un contratto di manutenzione, in corso di validità, stipulato con il produttore del software
- mantenere il proprio personale aggiornato sulle evoluzioni dei prodotti oggetto di assistenza da parte di Municipia

Il Cliente deve inoltre assicurare, a proprio carico:

- la disponibilità di una connessione internet "Always on" a band a larga che consenta l'operatività "call back", allo scopo di permettere ai tecnici di Municipia l'accesso remoto al sistema del Cliente in qualsiasi momento si renda necessario.
- la predisposizione di adeguati strumenti per l'accesso remoto per interventi di assistenza tempestivi ed efficienti.

REQUISITI PRELIMINARI PER ESECUZIONE DEI LAVORI

Per la corretta esecuzione del servizio è obbligatorio che il Cliente:

- nomini il proprio referente interno, quale **interlocutore unico**, che sarà dedicato a intrattenere i rapporti con la ns. Direzione Tecnica
- fornisca, se previsti, i documenti di "attivazione lavori" debitamente compilati e sottoscritti.

DURATA OFFERTA

L'offerta ha una validità di 60 gg. partire dalla data della presente.

ADESIONE - DURATA – RECESSO

L'**adesione** al servizio avviene attraverso la sottoscrizione del Modulo d'Ordine e l'invio della determina.

Il contratto di erogazione del servizio SaaS ha la **durata** indicata nel modulo d'ordine che costituisce parte integrante del documento.

Ogni annualità coincide con l'anno solare o, limitatamente al primo anno, alla parte di esso che va dalla data di attivazione fino al 31 Dicembre dell'anno stesso.

Sarà cura di Municipia inoltrare al Cliente la nota contenente il rinnovo del servizio per un periodo definito in accordo con il Cliente.

In caso di **recesso**, per la cui disciplina vige quanto stabilito dalle condizioni generali di contratto relative alla prestazione di servizi del bando MEPA di riferimento, Municipia, previa apposita comunicazione inviata al Cliente, provvederà ad interrompere i servizi di manutenzione, assistenza e adeguamento normativo del software utilizzato.

Garantirà per un periodo "di transizione" di tre mesi l'accesso all'applicazione al fine di consentire la continuità del servizio.

Durante il periodo di transizione dovrà essere riconosciuto a Municipia un canone corrispondente ad un terzo del valore contrattuale pattuito.

Il periodo di transizione si chiuderà, per esplicita richiesta del Cliente prima dei tre mesi dalla cessazione, oppure alla scadenza dei tre mesi.
Alla scadenza del periodo di transizione, previa comunicazione al Cliente, Municipia inibirà definitivamente l'accesso a tutti gli utenti del sistema e provvederà a conservare i contenuti della banca dati, in sicurezza, per il periodo necessario all'invio al Cliente e comunque non oltre due mesi dallo scadere del periodo di transizione.
I dati saranno resi disponibili sia secondo quanto concordato con il Cliente nel rispetto delle linee guida AGID di riferimento.
Tutte le banche dati riconsegnate al cliente saranno distrutte.
Il recesso potrà essere esercitato dal Cliente per iscritto a mezzo peci o raccomandata a/r.

CORRISPETTIVI- FATTURAZIONE - PAGAMENTI

I **corrispettivi** riferiti all'erogazione del/i servizio/i sono indicati nel capitolo della proposta economica e sono riportati al netto di IVA.
Gli importi dovuti dal Cliente sanno **fatturati** nella seguente modalità:

- servizi di avviamento (dopo collaudo finale con esito positivo);
- canone di manutenzione 2022 a seguito di fatture trimestrali posticipate previa verifica di conformità contrattuale e regolarità contributiva;
- counceling Bilancio Consolidato, a consuntivo sulle attività svolte.

In conformità con il D.Lgs 192/2012 i **pagamenti** dovranno essere effettuati tramite Bonifico Bancario entro 30 giorni data fattura.
In caso di ritardato pagamento gli interessi moratori ai sensi dell'art. 4 del suddetto D.Lgs decorrono, senza che sia necessaria la costituzione in mora, dal giorno successivo alla scadenza del termine di pagamento. Il tasso dell'interesse di mora (art. 5 del Dlgs 231/2002 modificato dal Dlgs 192/2012) è pari al saggio di interesse del principale strumento di rifinanziamento della Banca Centrale Europea rilevato il primo giorno di ogni semestre, aumentato di otto punti percentuali.

ESCLUSIONI

Non costituiscono oggetto del presente contratto:

- supporto di assistenza eventualmente richiesto presso la sede del Cliente (on site);
- attività di manutenzione correttiva imputabili a correzione o rimedio di malfunzionamenti attribuibili ad esempio a:
  - non osservanza della manualistica da parte del Cliente nell'utilizzo dei prodotti;
  - modifiche apportate, in modo erroneo, dal Cliente o da terzi alla configurazione del sistema;
  - negligenza, incuria, dolo del Cliente o di terzi nell'utilizzo del sistema;
  - cause di forza maggiore o altre cause imputabili al Cliente o a terzi.
  - supporto specialistico

COSTI SALUTE E SICUREZZA

Si rimanda a quanto previsto nella stipula MEPA e a quanto indicato nel Modulo D'Ordine.

PROTEZIONE DATI PERSONALI

In conformità a quanto previsto dal Regolamento 2016/679/UE (di seguito anche solo "Regolamento UE"), tutti i dati personali che verranno scambiati fra le Parti nel corso dello svolgimento del Contratto saranno trattati rispettivamente da ciascuna delle Parti per le sole finalità indicate nel Contratto ed in modo strumentale all'espletamento dello stesso, nonché per adempiere ad eventuali obblighi di legge, della normativa comunitaria e/o prescrizioni del Garante per la protezione dei dati personali e saranno trattati, con modalità manuali e/o automatizzate, secondo principi di liceità e correttezza ed in modo da tutelare la riservatezza e i diritti riconosciuti, nel rispetto di adeguate misure di sicurezza e di protezione dei dati anche sensibili o idonei a rivelare lo stato di salute, previsti dal Codice Privacy e dal Regolamento UE.
Ciascuna Parte riconosce ed accetta che i dati personali relativi all'altra Parte, nonché i dati personali (es. nominativi, indirizzo email aziendale, ecc.) di propri dipendenti/collaboratori, coinvolti nelle attività di cui al presente Contratto, saranno trattati dall'altra Parte in qualità di Titolare per finalità strettamente funzionali alla instaurazione e all'esecuzione del Contratto stesso ed in conformità con l'informativa resa da ognuna ai sensi e per gli effetti di cui all'articolo 13 del GDPR , che l'altra Parte si impegna sin da ora a portare a conoscenza dei propri dipendenti/collaboratori, nell'ambito delle proprie procedure interne.
L'informativa del Fornitore, che deve essere portata alla conoscenza dei dipendenti/collaboratori dell'altra Parte è reperibile nella sezione "Privacy Policy "del sito **www.municipia.eng.it**.
Per l'esecuzione del Contratto Municipia tratterà i dati in qualità di Responsabile del Trattamento a norma dell'art. 28 del Regolamento UE attenendosi a quanto riportato alla voce "Accordo Trattamento Dati Personali" del presente Contratto. Allo stesso modo, ove dalle dinamiche di esecuzione del Contratto emergesse una forma di contitolarità dei trattamenti di dati personali di terzi da parte di entrambe le Parti, queste ultime si impegnano a sottoscrivere, senza alcun onere aggiunto per alcuna Parte, un accordo di contitolarità a norma dell'art. 26 del Regolamento UE da allegarsi al presente Contratto e a rispettare gli obblighi di informativa verso gli interessati. Ciascuna Parte dichiara di essere a conoscenza della normativa prevista dall'art. 24-bis del D.L. 83/2012 e dalla delibera n. 666/08/CONS, relativa agli obblighi di iscrizione al Registro degli Operatori di Comunicazione degli operatori economici che svolgono attività di call center nonché dei soggetti terzi affidatari dei servizi di call center e ciascuna Parte dichiara altresì di aver adempiuto agli obblighi ivi previsti, se e in quanto applicabili al caso di specie, anche con riferimento all'obbligo di comunicare all'utente chiamante o chiamato il Paese dal quale si risponde.
In caso di effettuazione di chiamate verso numerazioni italiane, ciascuna Parte si impegna a rispettare, per quanto di propria competenza e in quanto applicabile, tutta la normativa vigente e applicabile in ogni momento e anche in futuro in Italia in materia di contatti a distanza per fini promozionali, di vendita diretta, di attività promozionali e ricerche di mercato, in particolare la legge 11 gennaio 2018, n. 5 e quanto previsto dai commi 3-bis, 3-ter, 3-quater dell'articolo 130 del Codice Privacy, dal D.P.R. 178/2010 e dal Provvedimento Generale del Garante per la protezione dei dati personali del 19 gennaio 2011, in materia di prescrizioni per il trattamento di dati personali per finalità di marketing, mediante l'impiego del telefono con operatore, a seguito dell'istituzione del registro pubblico delle opposizioni. La violazione delle previsioni contenute nel presente articolo espone la Parte inadempiente al risarcimento in favore dell'altra Parte dei danni eventualmente cagionati.

ACCORDO TRATTAMENTO DATI PERSONALI

L'Ente/Azienda quale Titolare dei dati cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali (di seguito "Titolare"), in persona del suo legale rappresentante designa ed istruisce MUNICIPIA SPA quale Responsabile dei trattamenti dei dati personali (di seguito "Responsabile") effettuati in relazione al Servizio oggetto del contratto di cui al punto precedente.

OBBLIGHI DEL TITOLARE

Il Titolare del trattamento è responsabile di garantire che il trattamento dei dati personali avvenga in conformità con l'articolo 24 del GDPR.
E' intenzione del Titolare consentire l'accesso sia al Responsabile che alle persone autorizzate al trattamento per i soli dati personali la cui conoscenza sia necessaria per adempiere ai compiti loro attribuiti.
Il Titolare affida al Responsabile tutte le operazioni di trattamento dei dati personali necessarie per dare piena esecuzione al Servizio innanzi indicato.
Il Titolare si impegna a comunicare per iscritto al Responsabile qualsiasi variazione si dovesse rendere necessaria nelle operazioni di trattamento dei dati.
Il Titolare dichiara, inoltre, che i dati da lui trasmessi al Responsabile:

- sono pertinenti e non eccedenti rispetto alle finalità per le quali sono stati raccolti e successivamente trattati;
- in ogni caso, i dati personali e/o le categorie particolari di dati personali, oggetto delle operazioni di trattamento affidate al Responsabile, sono raccolti e trasmessi rispettando ogni prescrizione della normativa applicabile.

Resta inteso che rimane a carico del Titolare l'onere di individuare la base legale del trattamento dei dati personali degli interessati.
Il Titolare ha il diritto e l'obbligo di prendere decisioni riguardo le finalità e i mezzi del trattamento di dati personali.

OBBLIGHI DEL RESPONSABILE

Il Responsabile deve procedere al trattamento secondo le istruzioni del Titolare documentate mediante il presente accordo.
Istruzioni successive potranno essere fornite dal Titolare anche durante il trattamento di dati personali purché documentate e/o previste dal Contratto principale. In ogni caso, qualora le dette istruzioni dovessero comportare implementazioni non previste e/o non prevedibili alla stipula del contratto principale, le stesse dovranno essere concordate di volta in volta in termini di tempi/costi e fattibilità tra le parti.
Il Responsabile del trattamento informa immediatamente il Titolare qualora le istruzioni impartite dallo stesso violino il GDPR o le disposizioni applicabili in materia di protezione dei dati dell'UE o degli Stati membri.
Sarà cura del Responsabile vincolare le persone autorizzate al trattamento alla riservatezza o ad un adeguato obbligo legale di confidenzialità anche per il periodo successivo all'estinzione del rapporto di collaborazione intrattenuto con il Responsabile, in relazione alle operazioni di trattamento da esse eseguite.
Il Responsabile, nel designare per iscritto le persone autorizzate al trattamento, dovrà assicurarsi che esse abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati. Dovrà inoltre curarne la formazione sui temi relativi alla protezione dei dati personali.
Inoltre, ove applicabile e per quanto concerne i trattamenti effettuati per l'erogazione della fornitura dalle persone autorizzate al trattamento con mansioni di "Amministratore di Sistema", il Responsabile è tenuto altresì al rispetto delle previsioni relative alla disciplina sugli amministratori di sistema contenute nel provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 modificato in base al provvedimento del 25 giugno 2009.
Il Responsabile, in particolare, si impegna a conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema, e a fornirli prontamente al Titolare su richiesta del medesimo.
In caso di danni derivanti dal trattamento, il Responsabile ne risponderà qualora non abbia adempiuto agli obblighi del GDPR specificatamente diretti ai Responsabili del trattamento o abbia agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare, a meno che non dimostri che l'evento dannoso non gli sia in alcun modo imputabile.

SICUREZZA DEL TRATTAMENTO

Tenendo conto dello stato dell'arte, dei costi di implementazione e della natura, ambito, contesto e finalità del trattamento, come anche della probabilità e severità del rischio per i diritti e le libertà delle persone fisiche, il Titolare ed il Responsabile implementano appropriate misure tecniche ed organizzative per assicurare un livello di sicurezza adeguato al rischio.
Il Titolare valuta i rischi inerenti al trattamento per i diritti e le libertà degli interessati, ed implementa le misure idonee a mitigarli. A seconda della loro rilevanza, tali misure posso includere le seguenti:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Il Responsabile assiste il Titolare nel garantire il rispetto degli obblighi relativi alle misure tecniche-organizzative di cui all'art. 32 GDPR, fornendo a quest'ultimo il dettaglio delle misure di sicurezza implementate per le operazioni del trattamento eseguite presso le proprie sedi e con i propri mezzi tecnico-organizzativi, insieme a tutte le altre informazioni necessarie al Titolare per ottemperare ai propri obblighi normativi.
Le misure di sicurezza tecnico-organizzative attuate dal Responsabile del trattamento sono elencate nell' **Appendice 1**, parte integrante del presente accordo.

SUB- RESPONSABILI

Il Responsabile del trattamento deve soddisfare i requisiti di cui all'articolo 28, paragrafi 2 e 4 del GDPR quando ricorre ad altro responsabile (altrimenti detto sub-responsabile).
Il Titolare concede al Responsabile preventiva autorizzazione generale per il ricorso a Sub-Responsabili. Il Responsabile informa per iscritto il Titolare di eventuali modifiche relative ad aggiunta o sostituzione di sub-responsabili con almeno 10 giorni

di preavviso, dando in tal modo al Titolare modo di opporsi a tali cambiamenti prima che tali sub-responsabili vengano ingaggiati.
L'elenco dei sub-responsabili già autorizzati dal Titolare del trattamento è riportato nell' **Appendice 2.**
Quando il Responsabile coinvolga un sub-responsabile per l'esecuzione di specifiche attività del trattamento operato per conto del Titolare, sullo stesso sub-responsabile devono essere imposte mediante un contratto o altro atto giuridico le stesse obbligazioni relative alla protezione dei dati contenute nel presente accordo, in particolare prevedendo sufficienti garanzie per quanto attiene all'adozione di appropriate misure tecniche ed organizzative tali da rendere il trattamento conforme ai requisiti del presente accordo e del GDPR.
Il Responsabile del trattamento è quindi responsabile di richiedere che il sub-responsabile soddisfi almeno gli obblighi cui è esso stesso soggetto ai sensi del presente accordo e del GDPR.

TRASFERIMENTO DATI IN UN PAESE TERZO

Qualsiasi trasferimento di dati personali verso paesi terzi o organizzazioni internazionali da parte del responsabile del trattamento dei dati deve avvenire esclusivamente sulla base di istruzioni documentate da parte del Titolare e deve sempre avvenire in conformità al Capitolo V del GDPR.
Nel caso di trasferimenti verso paesi terzi o organizzazioni internazionali, richiesti dalla legislazione dell'UE o degli Stati membri a cui è soggetto il Responsabile del trattamento, e che non siano stati richiesti dal Titolare del trattamento con specifica istruzione, il Responsabile del trattamento informa il Titolare del tale requisito legale prima del trattamento, a meno che la norma stessa non vieti tale comunicazione per importanti motivi di interesse pubblico.

ASSISTENZA AL TITOLARE

Il Responsabile del trattamento dei dati deve inoltre, tenendo conto della natura del trattamento e delle informazioni disponibili, fornire supporto al Titolare affinché possa ottemperare:

- all'obbligo del Titolare a effettuare senza indebito ritardo e, ove possibile, entro e non oltre 72 ore dalla sua conoscenza, la comunicazione circa una violazione dei dati personali all'Autorità per la Protezione dei Dati Personali a meno che non sia è improbabile che comporti un rischio per i diritti e le libertà delle persone fisiche;
- all'obbligo del Titolare di effettuare una valutazione dell'impatto delle operazioni di trattamento previste sulla protezione dei dati personali (una valutazione d'impatto sulla protezione dei dati); - all'obbligo del Titolare del trattamento di consultare l'Autorità per la Protezione dei Dati personali prima di porre in essere un trattamento qualora una valutazione d'impatto indicasse che il trattamento comporterebbe un rischio elevato (in assenza di misure adottate dal Titolare di mitigazione del rischio). agli obblighi del Titolare nei confronti delle richieste di esercizio dei diritti dell'interessato stabilite nel capitolo III GDPR per quanto applicabile.

Il Responsabile sarà, inoltre, tenuto a comunicare tempestivamente al Titolare eventuali istanze degli interessati, contestazioni, ispezioni o richieste dell'Autorità di Controllo e dalle Autorità Giudiziarie, ed ogni altra notizia rilevante in relazione al trattamento dei dati personali oggetto del contratto.

NOTIFICA DATA BREACH

In caso di violazione dei dati personali, il responsabile del trattamento deve informare il Titolare della violazione (o presunta violazione) entro 48 dopo che il responsabile ne è venuto a conoscenza per consentire al Titolare la notifica della violazione dei dati personali all'autorità di controllo competente così come previsto dall'Articolo 33 del GDPR.
Le parti definiscono nell' **Appendice 3** tutti gli elementi che devono essere forniti dal responsabile al Titolare del trattamento nella notifica di una violazione dei dati personali.

CANCELLAZIONE E RESTITUZIONE DEI DATI

Al termine delle operazioni di trattamento affidate, nonché all'atto della cessazione per qualsiasi causa del trattamento da parte del Responsabile, lo stesso a discrezione del Titolare sarà tenuto alternativamente a:

- restituire al Titolare i dati personali oggetti del trattamento
- provvedere alla loro integrale distruzione salvi solo i casi in cui la conservazione dei dati sia richiesta da norme di legge od altri fini (contabili, fiscali, ecc.).

Il Responsabile provvederà a rilasciare al Titolare apposita dichiarazione per iscritto contenente l'attestazione che presso il Responsabile non esista alcuna copia dei dati personali e delle informazioni di titolarità del Titolare.

AUDIT E ISPEZIONI

Il responsabile del trattamento mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare la conformità agli obblighi di cui all'articolo 28 GDPR e si rende disponibile per le attività di audit, comprese le ispezioni, condotte dal Titolare del trattamento, o da un altro revisore dallo stesso incaricato.
A tal scopo, il Responsabile riconosce al Titolare, ed agli incaricati del medesimo, il diritto richiedere evidenza delle certificazioni più recenti emesse da terze parti accreditate. In subordine, qualora il Titolare abbia bisogno di ulteriori informazioni per adempiere ai propri obblighi di audit, avrà la facoltà di richiedere al Responsabile ulteriori evidenze, e, se del caso, previo congruo preavviso di 5 giorni lavorativi, di accedere ai locali del fornitore presso i quali si svolgono le operazioni di trattamento.
In ogni caso, il Titolare si impegna per sé e per i terzi incaricati da quest'ultimo, a che le informazioni raccolte durante le operazioni di verifica siano utilizzate solo per finalità di audit, e che le operazioni di verifica si svolgano in modo tale da non interferire con la normale attività produttiva del Responsabile.

CESSAZIONE DELL'ACCORDO

La presente nomina avrà efficacia fintanto che venga erogato il Servizio. Qualora il Servizio comporti un'esecuzione periodica e/o continuativa, rinnovata di volta in volta con specifici contratti, la presente nomina si intende efficace per la durata complessiva del Servizio.

COMUNICAZIONI TRA LE PARTI

Le comunicazioni tra le parti, ai fini del presente incarico, dovranno essere indirizzate:

- **per il Responsabile del trattamento:** MUNICIPIA S.p.A., Via Adriano Olivetti, 7- Trento (TN)
  - pec: municipia.supportovendita@pec.it
- **per il Titolare del trattamento:** Comune di Cremona Piazza del Comune, 8 - 26100 Cremona – p.i: 00297960197

DIRITTI DI PROPRIETA' INTELLETTUALE

Il Fornitore, ovvero il terzo licenziante, resta pieno ed esclusivo titolare della proprietà intellettuale e/o industriale (ai sensi e per gli effetti della L. 22.4.1941, n. 633 come integrata e/o modificata dal D.L. 29.1.1992, n. 518 e relativo regolamento di esecuzione, "Legge sui Diritti di Autore" e/o "Legge"), sulle apparecchiature, programmi per elaboratore e/o software, manuali operativi e relativa documentazione eventualmente resi disponibili od utilizzati per l'erogazione della Fornitura.
L'erogazione da parte del Fornitore della Fornitura non fornisce in alcun modo al Cliente e/o a terzi titolo a diritti di proprietà intellettuale, che sono e rimangono di esclusiva proprietà del Fornitore e/o dei suoi licenzianti, in tal caso si applicheranno le garanzie dei terzi licenzianti, delle quali il Fornitore darà circostanziata informazione scritta al Cliente, nonché le condizioni di licenza d'uso dei suddetti terzi licenzianti, che il Cliente accetta di rispettare.
In caso di Fornitura avente ad oggetto lo sviluppo software, la proprietà del software e della relativa documentazione se il software è realizzato ad hoc per il Cliente resteranno del Cliente che concederà al Fornitore una licenza d'uso gratuita a tempo indeterminato.
In caso di servizi di outsourcing il software applicativo messo a disposizione dal Cliente è e resta di proprietà del Cliente e/o dei suoi licenzianti, fermo restando che al Fornitore sarà concessa dal Cliente licenza d'uso gratuita, ai soli fini dell'esecuzione delle Prestazioni previste dal Contratto. Il Cliente terrà il Fornitore pienamente mallevato e indenne da qualsiasi danno, onere, azione o conseguenza pregiudizievole in relazione al suddetto software applicativo utilizzato dal Fornitore per l'esecuzione delle Prestazioni, incluso il caso di rivendicazioni di terzi su detto software.
Il Cliente s'impegna ad adottare tutte le ragionevoli misure necessarie per tutelare i diritti di proprietà intellettuale, tra i quali – a titolo esemplificativo - i brevetti, marchi, nomi commerciali, invenzioni, copyright, know-how, segreti commerciali etc. Il Cliente dovrà tempestivamente comunicare per iscritto al Fornitore la scoperta di qualsiasi uso non autorizzato o violazione dei prodotti o dei diritti sui brevetti, copyright, marchi o altri diritti di proprietà intellettuale del Fornitore associati ai prodotti.

SICUREZZA E PROTEZIONE DELLE INFORMAZIONI IN CLOUD SAAS

CONDIVISIONE DI RESPONSABILITA' PER LA SICUREZZA DELLE INFORMAZIONI

Per quanto riguarda l'assunzione di responsabilità in merito ai ruoli che garantiscono la sicurezza delle informazioni, in particolare per le attività (ove applicabili) relative ad:

- Hardening di sistemi e apparati;
- Backup;
- Controlli crittografici (ove applicabile);
- Gestione delle vulnerabilità tecniche;
- Gestione degli incidenti;
- Controllo della conformità tecnica;
- Test di sicurezza;
- Auditing;
- Raccolta delle registrazioni (log);
- Protezione delle informazioni al termine del contratto;
- Autenticazione e controllo degli accessi

Si concorda che Cliente e Fornitore sono entrambi responsabili, ciascuno per le aree di propria competenza, che sono desumibili contrattualmente.
In linea generale vale la regola secondo cui l'onere di effettuare le attività che garantiscono la sicurezza delle informazioni spetta a chi detiene le password degli account con privilegi di amministrazione degli ambienti da mettere in sicurezza. Es.: In un contratto per la fornitura di servizi SaaS, ove il Fornitore fornisce e gestisce un layer applicativo su cui sono installati applicazioni e dati, il Fornitore è responsabile per gli adempimenti di sicurezza applicativa (es. predisposizione di funzionalità di autenticazione, logging, gestione di vulnerabilità applicative, etc.) e garantisce che siano implementate le misure di sicurezza infrastrutturale relative alla gestione degli ambienti virtualizzati che ospitano il layer applicativo. Il Fornitore, inoltre, si avvale di subfornitori qualificati e certificati che mettono a disposizione il layer infrastrutturale di base (in modalità IaaS e Paas), con cui sussistono accordi contrattuali in garanzia dell'adozione di misure di sicurezza adeguate.

PROTEZIONE DELLE INFORMAZIONI DEL CLIENTE NELL'AMBITO DEI SERVIZI CLOUD

GARANZIE

Il Fornitore garantisce ai propri Clienti, oltre all'applicazione delle idonee misure per la protezione dei **dati personali** previste dalla normativa vigente RE UE 679/2016, anche l'applicazione di una serie di misure idonee alla protezione **di tutti i dati**, tra cui l'adozione, l'applicazione e la certificazione di conformità della/alla norma di sicurezza volontaria ISO/IEC 27001:2013 "Information technology - Security techniques - Code of practice for information security management" ed il rispetto delle linea-guida:

- ISO/IEC 27018:2019 "Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors";
- ISO/IEC 27017:2015 "Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

Si forniscono maggiori informazioni con particolare riferimento ai seguenti controlli:
Gestione delle vulnerabilità Tecniche
Le vulnerabilità tecniche vengono gestite ciclicamente tramite un processo di individuazione strumentale delle vulnerabilità sugli asset (la frequenza è proporzionale al livello di esposizione degli asset stessi), gli input dei vendor e dei gruppi di interesse in contatto con i competence center tecnici oltre che da possibili inneschi provenienti da strumenti di monitoring o da segnalazioni utente.
La comunicazione ed il fixing delle vulnerabilità tecniche segue sempre un iter concordato tra le parti e da definire in fase di transition (change management) ed è comunque in funzione della gravità delle vulnerabilità stesse.
Hardening delle macchine virtuali

Le attività di hardening delle macchine virtuali che ospitano ambienti applicativi in SaaS per il Cliente saranno effettuate rispettivamente dal fornitore Saas e dai subfornitori IaaS e Paas, come previsto dai relativi accordi contrattuali.

TRATTAMENTO DELLE INFORMAZIONI

Le informazioni affidate al Fornitore vengono trattate per conto del Cliente secondo quanto previsto dalla giurisdizione di riferimento, che è quella **europea ed italiana**, solo ed esclusivamente per le finalità contrattualizzate, a meno di specifici ed espliciti accordi con il Cliente stesso.

In particolare, il Fornitore si impegna a non utilizzare le informazioni per finalità commerciali senza autorizzazione esplicita del Cliente e dichiara che tale autorizzazione non è mai precondizione necessaria all'erogazione dei propri servizi.

Le informazioni risiedono:

- **in Italia in uno o più dei Datacenter Engineering** (a meno di differenti specifici ed espliciti accordi con il Cliente) qualora il servizio SaaS si attesti su VCloud fornito da Engineering D.Hub
- **in UE in uno in uno o più dei Datacenter messi a disposizione da altri fornitori di infrastruttura Cloud** (ad es. Amazon WebServices) di cui Municipia si avvale, purchè essi siano in possesso delle certificazioni previste per l'accreditamento in Marketplace AgID.

I trattamenti vengono effettuati esclusivamente da personale qualificato, formalmente incaricato ai sensi delle normative Privacy ed istruito in tal senso.

DIFFUSIONE DELLE INFORMAZIONI

In caso di richiesta di consegna da parte di Autorità Giudiziarie o Amministrative (es. Polizia, Carabinieri, Guardia di Finanza, Magistratura), delle informazioni affidate al Fornitore dal Cliente, il Fornitore fornirà al Cliente tempestiva notifica di tale richiesta, tranne nei casi di divieto da parte dell'Autorità stessa.

NOTIFICA DEGLI INCIDENTI

Il Fornitore, in armonia alla procedura di Gruppo per la gestione degli incidenti di tipo "data breach" si impegna a notificare tempestivamente al Cliente gli incidenti di sicurezza informatica (data-breach) rilevati tramite strumenti di monitoraggio e controllo o da segnalazioni, che implichino o consistano in:

- Accessi non autorizzati
- Perdita di dati
- Alterazione di dati
- Diffusione indebita di dati

La notifica avverrà via posta elettronica (al riferimento indicato dal Cliente) o secondo le modalità contrattualizzate, di norma entro il giorno successivo alla rilevazione dell'incidente. Successivamente alla sua chiusura, sarà inviato al Cliente l'Incident Report descrittivo dell'accaduto e delle azioni intraprese.

TRASFERIMENTO O RESTITUZIONE DELLE INFORMAZIONI O RIMOZIONE A FINE CONTRATTO

Il trasferimento delle informazioni ad altro cloud provider, oppure la ri-consegna delle stesse al Cliente, sono garantite dal Fornitore che indirizzerà su base progettuale qualsiasi richiesta del Cliente in tal senso, stimando tempi e costi delle operazioni e sottoponendone proposta al Cliente. L'esecuzione delle attività è subordinata all'accettazione della proposta, e in tutti i casi è seguita dalla cancellazione sicura.

A fine contratto ed in assenza di richieste di trasferimento delle informazioni oppure di riconsegna come sopra descritte, il Fornitore provvede puntualmente alla cancellazione sicura dei dati cliente, con l'eccezione delle registrazioni che vengono ancora conservate secondo i termini di legge.

In ottemperanza alle linee guida di AgID, Municipia segue la procedura di reversibilità dei servizi SaaS pubblicata all'URL **https://confluence.municipia.eng.it/x/AgQ9BQ** .

UTILIZZO DI SUB-FORNITORI

L'utilizzo di sub-fornitori nell'erogazione dei servizi contrattualizzati è vincolato al consenso esplicito del Cliente (specifica lettera firmata o accettazione del Contratto in cui è contemplato l'utilizzo del sub-fornitore), al quale devono essere resi noti:

- il nome del sub-fornitore
- la/e nazione/i nella quale vengono operati i trattamenti delle informazioni

Nel richiedere tale consenso, Il Fornitore garantisce di aver esteso al sub-fornitore (o al "peer" service provider), le informazioni necessarie al rispetto delle norme per la sicurezza delle informazioni e che il sub-fornitore si sia impegnato a rispettarle.

BACKUP E RESTORE

Il backup dei dati Cliente è finalizzato a consentire il ripristino in caso di eventi avversi.

Il servizio di backup/restore è sempre dovuto dal Fornitore al Cliente tranne nei casi in cui, per natura del servizio o per esplicitazione contrattuale, è il Cliente stesso a provvedere autonomamente. Il backup dei dati Cliente, qualora dovuto, viene garantito in duplice copia per tutti i dati. Eventuali deroghe richieste dal Cliente possono riguardare ambienti o dati "non di produzione". Originali e copie dei backup vengono conservati in locazioni (fisiche o logiche) differenti e il trasferimento dei dati in sede diversa avviene solo sotto protezione crittografica. A meno di differenti accordi contrattuali, l'inizio dell'attività di restore dei dati in caso di incidente è sempre garantita, nel caso peggiore, nell'arco del giorno lavorativo successivo all'evento che rende necessario il ripristino. La durata complessiva dell'attività di restore è funzione del volume di dati da ripristinare.

LOGGING

La collezione e conservazione dei log a norma di legge è tipicamente effettuata dal Fornitore, sia direttamente, sia avvalendosi del servizio offerto dai propri sub-fornitori (IaaS e PaaS). I log vengono resi disponibili al Cliente in forma di report "spot", effettuato su richiesta estemporanea del Cliente oppure, se concordato tra i servizi contrattualizzati, in forma di report periodico, o garantendo l'accesso in visione ai dati via rete. In tutti i casi viene garantita la riservatezza delle informazioni nel senso che ogni Cliente ha visibilità esclusivamente dei log relativi a sistemi/servizi di sua pertinenza.

PROPRIETÀ INTELLETTUALI

Il Fornitore si impegna ad erogare servizi in Cloud utilizzando sistemi con installazioni di licenze valide, ove applicabile.

Reclami di pertinenza del Fornitore saranno indirizzati secondo il processo interno di Gestione dei Reclami

CAPITOLO 4

CONDIZIONI GENERALI DI VENDITA

Per quanto non espressamente previsto nel presente documento:

- **per acquisti tramite marketplace (es.MEPA):** si fa espresso rinvio alle condizioni generali di contratto relative al marketplace individuato dall'Ente per l'acquisto
- **per acquisti non effettuati tramite marketplace:** si fa espresso rinvio alla lex specialis di gara e alla normativa vigente.

Appendice 1	Misure tecniche e organizzative secondo l'articolo 30 del regolamento europeo sulla protezione dei dati (Regolamento (UE) 2016/679 - "GDPR") MD15_PGT01_0_Allegato_Caratteristiche_Trattamento_Dati
Prodotto/i	jEnte (SAAS) Jpartecipate Assistenza e Manutenzione | Sviluppo Prodotto

La **suite jEnte** rappresenta la soluzione ERP per la gestione di tutte le attività dell'Ente Locale.

Quanto indicato si riferisce alla suite jEnte nella sua installazione complete (tutte le aree).

Dettagli Trattamento

- Application Maintenance Management
- Network Management
- Funzioni di Amministratore Di Sistema
- Customer Support
- Sviluppo Prodotto

Categorie di Interessati

I Dati Personali trattati riguardano le seguenti categorie di Interessati:

- Clienti privati
- Dipendenti
- Minori

Tipologia di Dati Personali

- Dati personali comuni (es. dati anagrafici, di contatto, relativi all'istruzione, stato civile/familiare, esperienza professionale)
- Dati Finanziari (es. reddito, transazioni finanziarie, investimenti, carte di credito, fatture, ecc.)
- Dati Particolari (es. sulla salute, genetici, biometrici, opinioni politiche, vita sessuale, ecc.)

Caratteristiche del Trattamento

- Partial or Mixed Outsourcing
  - Il trattamento avviene (in toto o in parte) presso la sede del Responsabile
  - Il Responsabile svolge anche o solo attività di Amministratore di Sistema e/o gli accessi sono gestiti dal Responsabile
  - I desktop/laptop/mobile devices (o alcuni di essi) utilizzati per il trattamento sono forniti dal Responsabile
  - Il software/applicazione/ecc. utilizzato per il trattamento è fornito e/o manutenuto dal Responsabile
- Attività a supporto light (laptop/mobile devices forniti dal Titolare)
- Attività a supporto (laptop/mobile devices forniti dal Responsabile)

Misure di Sicurezza

In relazione alla rischiosità del trattamento definita dal Titolare, il Responsabile nell'ambito delle attività contrattualmente previste, garantisce di applicare le seguenti misure di sicurezza, che il Titolare conferma forniscano un adeguato livello di protezione dei Dati Personali in considerazione dei rischi associati al Trattamento dei Dati Personali.

Risk Level	Categoria	ID	Descrizione
B	**Security Policy e procedure per la protezione dei dati personali**	**A.1**	L'organizzazione documenta la propria politica in merito all'elaborazione dei dati personali come parte della sua politica di sicurezza delle informazioni.
B	**Security Policy e procedure per la protezione dei dati personali**	**A.2**	La politica di sicurezza è riesaminata e aggiornata, se necessario, su base annuale.

Risk Level	Categoria	ID	Descrizione
B	**Ruoli e responsabilità**	**B.1**	I ruoli e le responsabilità relativi al trattamento dei dati personali sono chiaramente definiti e assegnati in conformità con la politica di sicurezza.
M	**Ruoli e responsabilità**	**B.3**	E' effettuata una chiara individuazione e designazione delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.
A	**Ruoli e responsabilità**	**B.4**	Il responsabile della sicurezza è nominato formalmente (in modo documentato). Anche i compiti e le responsabilità del responsabile della sicurezza sono chiaramente definiti e documentati.
A	**Ruoli e responsabilità**	**B.5**	Doveri e aree di responsabilità che possono essere in conflitto, ad esempio i ruoli di responsabile della sicurezza, auditor e DPO, sono considerati separati per ridurre le opportunità di modifiche non autorizzate o non intenzionali o di uso improprio di dati personali.
M	**Policy per il controllo degli accessi**	**C.3**	La segregazione dei ruoli per gestire il controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, gestione degli accessi) è chiaramente definita e documentata.
B	**Gestione degli asset/risorse**	**D.1**	L'organizzazione dispone di un registro delle risorse IT utilizzate per il trattamento dei dati personali (hardware, software e rete). Il registro potrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. server, workstation), posizione (fisica o elettronica). Ad una persona specifica è assegnato il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).
B	**Gestione degli asset/risorse**	**D.2**	Le risorse IT sono riesaminate e aggiornate regolarmente.
A	**Gestione degli asset/risorse**	**D.4**	Le risorse IT sono riesaminate e aggiornate su base annuale.
B	**Gestione del cambiamento**	**E.1**	L'organizzazione deve assicurarsi che tutte le modifiche al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, responsabile IT o sicurezza). Questo processo è monitorato regolarmente.
B	**Responsabili del Trattamento**	**F.3**	Fra il titolare del trattamento dei dati e il responsabile del trattamento dei dati sono formalmente concordati requisiti formali e obblighi. Il Responsabile del trattamento dovrebbe fornire prove documentate sufficienti di conformità.
M	**Responsabili del Trattamento**	**F.4**	L'organizzazione Titolare del trattamento dei dati dovrebbe verificare regolarmente la conformità del Responsabile del trattamento al livello concordato di requisiti e obblighi.
A	**Gestione degli incidenti / Data Breaches**	**G.4**	Gli incidenti e le violazioni dei dati personali sono registrati insieme ai dettagli riguardanti l'evento e le successive azioni di mitigazione eseguite.
A	**Business Continuity**	**H.5**	Si prende in considerazione una struttura alternativa, a seconda dell'organizzazione e dei tempi di inattività accettabili del sistema IT.
M	**Formazione**	**J.2**	L'organizzazione dispone di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici (relativi alla protezione dei dati personali) per l'inserimento dei nuovi arrivati.

Risk Level	Categoria	ID	Descrizione
A	**Formazione**	**J.3**	Un piano di formazione con obiettivi e obiettivi definiti è preparato ed eseguito su base annuale.
B	**Controllo degli accessi ed autenticazione**	**K.1**	E' attuato un sistema di controllo accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, il riesame e l'eliminazione degli account degli utenti.
B	**Controllo degli accessi ed autenticazione**	**K.3**	E' presente un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sul sistema di controllo degli accessi). Come minimo è utilizzata una combinazione di user-id e password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità.
B	**Controllo degli accessi ed autenticazione**	**K.4**	Il sistema di controllo degli accessi è in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile).
M	**Controllo degli accessi ed autenticazione**	**K.6**	Le password degli utenti sono archiviate in formato "hash".
B	**Logging e monitoraggio**	**L.1**	I log sono attivati per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).
B	**Logging e monitoraggio**	**L.2**	I log sono registrati con marcatura temporale (timestamp) e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi sono sincronizzati con un'unica fonte temporale di riferimento.
M	**Logging e monitoraggio**	**L.3**	Vengono registrate le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / eliminazione / modifica dei diritti di accesso degli utenti.
M	**Logging e monitoraggio**	**L.4**	Non c'è alcuna possibilità di cancellazione o modifica del contenuto dei log. Anche l'accesso ai log è registrato oltre al monitoraggio per rilevare attività insolite.
B	**Server/Database security**	**M.1**	I database e application server sono configurati affinché lavorino con un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.
B	**Network/Communication security**	**O.1**	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione è crittografata tramite protocolli crittografici (TLS / SSL).
M	**Network/Communication security**	**O.2**	L'accesso wireless al sistema IT è consentito solo a utenti e processi specifici. E' protetto da meccanismi di crittografia.
A	**Network/Communication security**	**O.6**	La rete IT è separata dalle altre reti del titolare.
B	**Back-ups**	**P.2**	Ai backup è assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.

Risk Level	Categoria	ID	Descrizione
B	**Back-ups**	**P.3**	L'esecuzione dei backup è monitorata per garantire la completezza.
B	**Back-ups**	**P.4**	I backup completi sono eseguiti regolarmente.
M	**Back-ups**	**P.5**	I supporti di backup sono testati regolarmente per assicurarsi che possano essere utilizzati.
M	**Back-ups**	**P.6**	I backup incrementali programmati sono eseguiti almeno su base giornaliera.
M	**Back-ups**	**P.7**	Le copie del backup sono conservate in modo sicuro in luoghi diversi dai dati di origine.
B	**Sicurezza del ciclo di vita del software**	**R.4**	Sono seguiti standard e pratiche di codifica sicure.
M	**Sicurezza del ciclo di vita del software**	**R.6**	I vulnerability assessment, i penetration test applicativi e dell'infrastruttura sono eseguiti da una terza parte fidata prima del passaggio in ambiente di produzione. Il passaggio non può avvenire a meno che non sia raggiunto il livello di sicurezza richiesto.
M	**Sicurezza del ciclo di vita del software**	**R.7**	Sono eseguiti penetration test periodici.
M	**Sicurezza del ciclo di vita del software**	**R.8**	Si ottengono informazioni sulle vulnerabilità tecniche dei sistemi IT utilizzati.
M	**Sicurezza del ciclo di vita del software**	**R.9**	Le patch software sono testate e valutate prima di essere installate in ambiente di produzione.
B	**Sicurezza fisica**	**T.1**	Il perimetro fisico dell'infrastruttura IT non è accessibile da personale non autorizzato.
M	**Sicurezza fisica**	**T.2**	L'identificazione chiara, tramite mezzi appropriati, ad es. badge identificativi, per tutto il personale e i visitatori che accedono ai locali dell'organizzazione, è stabilita, a seconda dei casi.
M	**Sicurezza fisica**	**T.3**	Le zone sicure sono definite e protette da appropriati controlli di accesso. Un registro fisico o una traccia elettronica di controllo di tutti gli accessi sono mantenuti e monitorati in modo sicuro
M	**Sicurezza fisica**	**T.4**	I sistemi di rilevamento anti-intrusione sono installati in tutte le zone di sicurezza.

Risk Level	Categoria	ID	Descrizione
M	**Sicurezza fisica**	**T.5**	Le barriere fisiche sono costruite per impedire l'accesso fisico non autorizzato.
M	**Sicurezza fisica**	**T.6**	Le aree non usate sono fisicamente bloccate e periodicamente riesaminate.
M	**Sicurezza fisica**	**T.7**	Un sistema antincendio automatico, un sistema di climatizzazione dedicato e chiuso e un gruppo di continuità (UPS) sono usati nella sala server.
M	**Sicurezza fisica**	**T.8**	Il personale di supporto esterno ha accesso limitato alle aree protette.

Appendice 2	**Elenco Sub-Responsabili** MD14_PGT01_0_Allegato_Elenco_SubResponsabili
Prodotto/i	jEnte (SAAS)- Jpartecipate Assistenza e/o Manutenzione | Sviluppo Prodotto

Accettando la presente proposta il Titolare autorizza il Responsabile ad affidare parte delle operazioni di trattamento ai seguenti ulteriori sub-responsabili indicati per ciascun prodotto di riferimento.

Paese cui è stabilito Sub-Responsabile	Sub-Responsabili	Dati di contatto	Attività di trattamento affidata
Irlanda	AWS	https://aws.amazon.com/compliance/gdpr-center/	Service Provider (CSP qualificato AGID)

Qualora il Responsabile intendesse affidare ad un sub-responsabile trattamenti 'diversi' rispetto a quelli indicati in tabella e/o nell'offerta e/o nel contratto principale, o ingaggiare altri sub-responsabili diversi da quelli sopra indicati, provvederà a comunicare tali variazioni al Titolare.

Appendice 3	Scheda Evento Data Breach MD16_PGT01_0_Allegato_Scheda_Evento_Data_Breach

Denominazione della Banca Dati oggetto di incidente e breve descrizione della violazione

Quando si è verificata la violazione dei dati personali nell'ambito della Banca dati?

☐ il__/__/____

☐ tra il __/__/____e __/__/____

☐ in un periodo non ancora determinato

☐ E' possibile sia ancora in corso

Dove è avvenuta la violazione?
(specificare se avvenuta a seguito di smarrimento dispositivo o di supporto portatile)

Tipo Violazione

☐ Riservatezza (divulgazione dei dati, accesso agli stessi non autorizzati o accidentali)
☐ Integrità (modifica non autorizzata o accidentale dei dati)
☐ Disponibilità (perdita, accesso o distruzione accidentali o non autorizzati di dati)
☐ Lettura (i dati probabilmente non sono stati copiati)
☐ Copia (i dati sono ancora presenti sui sistemi del Titolare)
☐ Alterazione (i dati sono presenti nei sistemi ma sono stati alterati)
☐ Cancellazione (i dati non sono più nella disponibilità del Titolare o di terzi)
☐ Furto
☐ Altro:

Dispositivo oggetto della violazione

☐ Computer
☐ Rete
☐ Dispositivo mobile
☐ Strumento di Backup
☐ Documento Cartaceo
☐ Altro:

Sintetica descrizione dei sistemi di elaborazione e/o memorizzazione dati coinvolti

Ubicazione:

Quante persone sono state colpite dalla violazione

☐ N°_____persone
☐ Circa _____
☐ N° non ancora conosciuto:

Tipologia Dati Oggetto Di Violazione

☐ Dati anagrafici
☐ Dati di accesso/ identificazione
☐ Dati relativi a minori
☐ Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche ecc
☐ Dati personali idonei a rivelare lo stato di salute e la vita sessuale
☐ Dati Giudiziari
☐ Copia immagini documenti digitali
☐ Ancora sconosciuto
☐ Altro

Misure tecniche ed organizzative applicate ai dati oggetto di violazione
(indicare le misure di sicurezza implementate prima del verificarsi dell'evento che dovrebbero coincidere con quelle riportate nell'apposito accordo per il trattamento dei dati)

Quali misure tecnologiche ed organizzative sono state assunte o saranno assunte per contenere la violazione dei dati e/o prevenire simili violazioni
(indicare le misure di sicurezza adottate per arginare gli effetti della gli effetti della violazione e/o impedirne il perpetrarsi o il ripersi della stessa)

Gestione Partecipate

La soluzione a supporto del monitoraggio delle società partecipate e della formulazione del Bilancio Consolidato

Il **procedimento di esternalizzazione** (c.d. outsourcing) di un servizio pubblico costituisce una scelta strategica, operata dall'Amministrazione Pubblica, per l'organizzazione e la gestione di un'area di attività o di servizi, in vista del raggiungimento di standard qualitativi elevati.

Il gestore del servizio esternalizzato deve essere messo in condizione di perseguire un risultato efficiente; ma, al contempo, devono essere previsti **efficaci strumenti di controllo**, così che la gestione del servizio sia funzionale all'interesse generale della collettività.

Il monitoraggio dell'Ente deve essere **continuo e costante**. Addirittura, con riferimento alle proprie **società in house**, ossia le società a cui vengono affidati direttamente servizi senza l'espletamento di una procedura a evidenza pubblica, l'Ente esercita **un controllo c.d. analogo**, cioè un controllo uguale a quello che l'Amministrazione esercita sui propri servizi.

Considerato pertanto il ruolo di guida dell'Amministrazione che esternalizza, occorre individuare le modalità organizzative e gli strumenti operativi funzionali all'azione di monitoraggio e controllo concentrando l'attenzione verso il perseguimento di elevati standard qualitativi dei servizi.

La valutazione circa il miglior modello di *governance* da adottare, al fine di garantire un buon servizio al cittadino e la soddisfazione delle sue esigenze, **deve essere compiuta nell'azione pratica, ma soprattutto deve essere previsto un monitoraggio continuo della scelta effettuata, in modo da apportare tempestivamente gli opportuni correttivi.**

L'Amministrazione Pubblica non è più gestore, ma si pone come regolatrice delle attività di soggetti autonomi, sebbene ad essa legati, conservando tutta una serie di **responsabilità giuridiche e politiche**.

L'art. **147-quater** del TUEL prevede un **caso particolare e specifico** di controllo dell'ente locale sulle proprie società partecipate non quotate che fa carico obbligatoriamente agli enti locali con popolazione superiore a 15.000 abitanti di dotarsi di una modalità di controllo tale da permettere:

- di svolgere un **monitoraggio periodico** sull'andamento delle suddette società;
- di verificare il **rispetto degli obiettivi gestionali** definiti dall'Ente stesso;
- attraverso un adeguato sistema informativo e di controllo, di rilevare:
  - i rapporti finanziari tra l'ente e la società;
  - verificare la situazione contabile, gestionale e organizzativa della società;
  - i contratti di servizio;
  - la qualità dei servizi;
  - il rispetto delle norme di legge sui vincoli di finanza pubblica.

Il sistema delineato dall'art. 147-quater ha contribuito a rafforzare l'orientamento giurisprudenziale incline a rinvenire in capo all'ente locale l'obbligo di esercitare **una verifica effettiva e non meramente formale** sulla gestione delle partecipate, e la correlata responsabilità per l'eventuale dissesto.

Il Gruppo Amministrazione Pubblica va quindi considerato come un'entità unitaria, ancorché costituita da più soggetti giuridici. In tale contesto si inserisce il bisogno di redigere un bilancio di gruppo che permetta ai lettori dello stesso di avere informazioni trasparenti e complete e una visione chiara dell'andamento dell'ente e dei suoi organismi/società satellite.

L'allegato 4/4 del d.lgs. n. 118 del 2011 prevede che le Amministrazioni pubbliche redigano un bilancio consolidato che rappresenti in modo veritiero e corretto la situazione finanziaria e patrimoniale e il risultato economico della complessiva attività svolta dall'ente attraverso le proprie articolazioni organizzative e i propri enti strumentali e società controllati e partecipati. In particolare, il bilancio consolidato deve consentire di:

a) sopperire alle carenze informative e valutative dei bilanci degli enti che perseguono le proprie funzioni anche attraverso enti strumentali e che detengono rilevanti partecipazioni in società, dando una rappresentazione, anche di natura contabile, delle proprie scelte di indirizzo, pianificazione e controllo;
b) attribuire all'Amministrazione capogruppo un nuovo strumento per programmare, gestire e controllare con maggiore efficacia il proprio gruppo comprensivo di enti e società;
c) ottenere una visione completa delle consistenze patrimoniali e finanziarie di un gruppo di enti e società che fa capo a un'Amministrazione pubblica, incluso il risultato economico.

La redazione del bilancio consolidato, quindi, risponde a diverse esigenze informative. Da un lato, quella legata alla governance esterna dell'Amministrazione pubblica: gli amministratori necessitano di informazioni per l'attuazione di strategie, progetti e programmi dell'Amministrazione pubblica (secondo il principio di utilità, per cui il bilancio deve servire ad assumere decisioni corrette); dall'altro quella connessa alla necessità di informare i cittadini in modo chiaro, completo e corretto circa l'andamento e i risultati raggiunti dall'Amministrazione pubblica, nonché i costi legati ai servizi forniti (secondo il principio di *accountability*, che si riferisce alla responsabilità degli amministratori e funzionari che utilizzano risorse pubbliche e alla documentazione dell'utilizzo del denaro pubblico in funzione della verifica di efficienza ed efficacia della gestione); dall'altro ancora, quella legata alla necessità di fornire alla Corte dei conti uno strumento utile all'attività di controllo.

LA SOLUZIONE

In risposta alle sempre più stringenti necessità di supportare il processo di corretta applicazione delle norme e dei principi alla base del contesto normativo di riferimento, Municipia ha realizzato una piattaforma completa ed integrata finalizzata a supportare le Pubbliche Amministrazioni Locali nella determinazione di tutti quei processi operativi alla base del lavoro quotidiano delle strutture preposte, in grado di rappresentare la base dati informativa unica alla base di tutti gli adempimenti interni ed esterni all'Amministrazione.

I servizi applicativi in oggetto sono erogati, in linea con le ultime linee guida/riferimenti operativi di settore, in modalità Cloud presso CSP certificato AGID, attraverso un setup architetturale applicativo e infrastrutturale in grado di garantire il rispetto dei paradigmi di business continuity e sicurezza applicativa. In particolare le componenti applicative sono realizzate sulla base del framework Spring Boot/Angular HTML5/responsive compliant.

Principali obiettivi della soluzione

Obiettivo	Strumenti a supporto
Monitoraggio e controllo	Le Partecipate alimentano una banca dati unificata, mediante la compilazione di una serie di dati strutturati ed informazioni varie. Il sistema permette all'Amministrazione di acquisire estrazioni ed elaborazioni, proponendo uno strumento di supporto per i processi decisionali e gli adempimenti richiesti.
Certificazione delle informazioni	Definizione di una piattaforma dinamica all'interno della quale l'alimentazione dei dati è a cura delle Partecipate. L'Amministrazione governa in primo piano il processo di raccolta dati (attraverso la sezione Cruscotto di Monitoraggio). I dati e le informazioni raccolte sono sottoposte ad iter di certificazione e trasmesse all'Amministrazione secondo le modalità operative successivamente regolamentate dalla medesima.
Definizione del perimetro di pertinenza dei dati trattati	La piattaforma garantisce la gestione di diversi profili di accesso corrispondenti a differenti livelli di visibilità e di trattamento delle informazioni contenute nella banca dati. Le informazioni derivanti dalla profilazione migliorano la performance e l'ottimizzazione del flusso di lavoro.
Banca dati unificata	Il sistema rappresenta un vero e proprio Repository di archiviazione di tutti i documenti significativi inerenti l'Organismo Partecipato, dei dati di bilancio, dei dati anagrafici e dei contratti di servizio stipulati. Prevede l'archiviazione della relativa documentazione in un unico ambiente facilitandone il reperimento e la consultazione.
Planning	Pianificazione strategica**,** sezione contente le Informazioni quali ad esempio le attività svolte dalla Partecipata per l'Ente (Servizi affidati) con riferimento alla missione/programma del bilancio dell'Ente di riferimento, il valore del contratto e la durata dello stesso. Funzione di upload del Piano Gestionale Annuale e del Piano Industriale Pluriennale.
Monitoraggio degli SLA contrattuali	**Contratti di servizio**, sezione contente informazioni relative ad: • Obiettivi previsti dal contratto (economici, qualitativi, gestionali, modalità di fatturazione e di pagamento) • Adempimenti relativi alle Certificazioni obbligatorie previste dal contratto • Funzione di upload/download dei file relativi a tale Documentazione.
Raccolta dei dati di Bilancio	Sezione contente i dati di bilancio ovvero conto economico e stato patrimoniale (previsionale, infrannuale e consuntivo) delle Partecipate redatti secondo gli schemi contabili vigenti.

Riclassificazione di Bilancio ed Indicatori	Sezione in cui l'utente ha a disposizione diverse funzioni per la verifica della solidità delle Partecipate attraverso indicatori economico finanziari e patrimoniali. Inoltre, è data la possibilità di creare nuovi indicatori afferenti al bilancio riclassificato. E' eventualmente possibile prevedere indicatori di qualità predisposti dall'Ente relativamente agli obiettivi dei contratti di servizio nel suo complesso e dei singoli servizi. Tali indicatori potranno essere di tipo domanda/risposta che stabiliscono soglie minime per il raggiungimento degli obiettivi qualitativi.
Riconciliazione Debiti- Crediti	La sezione 'Riconciliazione' mette a disposizione funzionalità che consentono la verifica dei rapporti di debito e credito intercorrenti tra l'Ente Capogruppo e le proprie Partecipate. Consente analiticamente di evidenziare eventuali discordanze, per le quali dovranno essere adottati i provvedimenti necessari ai fini della riconciliazione delle partite debitorie e creditorie.
Scadenzario	Gestione delle scadenze collegate ad ogni Partecipata. A seguito del censimento degli Organi Sociali nella sezione Anagrafica, automaticamente tale sezione alimenta lo Scadenzario. E' possibile ricevere via email la notifica delle scadenze imminenti e tenere così sotto controllo le varie deadlines relative alle nomine collegiali e consiliari, ai contratti,... Le notifiche di inizio e la frequenza delle stesse vengono preimpostate dall'Amministrazione.
Perimetro di consolidamento	Il sistema identifica in automatico i componenti del "Gruppo Amministrazione Pubblica" e le partecipate che rientrano nell'area di consolidamento, rispettivamente Elenco n.1 ed Elenco n.2 (elenchi obbligatori per legge). Tramite automatismi viene inviata una email alle partecipate che rientrano nel perimetro con in allegato la Delibera di Giunta e avvio del processo di raccolta dati per il consolidamento.
Conversione degli schemi	Tramite upload del bilancio consuntivo/consolidato del file in formato xbrl il sistema consente di pre-popolare i dati di bilancio. Il sistema esegue la conversione del bilancio dallo schema IV Direttiva CEE allo schema D.Lgs. 118/2011.
Operazioni Intercompany	Gestione delle scritture di consolidamento (elisioni e le rettifiche) in modalità guidata o manuale. Definizione dell'aggregato provvisorio di partenza, elenco scritture di consolidamento e definizione volta per volta dell'aggregato fino all'ottenimento del bilancio consolidato dell'Ente Capogruppo (applicazione regole sulla base delle modalità di consolidamento definite).
Elaborazione degli output normativi	Elaborazione del bilancio consolidato dell'Ente Capogruppo. Elaborazione della Nota Integrativa le cui tabelle sono parametrizzate sulla base dei risultati ottenuti dal bilancio consolidato. Elaborazione file xbrl valido per upload del bilancio consolidato in BDAP.