Municipia S.p.A.

Sede legale:
38122 Trento - Via Adriano Olivetti, 7
Tel. 0461.158501 -Fax 0461.1585039
Codice fiscale 01973900838 - P. IVA 01973900838
R.E.A. TN - 209533
Registro Imprese Trento 01973900838
Capitale Sociale Euro 13.000.000,00 i.v.
società con socio unico

municipia@eng.it – municipia@pec.eng.it
www.municipia.eng.it
www.eng.it

Spettabile

Ente/Azienda
COMUNE DI CREMONA
Via Gallarati, 1 - CR

Riccardo Orsoni riccardo.orsoni@comune.cremona.it

INVIATA TRAMITE PEC *protocollo@comunedicremona.legalmail.it*

Bologna, 27 Ottobre 2020 | Rif. n. SR 177202

Oggetto: Contratto di servizio Assistenza e Manutenzione prodotti software Linea **jEnte** erogati **OnPremise-Home**

In allegato alla presente trasmettiamo il contratto di manutenzione e assistenza che può essere sottoscritto in forma:

- **annuale 2021:** in questo caso il servizio viene erogato per un anno ai prezzi indicati
- **triennale 2021-2023:** a parità di perimetro dell'installato i canoni non subiranno aumenti fino alla scadenza contrattuale. La fatturazione è annuale. Non devono essere espletate tre pratiche amministrative separate da parte dell'Ente ma una sola.

L' adesione – in base alla formula desiderata (annuale o triennale) - deve essere formalizzata entro e non oltre il **31/12/2020.** Evidenziamo l'importanza di rinnovare il contratto entro la scadenza indicata inoltrando il modulo d'ordine firmato in tutte le sue parti. La sottoscrizione include anche **l'accordo al "trattamento dati" indispensabile per l'erogazione del servizio.**

All'interno della presente proposta sono indicate anche le quotazioni per i **pacchetti di giornate di assistenza** il cui prezzo diminuisce in relazione al numero di giornate acquistate.

Cordiali saluti.

Municipa SpA
Il Procuratore

Firmato digitalmente da: PAOLO DOMENEGHETTI
Data: 29/10/2020 10:25:32

MUNICIPIA
GRUPPO ENGINEERING

CONTRATTO SERVIZIO ASSISTENZA E MANUTENZIONE PRODOTTI SOFTWARE LINEA JENTE

EROGATI IN ON PREMISE – HOME

Dati societari

MUNICIPIA S.p.A.

con sede legale in Trento – Via Adriano Olivetti, 7 - 38122, codice fiscale e numero di iscrizione del Registro delle Imprese di Trento 01973900838, iscritta al REA della CCIAA n° 209533, partita IVA n. 01973900838.

e

ENTE/AZIENDA

COMUNE DI CREMONA

con sede in *Via Gallarati, 1 COMUNE DI CREMONA CR - P.I./C.F. 00297960197*

Obbligo di riservatezza

Le informazioni contenute nel presente documento devono ritenersi strettamente confidenziali l'Amministrazione Comunale è tenuta, pertanto:

- a non utilizzarle per finalità diverse dalla valutazione della proposta;
- a 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;
- a non copiarle, riprodurle, duplicarle, senza il preventivo consenso scritto di Municipia

Contatto in Municipia

Per qualsiasi esigenza relativa a questa proposta, vogliate contattare:

per gli aspetti economici €

Cesare Rovati (Account Manager)

e-mail cesare.rovati@eng.it
mobile 3462359608

per gli aspetti tecnico operativi

Roberto Blasioli (Referente Tecnico)

e-mail roberto.blasioli@eng.it
mobile 3492712085

INDICE DEI CAPITOLI

1. PROPOSTA TECNICA _____ 5
2. PROPOSTA ECONOMICA – MODULO D'ORDINE _____ 12
3. CONDIZIONI SPECIFICHE DI FORNITURA _____ 12
4. CONDIZIONI GENERALI DI VENDITA _____ 21

1. PROPOSTA TECNICA

Questa proposta tecnica descrive le attività svolte da Municipia a seguito della sottoscrizione della "Commissione di Abbonamento" per il servizio di manutenzione e assistenza ai prodotti software utilizzati dall'Ente ed indicati nel Modulo d'Ordine.

Il servizio prevede l'esecuzione di tutte le attività che garantiscono il buon funzionamento degli applicativi da un punto di vista correttivo, adeguativo e migliorativo.

A queste attività si aggiunge l'erogazione del servizio di supporto al Cliente affinché possa utilizzare al meglio e nella piena consapevolezza tutte le funzionalità garantite dagli applicativi.

1.1. SERVIZIO DI MANUTENZIONE

In questa sezione 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 attraverso pacchetti di installazione ad attivazione manuale, i quali aggiornano automaticamente software e database.

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

1.2. 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.

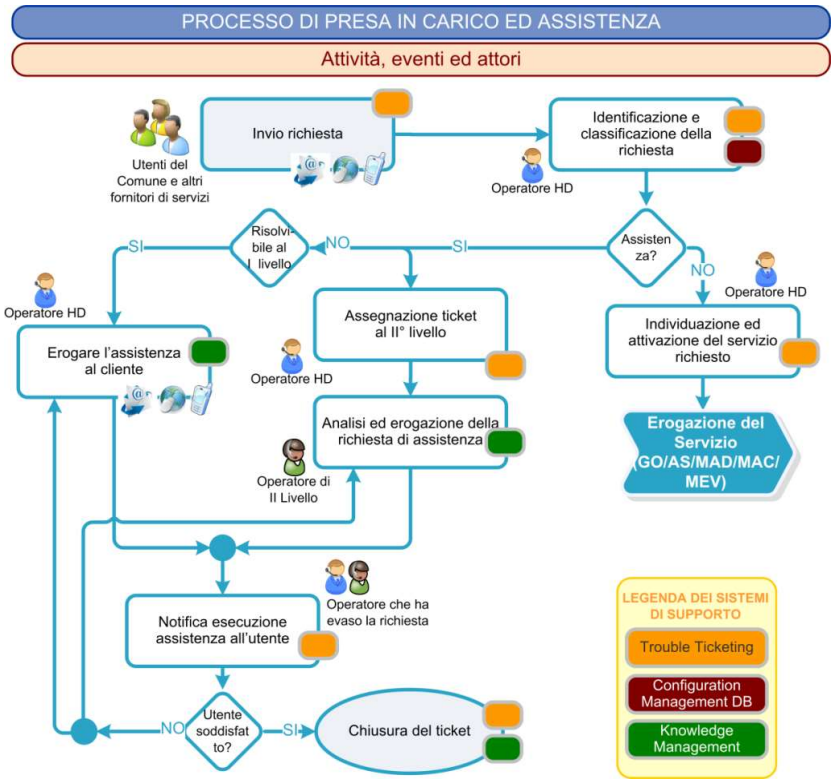
Resta in ogni caso in carico agli operatori Municipia, addetti al servizio di assistenza, la modifica della priorità d'intervento in base alla reale criticità della segnalazione.

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



1.3. 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 di oosservazione 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		

1.4. 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	470,00	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**

2. PROPOSTA ECONOMICA – MODULO D'ORDINE

L' Ente/Azienda **COMUNE DI CREMONA**
Prov. CR - **P.I./C.F.** 00297960197 - **Pec** protocollo@comunedicremona.legalmail.it
Richiede di accedere ai servizi di seguito riportati per i quali sarà emessa la fatturazione di riferimento.

Barrare la casella per il periodo scelto	☐	☐
SUITE jEnte – Aree e Moduli n.b. per i prodotti installati sono indicati i canoni da corrispondere per il periodo scelto.	CANONE ANNUO 2021	CANONE TRIENNIO 2021 -2023
Nucleo Informativo Centrale: Nucleo Informativo Centrale;Catasto Unità Immobiliari;Gestione Entrate Attese;Connettore Conservazione;	€ 2.655,94	€ 7.967,82
Segreteria Affari Generali: Gestione Atti ;Trasparenza amministrativa;Pubblicazione Atti in WEB;	€ 2.987,92	€ 8.963,76
Risorse Umane: Gestione Risorse Umane (Giuridica ed Economica);Modello 770 - Unico;	€ 6.639,84	€ 19.919,52
Pianificazione e Controllo di Gestione: Pianificazione Strategica e Controllo per Obiettivi;Controllo di Gestione per C/Costo;	€ 4.979,88	€ 14.939,64
Servizi Finanziari : Contabilità Finanziaria;Contabilità Economico Patrimoniale;Contabilità Analitica;Siope+;Mutui;Cespiti Patrimoniali;Movimentazione Magazzini;Cassa Economo e Agenti Contabili Diversi;Fatturazione Attiva;SDI link documenti attivi;SDI link documenti passivi;	€ 15.769,62	€ 47.308,86
Tributi: ICI-IMU;TIA/TARES/TARI;Altri tributi gestiti a misura e categoria tariffaria;	€ 8.299,80	€ 24.899,40
Totale	**€ 41.333,00**	**€ 123.999,00**

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).

In allegato delibera/determina n°	Data	CIG	Codice Univoco Ufficio

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. – 2. 3. – 4. 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

3. CONDIZIONI SPECIFICHE DI FORNITURA

3.1. OGGETTO DELLA COMMISSIONE DI ABBONAMENTO

Oggetto della commissione di abbonamento è l'erogazione da parte di Municipia dei servizi di manutenzione e assistenza ai prodotti software utilizzati dal Cliente che ha aderito alla presente proposta.

3.2. 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.

Al link seguente è specificato il processo di reversibilità seguito da Municipia **https://confluence.municipia.eng.it/pages/viewpage.action?pageId=87884802**.

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.

3.3. 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 sui quali sono installati i programmi assistiti
- 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 aggiornate le versioni dei prodotti applicativi; in caso contrario il Municipia non si ritiene obbligato ad assistere il Cliente per versioni inferiori all'ultima disponibile
- mantenere il proprio personale aggiornato sulle evoluzioni dei prodotti oggetto di assistenza da parte di Municipia
- garantire al personale di Municipia l'accesso alla documentazione di servizio, sia in lettura sia in aggiornamento, anche con accesso remoto.

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.

3.4. ADESIONE - DURATA – RECESSO

L’**adesione** al contratto deve avvenire al massimo entro il **31/12/2020**.

In caso di mancata adesione nei termini sopra indicati, Municipia potrà sospendere l’erogazione dei servizi di assistenza e invio aggiornamenti a decorrere dal 1° Gennaio.

A seguito della mancata adesione Municipia procederà, dandone apposita comunicazione al Cliente, a disabilitare le credenziali di accesso al servizio.

Si specifica che in caso di mancata sottoscrizione del presente documento che contiene l’accordo per il trattamento dei dati, Municipia non potrà proseguire detto trattamento.

Il contratto ha la durata indicata dal cliente 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 la “commissione di abbonamento” per il rinnovo del periodo successivo a quello di riferimento oggetto del presente contratto.

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 a disabilitare le credenziali di accesso al servizio. Il recesso potrà essere esercitato dal Cliente per iscritto a mezzo pec o raccomandata a/r.

3.5. CORRISPETTIVI

Il corrispettivo del servizio Manutenzione e Assistenza è indicato al netto di IVA e sarà fatturato in unica rata annuale anticipata per quanto di competenza di ogni singolo anno.
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.

3.6. ESCLUSIONI

Non costituiscono oggetto del presente contratto:

- il supporto di assistenza eventualmente richiesto presso la sede del Cliente (on site);

- le 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.
- il supporto specialistico

3.7. 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**.

In particolare, ciascuna Parte si impegna sin d'ora, nel caso in cui per l'esecuzione del Contratto sia tenuta a trattare dati personali di terzi per conto dell'altra Parte, a farsi designare da quest'ultima, senza alcun onere aggiunto per alcuna Parte, quale Responsabile del Trattamento a norma dell'art. 28 del Regolamento UE, con apposito atto da allegarsi al 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.

3.8. ACCORDO TRATTAMENTO DATI PERSONALI

L'Ente/Anzienda 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.

3.8.1. 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.

3.8.2. 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.

3.8.3. 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.

3.8.4. 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** *(presente solo nel caso in cui è da compilare per presenza di sub-responsabili).*

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.

3.8.5. 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.

3.8.6. 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.

3.8.7. 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.

3.8.8. 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.

3.8.9. 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.

3.8.10. 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.

3.8.11. 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 – 38122 Trento (TN) – pec: municipia.supportovendita@pec.it
- **per il Titolare del trattamento**: COMUNE DI CREMONA - Via Gallarati, 1 - (CR) – pec: protocollo@comunedicremona.legalmail.it.

3.9. 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.

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 di sicurezza, tecniche e organizzative
Prodotto/i	**jEnte On Premise – Assistenza e Manutenzione**

Dettagli Trattamento

Application Maintenance Management

Funzioni di Amministratore Di Sistema

Customer Support

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

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.)

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

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.
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.
B	**Policy per il controllo degli accessi**	**C.1**	I diritti specifici di controllo dell'accesso sono assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza.
M	**Policy per il controllo degli accessi**	**C.2**	Una politica di controllo degli accessi è dettagliata e documentata. L'organizzazione dovrebbe determinare in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti nel contesto dei processi e delle procedure relative ai 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.
A	**Policy per il controllo degli accessi**	**C.4**	I ruoli con diritti di accesso privilegiato sono chiaramente definiti e assegnati limitatamente a membri specifici dello staff.
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.

Risk Level	Categoria	ID	Descrizione
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.
M	**Gestione del cambiamento**	**E.3**	E' presente una politica dettagliata e documentata di gestione dei cambiamenti. Dovrebbe includere: un processo per l'introduzione dei cambiamenti, i ruoli / utenti che hanno i diritti di cambiamento, le tempistiche per l'introduzione dei cambiamenti. La politica di getione dei cambiamenti è regolarmente aggiornata.
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.
B	**Gestione degli incidenti / Data Breaches**	**G.1**	È definito un piano di risposta agli incidenti con procedure dettagliate per garantire una risposta efficace e ordinata agli incidenti relativi ai dati personali.
B	**Gestione degli incidenti / Data Breaches**	**G.2**	Le violazioni dei dati personali sono segnalate immediatamente alla Direzione. Sono in atto procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi dell'art. 33 e 34 GDPR.
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.
B	**Business Continuity**	**H.1**	L'organizzazione dovrebbe stabilire le procedure e i controlli principali da seguire al fine di garantire il livello richiesto di continuità e disponibilità del sistema informatico che elabora i dati personali (in caso di incidente / violazione dei dati personali).
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.
B	**Formazione**	**J.1**	L'organizzazione garantisce che tutto il personale sia adeguatamente informato sui controlli di sicurezza del sistema informatico relativi al suo lavoro quotidiano. Il personale coinvolto nel trattamento dei dati personali dovrebbe inoltre essere adeguatamente informato in merito ai requisiti in materia di protezione dei dati e agli obblighi legali attraverso regolari campagne di sensibilizzazione.

Risk Level	Categoria	ID	Descrizione
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.
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	**Sicurezza desktop/laptop/mobile**	**N.2**	Le applicazioni anti-virus e le relative signatures sono configurate su base settimanale.
B	**Sicurezza desktop/laptop/mobile**	**N.4**	Il sistema dovrebbe avere timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.
B	**Sicurezza desktop/laptop/mobile**	**N.5**	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema sono installati regolarmente.

Risk Level	Categoria	ID	Descrizione
M	**Sicurezza desktop/laptop/mobile**	**N.6**	Le applicazioni antivirus e le signature sono configurate su base giornaliera.
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.
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.
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 3	Scheda Evento Data Breach
Prodotto/i	**jEnte On Premise**

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)

_____

_____