COMUNE DI CASTEL IVANO

PROVINCIA DI TRENTO

DETERMINAZIONE DEL RESPONSABILE

SERVIZIO SEGRETERIA

N. 85

DI DATA 02/11/2023

Oggetto: **PNRR MISSIONE 1 COMPONENTE 1 INVESTIMENTO 1.2 "ABILITAZIONE AL CLOUD PER LE PA LOCALI COMUNI (LUGLIO 2022)" FINANZIATO DALL'UNIONE EUROPEA - NEXTGENERATION EU (CUP G51C22000750006). AFFIDAMENTO ALLA DITTA MUNICIPIA SPA SERVIZIO DI MIGRAZIONE AL CLOUD APPLICATIVO LINEA J-ENTE (CIG ZF83D11089)**

Assunta da:

IL SEGRETARIO COMUNALE

Feller dott.ssa Lucia

Documento informatico sottoscritto con firma digitale
ai sensi degli artt. 20 e 21 del D.Lgs. n. 82/2005 e ss.mm.ii.

Finanziato dall'Unione europea
NextGenerationEU

OGGETTO: PNRR MISSIONE 1 COMPONENTE 1 INVESTIMENTO 1.2 “ABILITAZIONE AL CLOUD PER LE PA LOCALI COMUNI (LUGLIO 2022)” FINANZIATO DALL’UNIONE EUROPEA - NEXTGENERATIONEU (CUP G51C22000750006). AFFIDAMENTO ALLA DITTA MUNICIPIA SPA SERVIZIO DI MIGRAZIONE AL CLOUD APPLICATIVO LINEA J-ENTE (CIG ZF83D11089)

IL SEGRETARIO COMUNALE

Premessa

In data 13 luglio 2021, in seguito alla Decisione di esecuzione del Consiglio UE-ECOFIN, è stata approvata la Valutazione del Piano Nazionale di Ripresa e Resilienza dell’Italia;

Con il decreto-legge del 31 maggio 2021 nr. 77, convertito con modificazioni dalla legge 29 luglio 2021 nr. 108 «Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure», sono state definite la strategia e il sistema di governance nazionali per l'attuazione degli interventi relativi al Piano Nazionale di Ripresa e Resilienza e al Piano Nazionale per gli investimenti complementari; il Decreto, inoltre, ha definito il quadro normativo nazionale finalizzato a semplificare e agevolare la realizzazione dei traguardi e degli obiettivi stabiliti dal Piano Nazionale di Ripresa e Resilienza, di cui al Regolamento (UE) 2021/241 del Parlamento Europeo e del Consiglio del 12 Febbraio 2021, dal Piano Nazionale per gli investimenti complementari di cui al Decreto-Legge 6 maggio 2021 n. 59, nonché dal Piano Nazionale Integrato per l'Energia e il Clima 2030 di cui al Regolamento (UE) 2018/1999 del Parlamento Europeo e del Consiglio dell'11 dicembre 2018.

Con il decreto del Ministro dell’economia e delle finanze del 6 agosto 2021 è stata disposta l'assegnazione delle risorse finanziarie per l'attuazione dei singoli interventi del PNRR alle Amministrazioni centrali titolari, indicando la somma complessiva spettante a ciascuna di esse e la ripartizione di traguardi e obiettivi per scadenze semestrali di rendicontazione.

Il PNRR contiene misure e finanziamenti per il sostegno della ripresa economica e per lo sviluppo sostenibile del Paese dopo la pandemia. In particolare:

- Il Piano Nazionale di Ripresa e Resilienza (PNRR) contiene un pacchetto coerente di riforme strutturali e di investimenti per il periodo 2021-2026. I progetti di investimento sono suddivisi in 16 componenti, raggruppate a loro volta in 6 missioni:
  1. Digitalizzazione, innovazione, competitività, cultura e turismo;
  2. Rivoluzione verde e transizione ecologica;
  3. Infrastrutture per una mobilità sostenibile;
  4. Istruzione e ricerca;
  5. Coesione e inclusione;
  6. Salute e Resilienza.
- All’interno delle suddette missioni è previsto un ampio spettro di investimenti e riforme a favore dei Comuni italiani, che vanno dal digitale al turismo, dal miglioramento dell’organizzazione interna agli interventi sociali; che le amministrazioni territoriali concorrono a realizzare il PNRR anche attraverso la diretta titolarità di specifiche progettualità (beneficiari/soggetti attuatori) e la loro concreta realizzazione, assumendo in tal caso la responsabilità della gestione dei singoli Progetti, sulla base degli specifici criteri e modalità stabiliti nei provvedimenti di assegnazione delle risorse adottati dalle Amministrazioni centrali titolari degli interventi.
- Le amministrazioni territoriali concorrono a realizzare il PNRR anche attraverso la diretta titolarità di specifiche progettualità (beneficiari/soggetti attuatori) e la loro concreta

realizzazione, assumendo in tal caso la responsabilità della gestione dei singoli Progetti, sulla base degli specifici criteri e modalità stabiliti nei provvedimenti di assegnazione delle risorse adottati dalle Amministrazioni centrali titolari degli interventi; in tale ipotesi gli enti territoriali:

- accedono ai finanziamenti partecipando ai Bandi/Avvisi emanati dai Ministeri competenti per la selezione dei progetti, ovvero ai provvedimenti di riparto fondi ove previsto;
- ricevono, di norma, direttamente dal MEF le risorse occorrenti per realizzare i progetti, mediante versamenti nei conti di tesoreria, salvo il caso di risorse già giacenti sui capitoli di bilancio dei Ministeri;
- devono realizzare gli interventi nel rispetto delle norme vigenti e delle regole specifiche stabilite per il PNRR;
- devono rispettare gli obblighi di monitoraggio, rendicontazione e controllo e concorrere al conseguimento di traguardi e obiettivi associati al progetto;
- devono prevenire e correggere eventuali irregolarità e restituire le risorse indebitamente utilizzate.

Tra gli obiettivi della Missione 1 ("Digitalizzazione, innovazione, competitività, cultura e turismo") rientrano in particolare la digitalizzazione della Pubblica Amministrazione e il rafforzamento delle competenze digitali, per il quale il Piano prevede il rafforzamento delle infrastrutture digitali della pubblica amministrazione, la facilitazione alla migrazione al cloud, un ampliamento dell'offerta di servizi ai cittadini in modalità digitale, la riforma dei processi di acquisto di servizi ICT, con l'obiettivo di portare le pubbliche amministrazioni locali alla migrazione verso ambienti Cloud certificati; gli interventi finanziabili consistono nell'implementazione di un Piano di migrazione al Cloud delle basi dati e delle applicazioni e servizi dell'amministrazione;

Visto il decreto della Presidenza dei Consiglio dei Ministri n. 85/2022-PNRR del 22/07/2022 di approvazione dell'Avviso pubblico per la presentazione di proposte di intervento a valere sul PNRR - MISSIONE 1 - COMPONENTE 1 - Investimento 1.2 "Abilitazione al Cloud per le PA locali" comuni (Luglio 2022);

Dato atto che l'importo del finanziamento concedibile ai Soggetti Attuatori è individuato, ai sensi dell'art. 53 par. 1. Lett. c) del Reg. UE 1060/2021, in un importo forfettario (lump sum) determinato in funzione:

- delle modalità di Migrazione al Cloud;
- della classe di popolazione residente di riferimento del medesimo Soggetto Attuatore.

Dato atto che la classe di popolazione residente di appartenenza del singolo Soggetto Attuatore è determinata sulla base di quanto al dato ISTAT 2021.

Dato atto che il finanziamento, nella misura dell'importo forfettario, sarà erogato in un'unica soluzione a seguito del perfezionamento delle attività di migrazione al cloud oggetto del finanziamento per come disposto all'art. 13 dell'Avviso.

Dato atto che in data 26/07/2022 il Comune di Castel Ivano ha inoltrato, mediante la piattaforma "PA digitale 2026" la candidatura n° 40217 all'Avviso pubblico "Misura 1.2. "Abilitazione al cloud per le PA Locali " Comuni Luglio 2022– M1C1 PNRR finanziato dall'Unione Europea -NextGenerationEU, richiesta per n. 13 servizi da migrare, uno in modalità "A – Trasferimento in sicurezza dell'infrastruttura IT" e 12 in modalità "B – aggiornamento in sicurezza di applicazioni Cloud", per un importo complessivo richiesto di Euro 75.180,00.

In tale ambito il Comune di Castel Ivano ha presentato la propria candidatura a valere sull'Avviso pubblico "Investimento 1.2 ABILITAZIONE AL CLOUD PER LE PA LOCALI COMUNI (LUGLIO 2022)' - M1C1 PNRR FINANZIATO DALL'UNIONE EUROPEA - NextGenerationEU";

Nella domanda di partecipazione sono stati elencati 13 servizi, di cui 5 relativi al Servizio

Finanziario, che utilizza l'applicativo Linea J-ENTE fornito dalla ditta Municipia spa, come di seguito elencati:

	SERVIZI oggetto di migrazione	Modalità di migrazione	Applicativo
1	CONTABILITA' E RAGIONERIA	B - Aggiornamento in sicurezza di applicazioni in Cloud	J-ENTE
2	ECONOMATO	B - Aggiornamento in sicurezza di applicazioni in Cloud	J-ENTE
3	GESTIONE ECONOMICA	B - Aggiornamento in sicurezza di applicazioni in Cloud	J-ENTE
4	REVISIONE CONTABILE	B - Aggiornamento in sicurezza di applicazioni in Cloud	J-ENTE
5	GESTIONE DEL PATRIMONIO	B - Aggiornamento in sicurezza di applicazioni in Cloud	J-ENTE

Con decreto nr. 85 - 1/2022 il Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri ha approvato il finanziamento degli interventi, nei quali rientra anche il Comune di Castel Ivano per l'importo di € 75.180,00;

Rilevato che in data 5 ottobre 2022, al prot. 13065 veniva notificata da parte del Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei Ministri, l'ammissione della candidatura n. 40217 relativa all'Avviso sopra specificato e, a seguito di tale comunicazione, veniva caricato a sistema il CUP G51C22000750006 assegnato al progetto medesimo.

Dato atto che in riferimento al Decreto della Presidenza del Consiglio dei Ministri n. 85 - 1/2022 - PNRR, come comunicato al prot. n. 16440 dd. 14.12.2022, veniva approvato l'elenco delle istanze a valere su "Avviso Investimento 1.2 Abilitazione al Cloud per le PA Locali - Comuni (Luglio 2022)" ed assegnato al Comune di Castel Ivano il finanziamento di Euro 75.180,00, per l'affido dell'incarico riferito all'attuazione della Misura medesima.

Al fine della liquidazione del finanziamento assegnato è necessario avviare il progetto (contrattualizzare il rapporto con il fornitore) entro il termine fissato dal decreto di assegnazione, inizialmente fissato l'11.09.2023, e concludere la realizzazione delle attività entro il 04.12.2024;

E' stato richiesto in data 16.08.2023 sul portale PAdigitale2026 di posticipare la data di scadenza di 30 gg, e successivamente di ulteriori trenta giorni; la contrattualizzazione con i fornitori deve avvenire entro il 09.11.2023;

Allo stato attuale il Comune opera attraverso l'utilizzo del software Linea J-ENTE fornita da Municipia S.p.A., con un costo annuale di assistenza sistematica di € 3.552,00 Iva esclusa, per un importo totale di € 4.333,44;

Il finanziamento ottenuto consente la migrazione "in cloud" dell'intera piattaforma tecnologica di Linea J-ENTE adottata dal Comune per la gestione dei programmi in uso presso il servizio finanziario, consentendo di aumentare ulteriormente la tutela che la salvaguardia dei dati nel loro insieme, gli aggiornamenti, i backup incrementali e tutte le attività di disaster recovery. Di fatto si tratta di un'importazione massiva su una nuova soluzione tecnologica che dispone di nuove funzionalità e integrazioni. Per questo sono previste giornate formative e di assistenza per tutto il personale amministrativo-gestionale nel rispetto di un cronoprogramma che sarà definito e concordato con la struttura comunale;

Municipia spa, in linea con quanto previsto per le Pubbliche Amministrazioni sia nel Piano Triennale dell'Informatica che nel Piano Nazionale di Ripresa e Resilienza, si impegna ad

adottare è una soluzione orientata al cloud delle Pubbliche Amministrazioni in modalità Software as a Service, in quanto la soluzione è qualificata da AGID e pubblicata nel Cloud Marketplace. La modalità di erogazione del servizio SaaS delle suite include, oltre all'erogazione delle funzionalità software, anche la fornitura di tutti i servizi necessari alla piena fruizione da parte del cliente. Il modello proposto evidenzia come la transizione al SaaS deleghi la gestione e la responsabilità dal cliente (il Comune titolare del dato) al fornitore di servizi cloud con un evidente beneficio in termini di efficienza e efficacia dell'organizzazione. L'ente è quindi sollevato da tutti i problemi di sicurezza, ridondanza dell'architettura, controllo degli accessi fisici e remoti, amministrazione, manutenzione, backup e recovery dei sistemi fisici. Può inoltre scalare risorse hardware e software in funzione delle proprie specifiche esigenze;

Il passaggio alla nuova soluzione tecnologica è quindi legato a un pacchetto di servizi comprensivo delle seguenti attività:
- attività tecniche per l'attivazione dell'ambiente applicativo per il funzionamento in cloud che deve essere utilizzato tramite web browser;
- attività di project management, assessment e documentazione ai fini del raggiungimento degli obiettivi del PNRR;
- attività di formazione sulle nuove interfacce, con l'obiettivo di garantire la massima fruibilità ed efficacia agli utenti anche in relazione alle modifiche apportate sia a livello di interfaccia che di logiche applicative rispetto alla precedente soluzione.

La migrazione in oggetto è relativa ad applicativi in dotazione al Comune di Castel Ivano forniti dalla ditta Municipia S.p.A. con propri applicativi esclusivi, per tale ragione risulta funzionale, sia sotto il profilo organizzativo del lavoro sia al fine del raggiungimento degli obiettivi per l'ottenimento del finanziamento PNRR, l'assegnazione alla medesima ditta del servizio di attivazione della nuova piattaforma tecnologica in modalità cloud;

Allo scopo è stata formulata apposita offerta da Municipia spa, pervenuta al protocollo comunale in data 30.10.2023 al nr. 13721 per l'installazione in cloud del modulo Gestione del patrimonio e al nr. 13722 per la migrazione in cloud degli altri 4 servizi da migrare in cloud, già presenti nell'applicativo attualmente in uso, come meglio dettagliato nella documentazione allegata;

Con l'offerta citata Municipia spa si impegna ad effettuare la migrazione in cloud alla nuova in modalità SaaS di 5 servizi afferenti ai programmi in uso al Servizio finanziario, di cui uno di nuova installazione (modulo gestione del patrimonio)

Vista al riguardo la normativa provinciale vigente in materia, con particolare riferimento alla L.P. 19.07.1990 nr. 23 "Disciplina dell'attività contrattuale e dell'amministrazione dei beni della Provincia di Trento" e alla L.P. 09.03.2016 nr. 2;

Richiamata altresì la L.P 8 agosto 2023, n. 9 "Assestamento del bilancio di previsione della Provincia autonoma di Trento per gli esercizi finanziari 2023-2025 pubblicata sul Numero Straordinario nr. 2 al B.U. n. 31 del 8 agosto 2023 e entrata in vigore il 27 maggio 2023, che prevede fra l'altro, in adeguamento alla disciplina del nuovo Codice dei contratti pubblici (D.Lgs. nr. 36/2023);

Atteso che tale norma prevede la possibilità di procedere all'affidamento diretto di lavori di importo inferiore a 150.000 euro e all'affidamento diretto di servizi e forniture, ivi compresi i servizi di ingegneria e architettura e l'attività di progettazione, di importo inferiore a 140.000 euro;

Dato atto che in riferimento alla conclusione di contratti di acquisto di beni e servizi l'art 21 comma 4 della Lp 23/1990 testualmente recita "Ove ricorrano le ipotesi di cui alle lettere b), b bis), b ter) ed e) del comma 2 nonché fino alla soglia prevista dalla normativa statale, il contratto può essere concluso mediante trattativa diretta con il soggetto o la ditta ritenuti idonei";

Ritenuto pertanto di procedere all'affidamento del contratto in parola direttamente con la ditta Municipia spa, trattandosi di un importo pari ad € 4.350,00 più IVA al 22%, comprensivi di attivazione una tantum del modulo "gestione del patrimonio", formazione on site, recupero dati da vecchia procedura, canone di manutenzione fino al 31.12.2023, oltre ad € 14.200,00 oltre ad IVA al 22%, per la migrazione in cloud dei restanti servizi dichiarati in premessa, servizi pertanto inferiore alla soglia prevista dalla normativa statale trattandosi di importo complessivo di € 18.550,00 più IVA;

Atteso che, in materia di acquisizione di beni, di servizi e di prestazioni la normativa di riferimento è quella disposta dalla L.P. n° 23/1990 e s.m. ed il suo regolamento di attuazione, dal D.Lgs n. 36/2023 e ss.mm. e dal relativo regolamento di attuazione, nonché dalla normativa contenuta nell'art. 1 del D.L. 06/07/2012 n. 95 (c.d. "spending review"), convertito con modifiche in Legge 07.08.2012 n° 135 e s.m.;

Visto che, ai sensi del comma 502 della Legge 208 di data 28.12.2015 (legge di stabilità 2016) per quanto riguarda l'acquisizione di beni e servizi, l'obbligo di ricorrere al mercato elettronico viene meno per importi inferiori ai 5.000 euro (modifica all'articolo 1, comma 450, della legge 27 dicembre 2006, n. 296, così come ulteriormente modificato dal comma 130 dell'art. 1 della Legge di Stabilità 30.12.2018, n. 145);

Visto e richiamato il comma 6 dell'art. 36 ter 1 della L.P. n 23/1990 e ss.mm.ii., in base al quale rimane ferma la possibilità per la Provincia, per gli enti locali e per le altre amministrazioni aggiudicatrici del sistema pubblico provinciale, di effettuare spese per acquisti di beni e servizi di importo inferiore a 5.000,00 Euro senza ricorrere al mercato elettronico o agli strumenti elettronici di acquisto gestiti dalla Provincia o da CONSIP;

Accertato che è presente sul Mercato Elettronico della Provincia Autonoma di Trento (ME-PAT) all'interno del bando di abilitazione di riferimento "Servizi informatici e di comunicazione" la categoria merceologica "Servizi applicativi_CPV72000000-5", all'interno della quale la ditta Municipia spa S.p.A. ha pubblicato nel catalogo servizi i metaprodotti:
- "MNP_CD_1014_23" (con condizioni e termini specificamente dettagliati nella documentazione esplicativa nr. 13722/prot. di data 30.10.2023 ALLEGATA), al costo di € 14.200,00 soggetto Iva 22% e quindi € 17.324,00 totali;
- "MCP_GG_2023" (con condizioni e termini specificamente dettagliati nella documentazione esplicativa nr. 13721/prot. di data 30.10.2023 ALLEGATA), al costo di € 4.350,00 soggetto Iva 22% e quindi € 5.307,00,00 totali;

Quantificata pertanto la spesa complessiva in € 18.550,00 più Iva e quindi € 22.631,00 totali la spesa a carico dell'ente;

Ritenuto, alla luce di quanto sopra, di disporre che l'assegnazione dell'incarico di migrazione "in cloud" della piattaforma tecnologica di Linea J-ENTE adottata dal Comune per il servizio finanziario avvenga a trattativa privata, ai sensi dell'articolo 21 co. 4 L.P. nr. 23/1990 come modificato dalla L.P. nr. 4/2023, mediante ordine diretto di acquisto (OdA) alla ditta MUNICIPIA S.p.A. con sede a Trento (TN) via Adriano Olivetti 7 P. Iva 01973900838;

Accertato che la presente determinazione vale quale provvedimento a contrarre ai sensi dell'art. 13 della L.P. 23/1990 e ss.mm.ii., in quanto indica il fine che con il contratto si intende perseguire, l'oggetto del contratto, la forma, le clausole essenziali e le modalità di scelta del contraente;

Effettuate le verifiche di regolarità sulla ditta Municipia spa, tutte con esito positivo/favorevole;

Dato atto in particolare che:
- Il fine che si intende perseguire con il contratto è la migrazione "in cloud" di quattro servizi attivi sulla piattaforma tecnologica Linea J_ENTE adottata dal Comune per il servizio finanziario, e l'installazione in cloud di un ulteriore modulo applicativo;

- Il finanziamento del progetto rientra nel Piano Nazionale di Ripresa e Resilienza (PNRR) - Missione 1 Componente 1 Investimento 1.2 “Abilitazione al cloud per le PA Locali Comuni Luglio 2022” per un importo complessivo di euro 75.180,00 IVA inclusa, come risulta dal decreto nr. 85 - 1/2022 del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri, ed è finanziato dall’Unione Europea NextGenerationEU;
- La modalità di scelta del contraente è quella dell’affidamento diretto sul mercato elettronico MePat mediante Ordine diretto di Acquisto (OdA) all’interno del bando di abilitazione di riferimento “Servizi informatici e di comunicazione” nella categoria merceologica “Servizi applicativi _CPV72000000-5”;
- Termine di esecuzione delle attività: 04.12.2024;
- CIG: ZF83D11089
- CUP: G51C22000750006
- La ditta incaricata prende atto che l’intervento oggetto di progettazione è finanziato con fondi del Piano Nazionale di Ripresa e Resilienza (PNRR) finanziato dall’Unione europea – Next Generation EU e in particolare rientra negli investimenti definiti alla Missione 1 Componente 1 Investimento 1.2 “Abilitazione al cloud per le PA Locali Comuni Luglio 2022”, e si impegna al rispetto di tutte le norme e degli obblighi derivanti dalla specifica disciplina dettata per il PNRR nonché degli obblighi specifici per l’attuazione dell’investimento in oggetto, compreso il principio Do No Significant Harm (DNSH), non arrecando alcun danno significativo all’ambiente; con particolare riferimento al principio del DNSH, Municipia S.p.A.
  Il servizio proposto, descritto nelle pagine seguenti, è erogato in SaaS coerentemente con i requisiti della qualificazione AgID, la cui scheda è reperibile all'url:
  https://catalogocloud.agid.gov.it/service/506
  Per poter gestire scenari dinamici ed in costante evoluzione, è importante costruire un approccio al Cloud che consenta di ridurre al minimo la complessità ed i costi di transizione tra diversi service provider. Per questo motivo si è deciso di adottare Kubernetes, che consente di raggiungere un livello di astrazione tale da poter rendere un intero data center auto contenuto e descritto da manifesti di configurazione replicabili e ripetibili. Il dispiegamento avviene attraverso l'orchestrazione di tecnologie moderne ed affidabili, al fine di costruire un'infrastruttura dinamica, robusta e con capacità computazionali adattive rispetto al carico di lavoro.
- La liquidazione alla ditta incaricata dell’importo pattuito tramite bonifico bancario su conto corrente bancario dedicato alle commesse pubbliche ai fini di assicurare la tracciabilità dei movimenti finanziari relativi a rapporti contrattuali in ambito pubblico previa emissione di fattura elettronica con imputazione e riferimento al presente impegno e riportante il relativo codice CIG vistata dal funzionario incaricato che attesti la regolarità della fornitura;
- La ditta incaricata, a pena di nullità assoluta del contratto, assume gli obblighi di tracciabilità dei flussi finanziari previsti dalla legge 13.08.2010 nr. 136 e ss.mm.ii. A tal fine si obbliga a comunicare alla stazione appaltante gli estremi identificativi del conto corrente dedicato, nonché le generalità e il codice fiscale delle persone delegate a operare su di esso entro 7 giorni. La ditta si obbliga a inserire nei contratti sottoscritti con gli eventuali subcontraenti a qualsiasi titolo interessati ai lavori oggetto del presente contratto un’apposita clausola con la quale ciascuno di essi assume gli obblighi di tracciabilità dei flussi finanziari di cui alla legge nr. 136/2010, pena la nullità degli stessi contratti;
- In applicazione dell’art. 2 co. 3 del D.P.R. 62/2013, gli obblighi di condotta ivi previsti e quelli contenuti nel “Codice di comportamento dei dipendenti” approvato con deliberazione della Giunta comunale di Castel Ivano nr. 274 di data 28.12.2022 si estendono anche ai collaboratori a qualsiasi titolo delle imprese fornitrici di beni o servizi o che realizzano opere in favore dell’Amministrazione. La violazione degli obblighi derivanti dal Codice di comportamento costituisce immediata causa di risoluzione o decadenza dal rapporto;
- Il contratto con la ditta incaricata, si intende validamente perfezionato al momento in cui l’ordine di acquisto firmato digitalmente è caricato nel sistema MePat;

Richiamata inoltre la nota prot. 11247 del 05.09.2023 con cui è stata richiesta alla ditta Municipia spa:

- la dichiarazione DNSH con l’indicazione di quale standard viene soddisfatto;

- la dichiarazione di parità di genere

Vista la documentazione in risposta alla nota citata, acquisita al prot. 11563 del 11.09.2023;

Visto il Codice degli Enti Locali della Regione Autonoma Trentino-Alto Adige approvato con Legge regionale 3 maggio 2018 nr. 2;

Visti gli atti di programmazione dell'attività dell'Ente, come risultanti da:
- Deliberazione del Consiglio Comunale nr. 8 del 14.02.2023, immediatamente esecutiva, avente ad oggetto "Approvazione della nota di aggiornamento al documento unico di programmazione, dello schema di bilancio di previsione finanziario 2023-2025, della nota integrativa, del piano degli indicatori e dei risultati attesi di bilancio (bilancio armonizzato di cui al d.lgs. 118/2011 e s.m.)";

- Deliberazione del Consiglio Comunale n. 9 dd. 27.02.2023, immediatamente esecutiva, avente ad oggetto "Approvazione del documento unico di programmazione, dello schema di bilancio di previsione finanziario 2023-2025, della nota integrativa, del piano degli indicatori e dei risultati attesi di bilancio (bilancio armonizzato di cui al d.lgs. 118/2011 e s.m.) rettifica della propria deliberazione n 8 del 14.02.2023";

- Deliberazione della giunta comunale n. 80 dd. 15.03.2023 con la quale sono stati approvati gli atti programmatici di indirizzo – parte finanziaria - per la gestione del bilancio di previsione 2023-2025: assegnazione dotazioni finanziarie ai Responsabili dei Servizi.

Attesa la propria competenza;

D E T E R M I N A

1. di disporre, per le motivazioni esposte in premessa, che l'assegnazione del servizio di migrazione al cloud degli applicativi in dotazione agli uffici comunali Linea J-ENTE, avvenga a trattativa privata ai sensi dell'articolo 21 co. 4 L.P. nr. 23/1990 come modificato dalla L.P. nr. 4/2023, mediante ordine diretto di acquisto (OdA) alla ditta Municipia S.p.A. per i seguenti metaprdotti pubblicati nel catalogo servizi del mercato elettronico MEPAT:
- "MNP_CD_1014_23" (con condizioni e termini specificamente dettagliati nella documentazione esplicativa nr. 13722/prot. di data 30.10.2023 ALLEGATA), al costo di € 14.200,00 soggetto Iva 22% e quindi € 17.324,00 totali;
- "MCP_GG_2023" (con condizioni e termini specificamente dettagliati nella documentazione esplicativa nr. 13721/prot. di data 30.10.2023 ALLEGATA), al costo di € 4.350,00 soggetto Iva 22% e quindi € 5.307,00,00 totali;

2. di dare atto che l'investimento in oggetto, individuato con CIG ZF83D11089/ CUP G51C22000750006, rientra nel PNRR Missione 1 Componente 1 Investimento 1.2 "ABILITAZIONE AL CLOUD PER LE PA LOCALI COMUNI (LUGLIO 2022)" finanziato dall'Unione Europea-NextgenerationEU;

3. di dare atto che l'incarico di cui al punto 1 è conferito con le seguenti clausole essenziali:
- Termine di esecuzione delle attività: 04.12.2024;
- La ditta incaricata prende atto che l'intervento oggetto di progettazione è finanziato con fondi del Piano Nazionale di Ripresa e Resilienza (PNRR) finanziato dall'Unione europea – Next Generation EU e in particolare rientra negli investimenti definiti alla Missione 1 Componente 1 Investimento 1.2 "Abilitazione al cloud per le PA Locali Comuni Luglio 2022", e si impegna al rispetto di tutte le norme e degli obblighi derivanti dalla specifica disciplina dettata per il PNRR nonché degli obblighi specifici per l'attuazione dell'investimento in oggetto;
- La ditta incaricata si impegna in particolare al rispetto del principio Do No Significant Harm (DNSH), non arrecando alcun danno significativo all'ambiente, con riferimento al quale

garantisce l'erogazione del servizio attraverso data center che, oltre a essere qualificati nel marketplace Agid, sono anche "DNSH compliant" in quanto iscritti al Codice di Condotta Europeo sull'efficientamento energetico dei Data Center (Data Centres Code of Conduct;
Il servizio proposto, descritto nelle pagine seguenti, è erogato in SaaS coerentemente con i requisiti della qualificazione AgID, la cui scheda è reperibile all'url:
https://catalogocloud.agid.gov.it/service/506
Per poter gestire scenari dinamici ed in costante evoluzione, è importante costruire un approccio al Cloud che consenta di ridurre al minimo la complessità ed i costi di transizione tra diversi service provider. Per questo motivo si è deciso di adottare Kubernetes, che consente di raggiungere un livello di astrazione tale da poter rendere un intero data center auto contenuto e descritto da manifesti di configurazione replicabili e ripetibili. Il dispiegamento avviene attraverso l'orchestrazione di tecnologie moderne ed affidabili, al fine di costruire un'infrastruttura dinamica, robusta e con capacità computazionali adattive rispetto al carico di lavoro.

- La liquidazione alla ditta incaricata dell'importo pattuito tramite bonifico bancario su conto corrente bancario dedicato alle commesse pubbliche ai fini di assicurare la tracciabilità dei movimenti finanziari relativi a rapporti contrattuali in ambito pubblico previa emissione di fattura elettronica con imputazione e riferimento al presente impegno e riportante il relativo codice CIG vistata dal funzionario incaricato che attesti la regolarità della fornitura;
- La ditta incaricata, a pena di nullità assoluta del contratto, assume gli obblighi di tracciabilità dei flussi finanziari previsti dalla legge 13.08.2010 nr. 136 e ss.mm.ii. A tal fine si obbliga a comunicare alla stazione appaltante gli estremi identificativi del conto corrente dedicato, nonché le generalità e il codice fiscale delle persone delegate a operare su di esso entro 7 giorni. La ditta si obbliga a inserire nei contratti sottoscritti con gli eventuali subcontraenti a qualsiasi titolo interessati ai lavori oggetto del presente contratto un'apposita clausola con la quale ciascuno di essi assume gli obblighi di tracciabilità dei flussi finanziari di cui alla legge nr. 136/2010, pena la nullità degli stessi contratti;
- In applicazione dell'art. 2 co. 3 del D.P.R. 62/2013, gli obblighi di condotta ivi previsti e quelli contenuti nel "Codice di comportamento dei dipendenti" approvato con deliberazione della Giunta comunale di Castel Ivano nr. 274 di data 28.12.2022 si estendono anche ai collaboratori a qualsiasi titolo delle imprese fornitrici di beni o servizi o che realizzano opere in favore dell'Amministrazione. La violazione degli obblighi derivanti dal Codice di comportamento costituisce immediata causa di risoluzione o decadenza dal rapporto;
- Il contratto con la ditta incaricata si intende validamente perfezionato nel momento in cui l'ordine di acquisto firmato digitalmente è caricato nel sistema MePat;

4. di dare atto che l'importo di € 75.180,00 quale quota parte del contributo assegnato con decreto nr. 85 - 1/2022 del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri a totale finanziamento dell'Investimento 1.2 M1C1 del PNRR, è stato accertato al capitolo 1800/400 piano finanziario 2.01.01.01.001 del bilancio di previsione 2023-2025, esercizio 2023;

5. di impegnare l'onere derivante dal presente provvedimento:
   - nella somma di € 18.550,00 più Iva 22% per totali € 22.631,00, alla missione 1 programma 8 titolo 1 macroaggregato 3, capitolo 108400 piano finanziario 1.03.02.19.999 del bilancio di previsione 2023-2025, esercizio 2023;

6. di dare atto che l'obbligazione giuridica derivante dal presente provvedimento è esigibile entro il 31.12.2023;

7. di dare atto che l'eccedenza del contributo di cui al punto n. 2 del presente dispositivo confluirà nei vincoli dell'avanzo di amministrazione e che lo stesso potrà essere applicato con le modalità previste dal testo unico e dai vigenti principi contabili previa approvazione del rendiconto di gestione;

8. di autorizzare fin da ora il servizio finanziario alla re-imputazione parziale e/o totale (sia per la

parte entrata che per la parte spesa) in base al momento di rendicontazione della spesa in modalità “lump sum”.

9. di dare atto che la società affidataria del servizio in oggetto viene ad assumere la figura di responsabile esterno del trattamento dati ed è tenuta ad assolvere tutti gli adempimenti previsti dall’art. 28 del Regolamento UE n. 2016/679 (GDPR).

10. di dare attuazione agli adempimenti di pubblicità prescritti dall’art. 29 del D.lgs. 50/2016 e agli adempimenti inerenti la pubblicazione sul portale “Amministrazione Trasparente” nel rispetto dell’articolo 37 del D.lgs. n. 33/2013 e dell’art. 1, comma 32 della legge n. 190/2012, nonchè dalla circolare del M.E.F. di data 10 febbraio 2022, n. 9.

11. di dare atto che, ai fini e per gli effetti di cui alla l. 136/2010 si subordina, a pena di nullità assoluta, il perfezionamento del contratto all’assunzione da parte dei fornitori contraenti degli obblighi in materia di tracciabilità dei flussi finanziari; il mancato adempimento costituisce causa di risoluzione del contratto ai sensi dell'art. 1456 del C.C.; il codice CIG assegnato è ZF83D11089;

12. di dare evidenza, ai sensi dell'art. 4 della L.P. 30.11.1992 nr. 23, che avverso il presente provvedimento, ai sensi dell’art. 4 della L.P. 30 novembre 1992, n. 23 e ss.mm. ed ii., sono ammessi:
    a) ricorso giurisdizionale al T.R.G.A. di Trento entro 60 giorni ai sensi dell'art. 29 del D.Lgs. 2 luglio 2010 n. 104;
    b) ricorso straordinario al Presidente della Repubblica entro 120 giorni, ai sensi dell'art. 8 del D.P.R. 24.11.1971, n. 1199.

Per gli atti relativi alle **procedure di affidamento di pubblici lavori, servizi e forniture**, ai sensi del combinato disposto degli art. 119, comma 1, lett. a) e 120 del D.Lgs. 2 luglio 2010 n. 104, è ammesso il ricorso sub. a) nel termine di 30 giorni e non è ammesso il ricorso straordinario sub. b).

MUNICIPIA
AUGMENTED CITY

PROPOSTA TECNICO ECONOMICA

DESTINATARIO:
Amministrazione Comunale di CASTEL IVANO
Alla c.a. Dr.ssa Lucia Feller
e-mail | pec lucia.feller@comune.castel-ivano.tn.it

DATA EMISSIONE 18/10/2023 –**RIFERIMENTO JOP- 239722**

OGGETTO
Soluzione jEnte On Premises:
Attivazione modulo Patrimonio Jente

RIFERIMENTO MUNICIPIA PER ASPETTI ECONOMICI
Valerio Falciani
e-mail: valerio.falciani@eng.it
mobile: 347 3668618

RIFERIMENTO MUNICIPIA PER ASPETTI TECNICI
Fabrizio Balboni
e-mail: fabrizio.balboni@eng.it
mobile: 346 7430493

MUNICIPIA
GRUPPO ENGINEERING

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

Società soggetta all'attività di direzione e coordinamento di Engineering Ingegneria Informatica Spa

Municipia S.p.A.
Il Procuratore

Firmato digitalmente da: MANUELA VESENTINI
Data: 18/10/2023 22:49:34

CAPITOLO 1

PROPOSTA ECONOMICA

DESCRIZIONE SOLUZIONE	IMPORTO	Barrare la casella
jEnte On Premises - Modulo Patrimonio ▪ Attivazione Una Tantum ▪ Formazione on site ▪ Recupero dati da vecchia procedura ▪ Canone Annuo di manutenzione e assistenza fino al 31/12/2023	€ 4.350,00	☐
TOTALE	**€ 4.350,00**	

N.B: Dal 01.01.2024 al 31.12.2024 il canone annuo di manutenzione sarà pari a: **€ 210,00**
Gli importi sopra indicati sono espressi in euro esono 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 CASTEL IVANO (TN)**

P.I. 02401920224 - **e-mail** | **Pec** info@pec.comune.castel-ivano.tn.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 DI IVA	CIG	CODICE UNIVOCO
N° _____ **DEL** _____			

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: jEnte On Premises

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** sono descritte qui di seguito.

Servizi Finanziari

Qualificato AGID SaaS

CESPITI PATRIMONIALI

Il sistema prevede la tenuta ed aggiornamento dell'Inventario dei beni immobili e mobili secondo le diverse tipologie previste. All'interno di ciascun tipo, i beni sono classificabili per specie e per categoria.
Pienamente integrato con il sistema contabile coopera con esso per la proposta automatica delle registrazioni da effettuare (esempio tutti i movimenti che hanno riguardato il titolo II della spesa) ma soprattutto per tutte le fasi di chiusura, finalizzate alla produzione dei rendiconti:

- conto economico (ammortamenti, plusvalenze, minusvalenze)
- conto del patrimonio (immobilizzazioni, immobilizzazioni in corso)

La puntuale gestione del cespite, all'interno del sistema contabile (esempio in sede di impegno o di fattura), consente un ottimo supporto in tutte le fasi di registrazione e di quadratura delle risultanze con il bilancio.
Per ciascun cespite vengono registrati i dati salienti quali: descrizione, titolo di possesso, data e valore all'acquisto, fornitore, stato di conservazione, ubicazione, centro di costo competente, consegnatario ecc.
Annotazioni sul bene sono registrabili data per data in modo da conservare traccia facilmente consultabile di tutti gli eventi significativi (manutenzioni straordinarie, prestiti temporanei ecc..).
Sui beni che lo prevedono sono inoltre gestibili le concessioni e le rendite.
Un apposito campo è destinato all'aggiornamento periodico, manuale o automatico (abbattimento annuo secondo percentuali variabili per tipo, specie o categoria) del valore attuale del bene (valore di stima).
Il calcolo dell'ammortamento è effettuato secondo i normali criteri civilistici in base a percentuali definite per specie, per categoria o specificatamente per il singolo cespite.
Risultati del calcolo dell'ammortamento sono:

- la stampa del registro;
- la produzione delle scritture contabili per la valorizzazione del fondo e dei costi (dettagliati per centro di costo e/o Missione/Programma).

È possibile collegare ad un cespite parti aggiuntive, tramite l'utilizzazione di un codice Sub sul n. di inventario.
In caso di vendita del bene è consentita la memorizzazione degli estremi di fatturazione e calcolata la plusvalenza o minusvalenza.
Nell'ambito della scheda cespite è attiva la "cartella documentale" attraverso la quale è possibile la memorizzazione di foto, piantine, atti di compravendita in formato elettronico.
Specifiche elaborazioni permettono di ottenere stampe dell'inventario a livello generale, per tipo/specie/categoria, per centro di costo, per consegnatario, ecc...
Per i beni mobili è prevista la movimentazione di carico/scarico del consegnatario (con produzione del verbale di consegna o dismissione) che rende possibile la stampa del "conto dei consegnatari" ed eventualmente l'aggiornamento conseguente della scheda inventario per stanza.

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 (da quotare ad hoc se non ricompresi nell'offerta)

Comprendono tutte le attività dello staff tecnico di Municipia, erogate per via telematica, per la configurazione, l'eventuale popolamento delle banche dati di riferimento e l'affiancamento degli 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 possono essere 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, ove prevista, 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

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 On Premises.

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.

Non sono inoltre comprese tutte le attività legate all'interazione e all'integrazione di servizi esterni come l'approvvigionamento, l'installazione e la configurazione di certificati di sicurezza impiegati con servizi di terze parti, o per cifrare i dati in transito nelle configurazioni On Premises. I dispiegamenti SaaS dei certificati di sicurezza per la cifratura dei dati in transito sono a cura di Municipia. Le stesse premesse si estendono anche a eventuali servizi di terze parti (es.: caselle PEC). Municipia è a disposizione per fornire supporto nell'individuazione delle migliori soluzioni e per eventuali implementazioni in regime di supporto specialistico.

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

Gli aggiornamenti periodici sono resi disponibili da Municipia attraverso pacchetti di rilascio. Ove non contrattualmente definito, la loro installazione è a carico dell'Amministrazione

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:

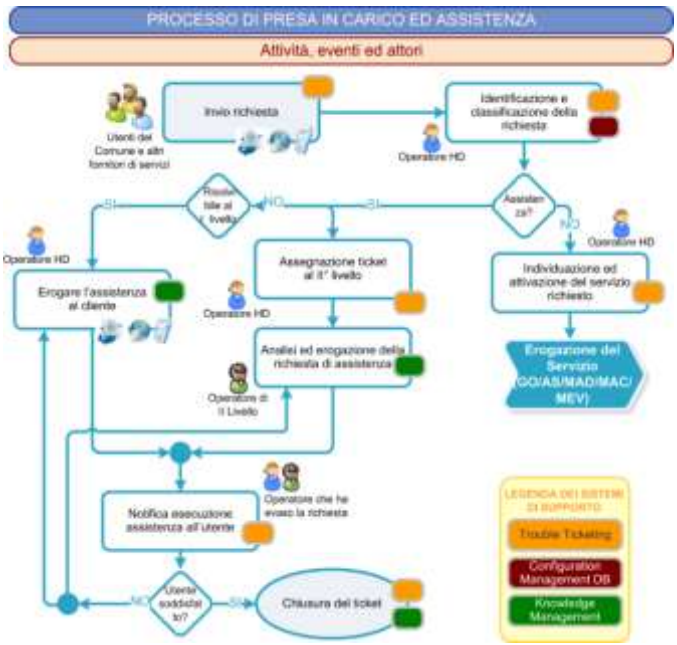
- consultare tutte le proprie segnalazioni con i dettagli della conversazione;
- caricare, visualizzare e gestire eventuali allegati inviati o ricevuti;
- usufruire di un'area per rispondere in modo semplice senza creare duplicati nelle richieste di assistenza;
- monitorare lo stato di avanzamento della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

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)
- **Minore**
  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
MFSRT *(Maximum First-Support Response Time)*	Tempo di presa in carico	Bloccante	Tutti	4 ore lavorative
		Maggiore	Tutti	8 ore lavorative
		Minore	Tutti	16 ore lavorative
TTR *(Time To Resolution)*	Tempo di risoluzione	Bloccante	Assistenza	8 ore lavorative
		Maggiore	Assistenza	16 ore lavorative
		Minore	Assistenza	40 ore lavorative
		Bloccante	Correttiva	16 ore lavorative
		Maggiore	Correttiva	24 ore lavorative
		Minore	Correttiva	80 ore lavorative

Le tempistiche di risoluzione non possono tenere conto di eventi fuori dal controllo Municipia (es. verifiche congruità App effettuate dagli store previa pubblicazione – indisponibilità sistemi terze parti con cui le soluzioni Municipia sono integrate).

PENALI
La determinazione delle penali si riferisce allo scostamento del valore determinato per gli SLA (MFSRT e TTR) in termini di percentuale in un periodo di osservazione ed il valore target.
Il periodo di 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
MFSRT *(Maximum First-Support Response Time)*	Tempo di presa in carico	Bloccante	Tutti	4 ore lavorative	90%	2 ‰ CAM del periodo
		Maggiore	Tutti	8 ore lavorative		
		Minore	Tutti	16 ore lavorative		

TTR *(Time To Resolution)*	Tempo di risoluzione	Bloccante	Assistenza	8 ore lavorative	90%	2 ‰ CAM del periodo
		Maggiore	Assistenza	16 ore lavorative		
		Minore	Assistenza	40 ore lavorative		
		Bloccante	Correttiva	16 ore lavorative	90%	2 ‰ CAM del periodo
		Maggiore	Correttiva	24 ore lavorative		
		Minore	Correttiva	80 ore lavorative		

SUPPORTO SPECIALISTICO (DA REMOTO E/O ON SITE)

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 n. giornate	**SUGRCS01** 1 giornata	**SUGRCS03** 3 giornate	**SUGRCS05** 5 giornate	**SUGRCS10** 10 giornate	**SUGRCS20** 20 giornate
Importo a 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 n. giornate	**SUGSCS01** 1 giornata	**SUGSCS03** 3 giornate	**SUGSCS05** 5 giornate	**SUGSCS10** 10 giornate	**SUGSCS20** 20 giornate
Importo a 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

L'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 richiesta, gli archivi di propria competenza in formato CSV corredato del relativo tracciato dati. È possibile, su richiesta, avere anche l'esportazione della banca dati direttamente nel formato nativo dell'applicazione. 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 di Municipia preposte all'erogazione della Fornitura.
- 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 i documenti di "attivazione lavori" debitamente compilati e sottoscritti (laddove previsti)
- rispetti le tempistiche indicate nelle schede tecniche per la fornitura dei flussi informativi oggetto della fornitura (laddove previsti)

DURATA OFFERTA

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

ADESIONE - DURATA – RECESSO

L'**adesione** al contratto deve avvenire attraverso la sottoscrizione del Modulo d'Ordine e l'invio della determina
Il contratto di manutenzione e assistenza 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 a disabilitare le credenziali di accesso al servizio.
Il recesso potrà essere esercitato dal Cliente per iscritto a mezzo PEC 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.
Per quanto riguarda l'attivazione dell'ambiente della soluzione oggetto della fornitura (go live e canone di manutenzione e assistenza del primo anno) gli importi dovuti dal Cliente saranno **fatturati** a conclusione delle attività contrattualizzate
Per i canoni annuali di **manutenzione e assistenza** successivi al primo anno sarà predisposto apposito contratto.
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.

È 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 CASTEL IVANO, PIAZZA MUNICIPIO, 12, 38059 CASTEL IVANO, (TN)
  pec: info@pec.comune.castel-ivano.tn.it

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.

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 (On Premises) 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
- 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.
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.

Risk Level	Categoria	ID	Descrizione
A	**Ruoli e responsabilità**	**B.4**	Il responsabile della sicurezza 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.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.
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**	È 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**	È 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.

Risk Level	Categoria	ID	Descrizione
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**	È necessario registrare 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. È 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 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 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 accessibile da personale non autorizzato.

Appendice 2	Elenco Sub-Responsabili MD14_PGT01_0_Allegato_Elenco_SubResponsabili
Prodotto/i	jEnte (On Premises) Assistenza e 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

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

☐ È 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 violazione e/o impedirne il perpetrarsi o il ripersi della stessa)

_____

_____

PROPOSTA TECNICO ECONOMICA

DESTINATARIO:
Amministrazione Comunale di **CASTEL IVANO**
Alla c.a. Dott.ssa Lucia Feller
e-mail | pec lucia.feller@comune.castel-ivano.tn.it

DATA EMISSIONE 23/09/2022 - **RIFERIMENTO PNRR MGJNT - 251163**

OGGETTO
PNRR – MIGRAZIONE AL CLOUD –
Missione 1 - 1.2 Abilitazione e facilitazione migrazione al cloud
Suite jEnte - Servizio di Migrazione a SaaS (Cloud certificato Agid)

RIFERIMENTO MUNICIPIA PER ASPETTI ECONOMICI
Valerio Falciani
e-mail: valerio.falciani@eng.it
mobile: 347 3668618

RIFERIMENTO MUNICIPIA PER ASPETTI TECNICI
Fabrizio Balboni
e-mail: fabrizio.balboni@eng.it
mobile: 346 7430493

MUNICIPIA
GRUPPO ENGINEERING

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

Municipia S.p.A.
Il Procuratore
Firmato digitalmente da: Raffaele Mazza
Organizzazione: MUNICIPIA S.P.A./01973900838
Data: 03/10/2022 07:30:45

PREMESSA

PNRR – MIGRAZIONE AL CLOUD – Missione 1 - 1.2 Abilitazione e facilitazione migrazione al cloud

La "**Transizione Digitale**" ha l'obiettivo sostanziale di realizzare un'Amministrazione Pubblica **digitale** e aperta, **che** possa offrire a cittadini e imprese servizi **digitali** semplici, sicuri e di qualità, tali da garantire una relazione trasparente, aperta e soprattutto sicura.

Il primo passo sostanziale da compiere è **la migrazione al Cloud**. Lo scopo della ***Missione 1 – 1.2 Abilitazione e migrazione al cloud*** nell'ambito del PNRR è proprio quello di consentire alle Pubbliche Amministrazioni Locali di trasferire dataset e applicazioni verso un'infrastruttura cloud nativa e sicura.

Migrare al cloud si traduce:

- accelerare l'innovazione utilizzando la tecnologia di sviluppo e automazione cloud-native
- migliorare l'agilità
- semplificare le operazioni di cittadini e imprese in un ambiente sicuro
- ridurre i costi

In tale contesto e facendo seguito ai colloqui intercorsi con codesta Amministrazione, in questo documento descriviamo sia la componente economica sia quella tecnica per prestare il nostro supporto nel processo di migrazione delle diverse aree applicative gestite attraverso la Suite jEnte.

Il documento è strutturato nei seguenti capitoli:

- **nel capitolo 1 (Proposta Economica)** – è indicato l'impegno di spesa riferito al progetto di migrazione proposto
- **nel capitolo 2 (Proposta Tecnica)** – è contenuta la descrizione tecnica del progetto ed in particolar modo le caratteristiche di erogazione del servizio SaaS e della migrazione.
- **nel capitolo 3 (Condizioni Specifiche di Fornitura) –** sono descritte le indicazioni riferite a Obblighi del Cliente e del Fornitore nonché la durata contrattuale, le modalità di fatturazione e dei pagamenti, ecc.
- **nel capitolo 4 (Condizione Generali di Vendita)** – è indicato il rimando alle condizioni MEPA

CAPITOLO 1

PNRR – MIGRAZIONE A CLOUD - PROPOSTA ECONOMICA

Come descritto in premessa, la trasformazione digitale della PA deve seguire un approccio "Cloud first", con l'obiettivo di una adozione del Cloud (migrazione dati e servizi) del 75% entro fine 2025. Il passaggio a tecnologie Cloud rappresenta un forte opportunità per elevare gli standard della PA e centrare gli obiettivi indicati nel PNRR". Questo aspetto, in una fase in cui la realizzazione di un ecosistema evoluto di "cittadinanza digitale" rappresenta una delle sfide principali, è tutt'altro che secondario.

In questo capitolo è indicata la quotazione del progetto di migrazione a Cloud riferito alle aree applicative della **suite jEnte** indicate nella seguente tabella.

La descrizione tecnica di dettaglio del progetto è rimandata al successivo Capitolo 2 (Proposta Tecnica).

PNRR – DESCRIZIONE DELLA SOLUZIONE	IMPORTO	Barrare la casella
Aree Suite Jente oggetto di Migrazione a Cloud • Nucleo Informativo Centrale • Servizi Finanziari • Entrate Attese *L'importo indicato è comprensivo dei seguenti servizi aggiuntivi:* Servizio per Migrazione DB Servizio per Occupazione Spazio	€ 14.200,00	☐

> A partire dal mese di gennaio successivo all'anno di migrazione, sulle componenti sopra descritte sarà applicato il canone annuo di erogazione SaaS, comprensivo della attività di manutenzione e assistenza. A tal proposito sarà trasmesso da Municipia al Cliente un apposito contratto.
> Ovviamente tale contratto non contemplerà eventuali nuovi servizi aggiuntivi che l'Amministrazione volesse attivare.
> Il costo annuale da prevedere sarà aumentato nell'ordine del 30% rispetto ai canoni attualmente in essere.

Gli importi sopra indicati sono espressi in euro e 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 CASTEL IVANO (TN)**
P.I. 02401920224- **e-mail** | **Pec** info@pec.comune.castel-ivano.tn.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 DI IVA	CIG	CUP (CODICE UNICO DI PROGETTO)	CODICE UNIVOCO
N° _____ **DEL** _____				

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

PNRR - MIGRAZIONE A CLOUD - PROPOSTA TECNICA

Come indicato nell'introduzione al Capitolo 1 (Proposta Economica), all'interno degli investimenti del PNRR, la migrazione verso il cloud della Pubblica Amministrazione rappresenta un corposo capitolo nel processo di modernizzazione del settore pubblico. La Pubblica Amministrazione, infatti, deve essere in grado di fornire servizi sempre più digitalmente efficienti in termini di contenuti, strumenti di fruizione, garanzie di sicurezza.

In tale contesto Municipia descrive di seguito il progetto tecnico per la migrazione della Suite jEnte e in particolar modo le caratteristiche di erogazione del servizio SaaS e della migrazione riferito a quanto quotato nel Capitolo 1 (Proposta Economica).

CARATTERISTICHE EROGAZIONE JENTE CLOUD

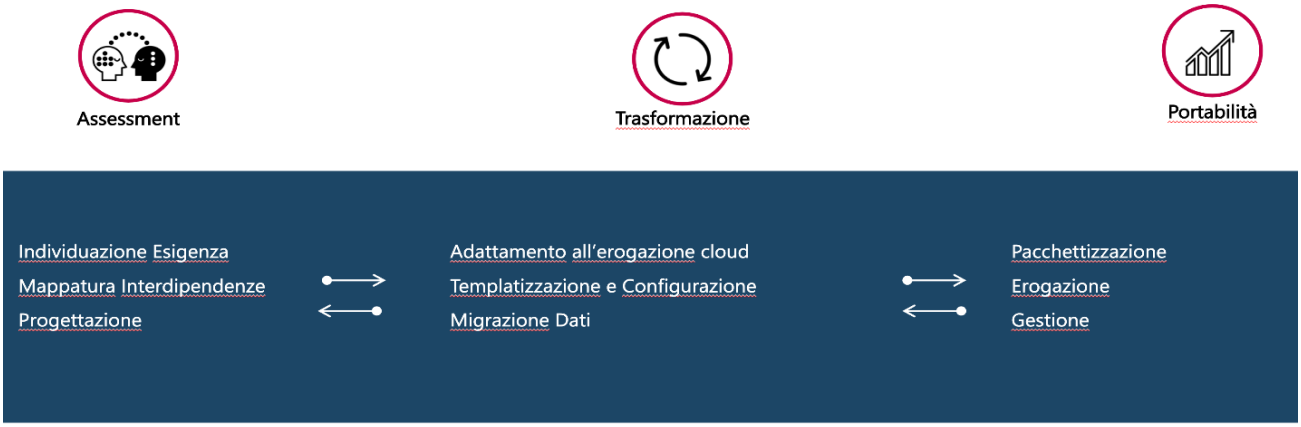
Il servizio proposto, descritto nelle pagine seguenti, è erogato in SaaS coerentemente con i requisiti della qualificazione AgID, la cui scheda è reperibile all'url:

https://catalogocloud.agid.gov.it/service/506

Per poter gestire scenari dinamici ed in costante evoluzione, è importante costruire un approccio al Cloud che consenta di ridurre al minimo la complessità ed i costi di transizione tra diversi service provider. Per questo motivo si è deciso di adottare Kubernetes, che consente di raggiungere un livello di astrazione tale da poter rendere un intero data center auto contenuto e descritto da manifesti di configurazione replicabili e ripetibili. Il dispiegamento avviene attraverso l'orchestrazione di tecnologie moderne ed affidabili, al fine di costruire un'infrastruttura dinamica, robusta e con capacità computazionali adattive rispetto al carico di lavoro.

TRASFORMAZIONE

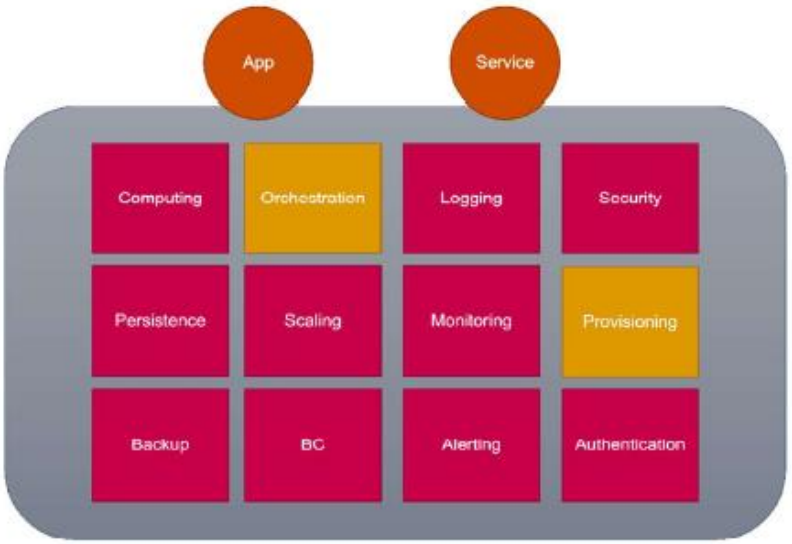
L'approccio è dunque orientato alla trasformazione più che alla migrazione.



La trasformazione permette di effettuare un re-platforming che evolve le applicazioni secondo uno schema che le renda scalabili, pacchettizzabili e trasportabili. Questo consente di potersi adattare rapidamente e con sforzi contenuti a nuovi scenari, quale il cambio di Cloud Service Provider o la distribuzione su più Cloud Service Provider delle componenti.

LA PIATTAFORMA MPC – MUNICIPIA PORTABLE CLOUD

La piattaforma MPC è basata su concetti nativi del cloud, tra i quali ricordiamo: Applicazioni e servizi standardizzati - Immutable Infrastructure - Infrastructure as code - Replicabilità – Trasportabilità - Orchestrazione centralizzata.



Il paradigma cloud richiede che siano fornite a corredo delle applicazioni una serie di componenti sintetizzate per macrocategorie nella figura di cui sopra.

Questi servizi sono stati progettati per l'erogazione SaaS di Municipia, ma sono anche stati pacchettizzati per poterli impiegare laddove necessario anche in contesti esterni e resi fruibili da remoto per integrarsi con ambienti eterogenei.

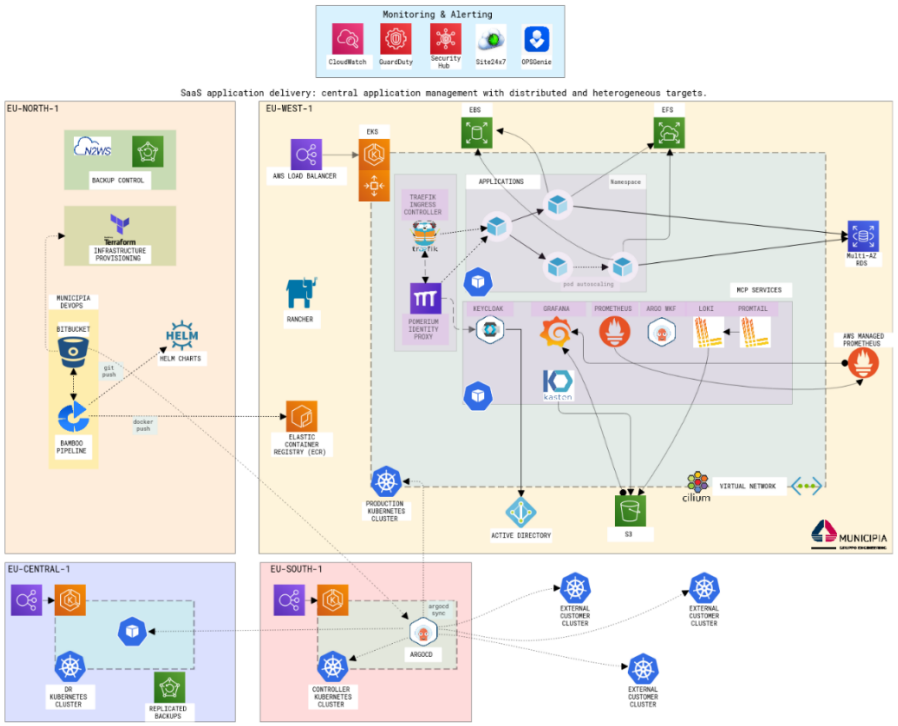
Sia gli applicativi che le componenti a corredo sono orchestrati da un sistema centralizzato che consente il dispiegamento e la configurazione degli stessi internamente o esternamente al cloud di Municipia.

Il servizio SaaS di Municipia è erogato attraverso Amazon Web Services, ed è progettato per essere resiliente. Il modello sfrutta appieno le potenzialità di ridondanza e scalabilità offerte da AWS, facendo leva sulla multi zonalità e la multi geograficità e sui relativi servizi di piattaforma. AWS divide i data center in regioni e zone di disponibilità. Una regione (Region) è un'area geografica, una zona di disponibilità (AZ) è un data center di quell'area interconnesso con le altre AZ. Le interconnessioni sono effettuate con canali trasmissivi ad alta velocità ed affidabilità.

Le applicazioni sono dispiegate in maniera tale per cui il load balancer di frontiera, componente di piattaforma AWS auto scalante ed auto ridondato, inoltri le richieste alle istanze applicative su tutte e tre le AZ. I nodi EC2 che forniscono la potenza computazionale sono distribuiti su tutte e tre le zone, mentre la banca dati ha una zona di elezione e una replica su un'altra zona. Nel caso si rendesse indisponibile una zona, l'erogazione proseguirebbe dalle zone ancora disponibili. In caso di necessità di maggiore potenza computazionale, il sistema aggiungerà nodi EC2 per garantire livelli prestazionali adeguati. L'adeguamento computazionale della banca dati avverrà tramite un monitoraggio costante delle prestazioni, con implementazione della scalabilità secondo necessità e senza interruzione di servizio.

Il sistema di gestione di Backup e DR è dispiegato in una regione differente rispetto agli applicativi). L'immagine dei dati è replicata su altra regione, in modo da garantire le attività di Backup e DR anche in caso di indisponibilità della regione principale.

Tutte le componenti infrastrutturali sono dispiegate secondo una libreria di codice sorgente che le rappresenta e, grazie al backup dei dati replicato su un'altra regione, sarebbe possibile ripristinare l'intero sistema partendo dal codice stesso. Per ottimizzare i tempi, è mantenuto attivo un cluster di DR, in modo da poter partire già da un sistema con le componenti base pronte all'uso.



CARATTERISTICHE DELL'EROGAZIONE SAAS DI MUNICIPIA

I servizi SaaS standard di Municipia sono erogati dai data centre di Amazon Web Services, qualificato come CSP sul marketplace AGID, ubicati nel territorio dell'Unione Europea e rispondenti a tutte le caratteristiche di sicurezza, disponibilità e tutela del dato necessarie.

La tabella seguente riporta le caratteristiche principali del modello di erogazione standard offerto da Municipia.

Nome	Definizione	Valore
Profondità di Backup	Tempo di conservazione in giorni dei backup della banca dati applicativa.	30 giorni sul sito primario 7 giorni sul sito secondario
Granularità di Backup	Punti di ripristino point-in-time nel perimetro della profondità di backup.	5 minuti
Disastro	Indisponibilità completa e persistente della regione di erogazione primaria che non consente l'utilizzo delle applicazioni da parte degli utenti finali.	
RPO (Recovery Point Objective)	Anzianità del dato ripristinato rispetto all'occorrenza dell'evento disastroso.	5 minuti
RTO (Recovery Time Objective)	Tempo necessario al ripristino delle funzionalità minime necessarie all'operatività del sistema. Si calcola a partire dalla dichiarazione dell'evento disastroso.	12h
Availability Media	Disponibilità media dei sistemi erogati in SaaS nel periodo di esercizio da contratto.	99,2%
Numero di zone di disponibilità	Zone geografiche distinte di erogazione contemporanea e replica dati all'interno di una Regione	3

I sistemi sono disponibili agli utilizzatori garantendo una percentuale di availability media pari al 99,2%. Municipia si riserva di operare, con comunicazione al cliente anticipata di 3 giornate lavorative, interventi di manutenzione programmata, nella finestra temporale dalle 21 alle 5. Tali interventi non ricadono nel computo dei livelli di servizio collegati alla disponibilità dei sistemi.

PROPOSTA PROGETTUALE

Di seguito sono descritte brevemente le macro-attività che il progetto di migrazione prevede; la puntuale organizzazione e le specifiche modalità di dispiegamento. Queste ultime saranno naturalmente convenute con i Vostri uffici con l'obiettivo di massimizzare l'efficacia del processo di verifica preliminare, minimizzando invece gli impatti operativi al momento dell'esecuzione dell'effettiva migrazione.

ATTIVITA' DI MIGRAZIONE STANDARD

La migrazione verso il Cloud prevede le seguenti attività:

- Attività di migrazione standardizzata o personalizzata, per adattare al meglio tempi e modalità di trasferimento dei servizi in Cloud: la migrazione personalizzata permette di mantenere, possibilmente per un periodo limitato e in attesa del completo adeguamento dei servizi terzi, eventuali integrazioni o personalizzazioni che non consentano una migrazione standardizzata. La migrazione personalizzata avrà impatti sui tempi di migrazione e renderà il dispiegamento SaaS dipendente da servizi e sistemi fuori dal controllo di Municipia, ma consentirà di migrare lo stesso qualora i servizi integrati non fossero pronti.
- Attivazione istanza JEnte Cloud;
- Migrazione banca dati Ente: JEnte Cloud utilizza come RDBMS PostgreSQL. Qualora il RDMBS utilizzato on-premises fosse diverso da quello utilizzato in Cloud è prevista un'attività di conversione
- Migrazione file, directory, documenti;
- Attivazione istanza Servizi On-Line e Portale Dipendenti (ove presenti);
- Attivazione processi automatizzati quali acquisizione timbrature (ove presenti), estrazioni standard applicativi (anagrafe, etc.);
- Trasferimento e adeguamento WS a requisiti di sicurezza. L'esposizione di servizi in ambiente Cloud sarà erogata secondo i più moderni standard di sicurezza. Qualora l'Ente volesse mantenere inalterati gli end-point dei servizi esposti da jEnte è disponibile un *servizio aggiuntivo* standard di VPN tra selezionate macchine dell'Ente e il Cloud Municipia (jProxyCloud). Si consiglia tuttavia di utilizzare solo temporaneamente questa soluzione e di effettuare quanto prima l'adeguamento all'erogazione standard e protetta di servizi in Cloud. Queste considerazioni sono valide sia per i servizi esposti che per i servizi richiamati da jEnte;
- Coordinamento processi con interazioni esterne (WS server, WS client, servizi condivisione file, fornitori PEC ed e-mail ordinarie, servizi regionali, etc.) e mappatura processi schedulati.
- Attività di testing funzionalità di base Ente in ambiente Cloud;
- Valutazione generale comprensiva di intervista con il cliente e compilazione scheda parametri. Questa attività è di fondamentale importanza per individuare caratteristiche applicative fuori standard e permettere lo studio di una soluzione personalizzata o attraverso servizi aggiuntivi.
- Attività di coordinamento alla migrazione.
- Migrazione definitiva verso l'ambiente cloud.

SERVIZI AGGIUNTIVI

A seconda delle caratteristiche dell'installazione On Premise dell'Ente è possibile che si rendano necessarie attività aggiuntive descritte nelle pagine seguenti e quotate nel Capitolo 1 Proposta Economica.

MIGRAZIONE DB

In fase di valutazione è stato censito l'utilizzo di un DB diverso dallo standard, PostgresSQL. Il servizio aggiuntivo prevede la migrazione dal DB Oracle o MS-SQL Server.

COLLEGAMENTO LDAP ENTE

In fase di valutazione è stata censita la necessità di collegamento del sistema di autenticazione utenti con il sistema LDAP in uso presso l'Ente. Il servizio prevede che il sistema di autenticazione in ambiente Cloud venga configurato per interagire con l'LDAP installato presso il cliente. L'Ente si impegna ad esporre in maniera pubblica e sicura il proprio sistema LDAP (cifratura, scambio certificati, filtri IP, etc…). Qualora non sia possibile garantire una modalità sicura e certificata di esposizione del proprio sistema LDAP verrà compreso nell'offerta il servizio jProxyCloud. Una volta collegato il sistema di autenticazione di JEnte al sistema LDAP dell'Ente verrà creata una dipendenza in termini di corretto funzionamento; malfunzionamenti o disservizi dovuti a sistemi erogati direttamente dall'Ente (esempio ldap dell'Ente non funzionante) implicheranno anche la mancata fruizione della suite jEnte.

JPROXYCLOUD

In fase di valutazione è stata censita la necessità da parte dell'Ente di accedere alla propria installazione in Cloud fuori dai canali standard in termini di sicurezza. Il servizio prevede l'attivazione, tra ambiente Municipia Cloud e quello dell'Ente di una VPN site-to-site, chiamata jProxyCloud. Tale componente permette, ad esempio, l'accesso a un LDAP non esposto in sicurezza, l'accesso diretto al DB o al file system, etc. Questa VPN è basata sul protocollo Wireguard, e prevede l'installazione di un agent su ogni macchina che dovrà essere in grado di comunicare con i sistemi in Cloud. L'agent si configurerà automaticamente comunicando con il sistema cloud di Municipia, che sarà in grado di gestirlo centralmente. L'Ente si impegna a mettere a disposizione macchine che supportino i requisiti della VPN jProxyCloud, e a mantenerle attive e funzionanti per tutto il periodo di necessità della VPN.

SFTP DEDICATO

In fase di valutazione è stata censita la necessità di creare un'area di interscambio tra le applicazioni JEnte Cloud e altre realtà. Il servizio prevede l'attivazione di un'area di scambio SFTP dove l'Ente potrà accedere direttamente o garantire l'accesso ad applicativi terzi, per scaricare o caricare flussi di interscambio.

MODALITA' DI MIGRAZIONE

Per quanto riguarda la migrazione sarà effettuata in **modalità standard** senza nessun accesso diretto da parte dell'Ente al database, filesystem o infrastruttura erogata in modalità SaaS da Municipia e che non sarà previsto nessun accesso diretto dall'infrastruttura SaaS Municipia all'infrastruttura interna dell'Ente.

CARATTERISTICHE DEL SERVIZIO DI MANUTENZIONE E ASSISTENZA

Per prendere visione delle caratteristiche del servizio di Manutenzione e Assistenza erogati da Municipia cliccare qui .

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

L'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
- garantire l'interoperabilità del servizio SaaS e la portabilità del servizio e dei dati, come previsto dalla circ. AgID n.3 del 9/4/18
- a restituire al Cliente, in caso di richiesta, gli archivi di propria competenza in formato CSV corredato del relativo tracciato dati. È possibile, su richiesta, avere anche l'esportazione della banca dati direttamente nel formato nativo dell'applicazione. 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 di 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 i documenti di "attivazione lavori" debitamente compilati e sottoscritti (laddove previsti)
- rispetti le tempistiche indicate nelle schede tecniche per la fornitura dei flussi informativi oggetto della fornitura (laddove previsti)

DURATA OFFERTA

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

ADESIONE - DURATA – RECESSO

L'**adesione** al contratto deve avvenire attraverso la sottoscrizione del Modulo d'Ordine e l'invio determina.
Il contratto termina con la fine del progetto di migrazione.
La prosecuzione del servizio di erogazione SaaS, manutenzione ed assistenza sarà regolamentata dall'emissione e sottoscrizione di specifico contratto. Sarà cura di Municipia inoltrare al Cliente il contratto di rinnovo del servizio per un periodo definito in accordo con il Cliente.

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.

Per il **recesso** vige quanto stabilito dalle condizioni generali di contratto relative alla prestazione di servizi del bando MEPA di riferimento.

In caso di recesso formalizzato dal Cliente, Municipia, previa apposita comunicazione inviata al Cliente, provvederà a disabilitare le credenziali di accesso al servizio.

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.

La **fatturazione** avverrà a conclusione delle attività contrattualizzate.

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 tutte le attività non strettamente connesse al progetto di migrazione.

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.
Riferimento e-mail: **dpo.privacy.municipia@eng.it – dpo.privacy@eng.it**

DIRITTI E 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.
È 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:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) 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'**Allegato 2**, 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'**Allegato 1**.
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 DEI 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.
Fermo restando quanto stabilito al precedente articolo 4, il Responsabile del trattamento, nell'ipotesi in cui nomini Sub-Responsabili che siano stabiliti fuori dall'Unione Europea, si obbliga a rispettare le previsioni di cui agli artt. 44-50 del Regolamento. In particolare, nei casi in cui sussista la necessità che il trasferimento dei Dati Personali avvenga in conformità alle Clausole Contrattuali Tipo, il Responsabile, in forza del presente Accordo, deve intendersi espressamente autorizzato a concludere con i propri Sub-Responsabili le Clausole Contrattuali Tipo che disciplinano il trasferimento da responsabile del trattamento a responsabile del trattamento in conformità a quanto previsto nella decisione 2021/914 della Commissione Europea del 4 giugno 2021. Le Clausole Contrattuali Tipo che disciplinano il trasferimento da responsabile del trattamento a responsabile del trattamento dovranno essere sottoscritte qualora i Sub-Responsabili siano stabiliti in un Paese non appartenente allo Spazio Economico Europeo per il quale la Commissione Europea non ha emesso una decisione di adeguatezza, in aggiunta ad eventuali misure supplementari individuate conformemente a quanto indicato dal Comitato Europeo per la protezione dei dati personali ("EDPB"), secondo quanto indicato nelle "*Raccomandazioni 01/2020 sulle misure che integrano gli strumenti di trasferimento per garantire il rispetto del livello di protezione dei dati personali nell'UE*" e nelle "*Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza*".
In particolare, il Cliente è reso edotto che il Responsabile del trattamento potrà avvalersi ai fini dell'esecuzione del Servizio anche delle proprie controllate situate al di fuori dello Spazio Economico Europeo, fermo restando il rispetto di quanto previsto nel presente accordo ed, in ogni caso, attenendosi alle eventuali specifiche istruzioni ricevute dal Titolare.
Previa richiesta, il Titolare può autorizzare il Responsabile a procedere alla revisione delle Clausole Contrattuali Tipo solo per estendere all'entità extra SEE obblighi più rigorosi e ottenerne una copia integrale dal Responsabile del Trattamento.

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 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 DEL DATA BREACH

In caso di violazione dei dati personali, il responsabile del trattamento deve informare il Titolare della violazione (o presunta violazione) entro 48 ore 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'**Allegato 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 SPA – TRENTO - PEC** municipia@pec.eng.it
- per il Titolare del trattamento **COMUNE DI CASTEL IVANO,** PIAZZA MUNICIPIO, 12, 38059 CASTEL IVANO, (TN)
  PEC info@pec.comune.castel-ivano.tn.it

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 terzo 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 o in UE su uno o più Datacenter di Engineering o di Fornitori Terzi di Infrastruttusa Cloud (a titolo di es. AWS), che rispettano la certificazione Agid prevista dalle normative e dalle linee di indirizzo, nonché dai bandi PNRR.

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.

Allegato 1	**ELENCO SUB-RESPONSABILI** **MD14_PGT01_0_Allegato_Elenco_SubResponsabili**
Prodotto/i	jEnte (SaaS) Assistenza e Manutenzione | Sviluppo Prodotto

Ad integrazione di quanto specificato nell'offerta e/o nel contratto principale relativamente ai fornitori che tratteranno dati per conto del Titolare come sub-responsabili del trattamento, e che si intendono dal Titolare già autorizzati con l'accettazione dell'offerta, il Titolare autorizza il Responsabile ad affidare parte delle operazioni di trattamento ai seguenti ulteriori sub-responsabili:

Paese cui è stabilito Sub-Responsabile	**Sub-Responsabili**	**Dati di contatto**	**Attività di trattamento affidata**
Lussemburgo	Amazon Web Services EMEA SARL	https://aws.amazon.com/it/contact-us/	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.

Allegato 2	**CARATTERISTICHE DEL TRATTAMENTO E MISURE TECNICHE E ORGANIZZATIVE** **MD15_PGT01_0_Allegato_Caratteristiche_Trattamento_Dati**
Prodotto/i	jEnte (SaaS) 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
Il Responsabile e/o Sub-Responsabile e/o suoi ulteriori Responsabili adotteranno le seguenti misure di sicurezza al fine di garantire un livello di sicurezza adeguato al rischio relativo alle attività che ricadono nella loro diretta responsabilità.

Il Cliente, in considerazione dei rischi associati al Trattamento dei Dati Personali, conferma che le Misure di Sicurezza adottate dal Responsabile e/o Sub-Responsabile e/o suoi ulteriori Responsabili sono idonee a fornire un adeguato livello di protezione dei Dati Personali trattati per conto dello stesso.

Nel caso in cui il Cliente operasse per conto di un Titolare terzo, il Cliente si riserverà di integrare e/o modificare le misure di sicurezza come richiesto dallo stesso Titolare.

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.

Risk Level	Categoria	ID	Descrizione
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**	È 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 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.
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**	È 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.

Risk Level	Categoria	ID	Descrizione
B	**Controllo degli accessi ed autenticazione**	**K.3**	È 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**	È necessario registrare 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. È 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 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 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.

Risk Level	Categoria	ID	Descrizione
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 accessibile da personale non autorizzato.
M	**Sicurezza fisica** (solo per Cloud SaaS)	**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, stabilita, a seconda dei casi.
M	**Sicurezza fisica** (solo per Cloud SaaS)	**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** (solo per Cloud SaaS)	**T.4**	I sistemi di rilevamento antintrusione sono installati in tutte le zone di sicurezza.
M	**Sicurezza fisica** (solo per Cloud SaaS)	**T.5**	Le barriere fisiche sono costruite per impedire l'accesso fisico non autorizzato.
M	**Sicurezza fisica** (solo per Cloud SaaS)	**T.6**	Le aree non usate sono fisicamente bloccate e periodicamente riesaminate.
M	**Sicurezza fisica** (solo per Cloud SaaS)	**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** (solo per Cloud SaaS)	**T.8**	Il personale di supporto esterno ha accesso limitato alle aree protette.

Allegato 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
☐ È 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 violazione e/o impedirne il perpetrarsi o il ripersi della stessa)

_____

_____