MUNICIPIA
AUGMENTED CITY

PROPOSTA TECNICO ECONOMICA

RINNOVO DEL SERVIZIO DI MANUTENZIONE E ASSISTENZA SOLUZIONI MUNICIPIA

Spettabile Amministrazione Comunale di
REGGIO EMILIA
pec comune.reggioemilia@cert.provincia.re.it

Alla cortese attenzione
Nando Rinaldi
mail segreteria.istituzione@comune.re.it

DATA EMISSIONE 22/12/2022 - **RIF.** MAN-256593/2022

OGGETTO
Rinnovo Contratto di manutenzione e assistenza
Suite jEnte per Istituzione Scuole e Nidi d'Infanzia del Comune di Reggio Emilia

RIFERIMENTO MUNICIPIA
Account Manager Cesare Rovati
e-mail Cesare.Rovati@eng.it
mobile 3462359608

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: Raffaele Mazza
Organizzazione: MUNICIPIA S.P.A./01973900838
Data: 27/12/2022 11:28:57

PREMESSA

RINNOVO DEL SERVIZIO DI MANUTENZIONE E ASSISTENZA SIA PER LE EROGAZIONI ON PREMISES SIA PER QUELLE IN CLOUD SAAS

Questo documento rappresenta la proposta tecnico economica per il rinnovo del canone di **manutenzione e assistenza** delle soluzioni Municipia sia per le erogazioni On Premises sia per quelle in Cloud SaaS.

L'Ente può aderire al rinnovo in forma:

- **Annuale 2023:** in questo caso il servizio viene erogato per un anno solare (01 Dicembre – 31 Gennaio) ai prezzi indicati nel contratto
- **Triennale 2023-2025:** in questo caso il servizio viene erogato per n. 3 (tre) annualità. A parità di perimetro dell'installato i canoni non subiranno aumenti fino alla scadenza contrattuale. La fatturazione sarà emessa in forma annuale

L' adesione – in base alla formula desiderata (annuale o triennale) - deve essere formalizzata **entro e non oltre il 31/12/2022.**

In questo documento sono indicate anche le quotazioni per i **pacchetti di giornate di assistenza** acquistabili su **MEPA.**

CAPITOLO 1

PROPOSTA ECONOMICA

Nella seguente tabella sono riportati gli importi per il rinnovo contrattuale per le soluzioni Municipia adottate dal Cliente:

Soluzioni Municipia | Servizio di Manutenzione-Assistenza	Canone Annuale dal 01/01/23 al 31/12/23	Canone Triennale dal 01/01/23 al 31/12/25
Barrare la casella per il periodo scelto	☐	☐
Suite jEnte per Istituzione Scuole e Nidi d'Infanzia del Comune di Reggio Emilia **Tipo Erogazione:** ON PREMISES **Area Nucleo Informativo Centrale|** Nucleo Informativo Centrale **Area Servizi Finanziari |** Buoni d'Ordine a Fornitori - Cespiti Patrimoniali - Contabilità Analitica - Contabilità Economico Patrimoniale - Contabilità Finanziaria - Fatturazione Attiva (integrazione con PagoPa) - Richieste Interne di approvvigionamento - SDI Link documenti passivi - Siope+	5.722,00	18.088,00
TOTALE MANUTENZIONE E ASSISTENZA	**5.722,00**	**18.088,00**
Installazione release di aggiornamento presso la server farm dell'Amministrazione (a cura di Municipa)		
TOTALE GENERALE	**5.722,00**	**18.088,00**

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.

Gli importi sopra indicati, riferiti al servizio si manutenzione e assistenza, sono comprensivi di un (lieve) aumento che deriva dall'applicazione della rivalutazione dei costi (Istat), costi che quest'anno non riusciamo ad assorbire.

MODULO D'ORDINE

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

L' Ente / Azienda: **REGGIO EMILIA**
PI **00145920351** CF **00145920351** - Pec comune.reggioemilia@cert.provincia.re.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

PROPOSTA TECNICA

Municipia fornisce al Cliente, che sottoscrive il presente contratto, il servizio di manutenzione e assistenza per le soluzioni software indicate nel capitolo 1. Proposta Economica "Modulo d'Ordine" che contiene anche il prezzo della fornitura.

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

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

Il servizio è erogato come di seguito descritto:

MANUTENZIONE

In questa sezione sono descritte le caratteristiche della manutenzione effettuata sugli applicativi al fine di garantirne il corretto funzionamento; sono anche indicate le modalità di rilascio degli aggiornamenti.

MANUTENZIONE CORRETTIVA

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

La metodologia applicata da Municipia segue due approcci:

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

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

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

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.

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

PER EROGAZIONE IN SAAS

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

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

PER EROGAZIONE ON PREMISE

Il cliente è messo nelle condizioni di aggiornare autonomamente i propri ambienti on premise, qualora decida di avvalersi del supporto di Municipia, si evidenzia che tale servizio è a pagamento a meno di differenti accordi contrattuali già in essere.

Nel caso in cui il cliente intenda affidare a Municipia l'installazione degli aggiornamenti, nel modulo d'ordine è indicato l'importo da riconoscere per l'esecuzione di tale attività.

Nel caso in cui il cliente abbia già acquistato il pacchetto di installazione e questo sia in corso di validità, l'attività non deve essere barrata nel modulo d'ordine.

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

ASSISTENZA – SERVICE DESK

Le attività di assistenza vengono prestate da Municipia esclusivamente a personale del Cliente (Comune, Unione, Altro) e/o a suoi delegati. Pertanto non è compresa, in questo contratto, l'erogazione di assistenza verso personale diverso da quello sopra indicato (ad esempio cittadini, e/o imprese.)

Di seguito sono descritte 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), *in assenza di vincoli contrattuali diversi*, è garantita per tutto l'anno sulla base del modello "5 x 8", 5 giorni alla settimana per 8 ore al giorno

Orari di assistenza per le procedure ARGO TRIBOX GEIS GNOSIS MUNIPAY INES
dal lunedì al venerdì (nei giorni feriali) - dalle 09:00 alle 13:00 e dalle 14:00 alle 18:00

Orari di assistenza per la SUITE JENTE
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		

CARATTERISTICHE TECNOLOGICHE INFRASTRUTTURA (QUESTA SEZIONE È VALIDA SOLO PER L'EROGAZIONE IN SAAS)

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

Dettagliamo di seguito alcuni aspetti di interesse:

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

Backup e sicurezza dei dati: le parti applicative sono salvate con procedure automatiche centralizzate incrementali e a

rotazione. È possibile ripristinare selettivamente le basi dati, per Enti o per singolo dato. Le politiche di ritenzione del dato prevedono:

Istanze Applicative: Back-up snapshot based giornaliero incrementale con conservazione degli ultimi 7 giorni.

DataBase: Backup giornaliero con retention di 30 giorni.

Architettura Backup: il backup e il ripristino dei dati avvengono attraverso una copia consistente della banca dati del singolo Ente. L'intera area di backup è clonata al termine delle procedure di backup su altro datastore per garantire il ripristino in caso di indisponibilità dell'area di backup principale.

Casi e tempi di ripristino: nel caso di un evento distruttivo sul datastore che ospita il database, è possibile il ripristino alla sera del giorno precedente l'evento, combinando i dati salvati dai backup periodici e il backup della macchina DB. Nel caso di una modifica involontaria o di un errore applicativo che abbia reso inconsistente il database, è possibile il ripristino a un qualsiasi backup eseguito nell'ambito delle politiche di ritenzione. I tempi di ripristino sono entro le 24 ore lavorative.

Architettura Backup Macchine Applicative: le aree applicative sono salvate con sistemi di backup che, secondo i livelli di ritenzione illustrati, conservano l'intero file system e i parametri dell'ambiente. I dati sono salvati su datastore diversi da quelli sui quali risiedono le macchine stesse.

Casi e tempi di ripristino: nel caso di perdita completa dell'area applicativa, è possibile un ripristino completo entro 8 ore lavorative. Nel caso di necessità di ripristino di parti del file system in seguito a errori applicativi o umani, è possibile un ripristino entro 4 ore lavorative. In entrambi i casi è possibile ripristinare a un qualsiasi punto conservato secondo le specifiche di ritenzione del dato.

Business Continuity: L'erogazione dei servizi di connettività, alimentazione, sicurezza è garantito 24x7x365 dal Data Center. Le strutture che ospitano gli ambienti sono completamente ridondate per il *single point of failure* verso lo storage e la connettività.

ARCHITETTURA

L'**architettura** software proposta, come è stato evidenziato nel precedente paragrafo, è sicura e in linea con i più evoluti orientamenti *SaaS*. Le applicazioni e la banca dati risiedono su ambienti gestiti da Municipia ed è possibile fruirli attraverso un qualsiasi browser Internet aggiornato.

L'aggiornamento del software con l'installazione delle nuove versioni rilasciate e i salvataggi della banca dati sono demandati a Municipia.

L'architettura proposta ha diversi vantaggi che riepiloghiamo brevemente:

Sicurezza della Banca Dati Presso il CSP sono attivi sistemi di sicurezza, back-up e protezione del dato, che assicurano che nessuna informazione delle Banche Dati custodite vada perduta.

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

LIVELLI DI SERVIZIO

I sistemi sono disponibili agli utilizzatori 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.

PENALI

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

REQUISITI MINIMI PER L'EROGAZIONE ON PREMISE

Ai seguenti link sono riportati i requisiti minimi infrastrutturali che garantiscono un corretto funzionamento degli applicativi installati c/o il Cliente:

- **TRIBOX** https://confluence.municipia.eng.it/x/opBaCQ
- **JENTE** https://confluence.municipia.eng.it/x/r5BaCQ

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.

Si precisa che, in caso di acquisto di pacchetto, il prezzo delle giornate diminuisce rispetto all'acquisto della singola giornata

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 il prodotto **INES Cloud e assimilati (Settore Mobilità)** sono erogate solo giornate da remoto.
- L'orario di erogazione delle attività acquistate con il pacchetto di giornate è quello d'ufficio.

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**

AMBIENTE DI COLLAUDO

Si specifica che, *a meno di accordi contrattuali già in essere con il Cliente*, l'ambiente di collaudo non è compreso in questo contratto.

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 del servizio di manutenzione e assistenza relativo ai prodotti software utilizzati dal cliente che ha aderito alla presente proposta (commissione abbonamento).

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.

DURATA OFFERTA

L'offerta ha validità fino al **31/12/2022**.

ADESIONE - DURATA – RECESSO

L'**adesione** al contratto deve avvenire attraverso la sottoscrizione del Modulo d'Ordine entro il 31/12/2022 ed il successivo invio della determina.

In caso di mancata adesione nei termini sopra indicati, Municipia potrà sospendere l'erogazione dei servizi di assistenza e invio aggiornamenti a decorrere dal 1° Gennaio dell'anno non avente copertura contrattuale.
A seguito della mancata adesione Municipia procederà, dandone apposita comunicazione al Cliente, a disabilitare le credenziali di accesso al servizio.
Il contratto di erogazione del servizio 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 al servizio di manutenzione e assistenza sono indicati nel capitolo della proposta economica e sono riportati al netto di IVA. Gli importi dovuti dal Cliente saranno **fatturati** in unica rata annuale anticipata per quanto di competenza di ogni singolo anno. In conformità con il D.lgs. 192/2012 **i pagamenti** dovranno essere effettuati tramite Bonifico Bancario entro 30 giorni data fattura. In caso di ritardato pagamento gli interessi moratori ai sensi dell'art. 4 del suddetto D.lgs. decorrono, senza che sia necessaria la costituzione in mora, dal giorno successivo alla scadenza del termine di pagamento. Il tasso dell'interesse di mora (art. 5 del Dlgs 231/2002 modificato dal Dlgs 192/2012) è pari al saggio di interesse del principale strumento di rifinanziamento della Banca Centrale Europea rilevato il primo giorno di ogni semestre, aumentato di otto punti percentuali.

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 nelle condizioni di acquisto dei Mercati Elettronici 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.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**

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 il 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.

ACCORDO AL TRATTAMENTO DATI PERSONALI

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

PREMESSO CHE

A) Le vigenti disposizioni in materia di Trattamento dei Dati Personali prevedono che qualora un Trattamento di dati personali sia effettuato per conto di un Titolare del trattamento ("Titolare"), da una persona fisica o giuridica, una pubblica amministrazione o qualsiasi altro ente o associazione, quale Responsabile del Trattamento, il Titolare ricorra a soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di Trattamento dei Dati Personali, ivi compreso il profilo della sicurezza; pertanto il Responsabile del Trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti richiesti dalle Leggi applicabili in materia di protezione dei Dati Personali pro tempore vigenti in materia e garantisca la tutela dei diritti dell'Interessato;

B) che **Istituzione Scuole e Nidi d'Infanzia del Comune di Reggio Emilia** in qualità di Titolare del trattamento dei dati personali (di seguito il "Titolare"), relativamente alle informazioni identificate in oggetto, ha designato **REGGIO EMILIA,** (di seguito **il "Responsabile"**) come Responsabile del trattamento ai sensi dell'art. 28 del Regolamento;

C) che il Responsabile ha sottoscritto con il Titolare un contratto di trattamento dei dati personali che prevede un'autorizzazione generale in favore della prima per la stipula di contratti di trattamento con ulteriori soggetti che trattano dati personali nella fornitura dei servizi contrattualizzati;

D) che in forza del mandato conferito dal Titolare a Responsabile quest'ultimo affida a **Municipia SpA** con sede legale in Via A. Olivetti, 7 TRENTO (di seguito, **"Sub-responsabile"**), lo svolgimento del Servizio relativo alla fornitura e la gestione delle attività di "**Manutenzione e Assistenza Soluzioni Software**" così come specificate nel Contratto stipulato fra Responsabile e il Sub-responsabile di seguito, **le "Parti"**), nell'interesse di Titolare del Trattamento. A tal fine, il Responsabile nomina il Sub-responsabile del trattamento dei dati personali con riguardo alle operazioni di trattamento connesse all'esecuzione del Servizio, nel rispetto degli stessi obblighi in materia di protezione dei dati contenuti nell'Accordo TDP stipulato fra il Titolare e il Responsabile del trattamento.

E) Il Sub-responsabile deve procedere al trattamento secondo le istruzioni impartite dal Responsabile per iscritto con il presente accordo e i suoi allegati (congiuntamente denominati "Accordo per il Trattamento dei Dati Personali" o anche "Accordo TDP"), e deve inoltre presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti della normativa richiesti dalle disposizioni pro tempore vigenti in materia, e garantisca la tutela dei diritti dell'interessato;

F) È intenzione del Responsabile consentire l'accesso sia al Sub-responsabile che alle persone autorizzate al trattamento per i soli dati personali la cui conoscenza è necessaria per adempiere ai compiti loro attribuiti;

G) Con riferimento al servizio fornito dal Sub-responsabile, la descrizione delle finalità perseguite, della tipologia e delle modalità del Trattamento dei Dati Personali, così come indicate dal Titolare, è contenuta nell'**Allegato 2** del presente Accordo TDP.

DEFINIZIONI

Salvo che sia diversamente definito nel presente Accordo TDP, tutti i termini in maiuscolo utilizzati nel presente documento e nei suoi Allegati hanno il significato loro attribuito nel Contratto.

"**Autorità di Controllo**" indica ogni autorità competente a vigilare ed assicurare l'applicazione delle Leggi applicabili in materia di protezione dei Dati Personali con riferimento al Trattamento dei Dati Personali svolti per mezzo del Servizio;

"Categorie Particolari di Dati Personali" indica i Dati Personali che rivelino: l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il Trattamento di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

"Clausole Contrattuali Tipo" indica le "Standard Contractual Clauses" intese a disciplinare, nel rispetto del Regolamento, il trasferimento all'estero dei dati personali da titolare del trattamento a responsabile del trattamento ovvero il trasferimento all'estero dei dati personali da responsabile del trattamento a responsabile del trattamento, adottate dalla Commissione Europea con la Decisione 2021/914 del 4 giugno 2021;

"**Contratto**" indica l'accordo disciplinante la fornitura di servizi oggetto del contratto concluso tra le Parti, che si intende integrato nel presente Accordo TDP;

"**Accordo per il Trattamento dei Dati Personali" o "Accordo TDP**" indica il presente accordo per il Trattamento dei Dati Personali comprensivo degli Allegati 1 e 2 e 3 di eventuali accordi modificativi o integrativi;

"**Dati Giudiziari**" indica i dati relativi a condanne penali e a reati o alle relative misure di sicurezza;

"**Dati Personali del Titolare**" indica i Dati Personali trattati in relazione al Servizio fornito dal Responsabile per conto del Titolare per l'esecuzione del Contratto;

"Dati Personali" significa qualsiasi informazione riguardante una persona fisica identificata o identificabile ("Interessato") oggetto di Trattamento da parte del Responsabile per conto del Titolare in esecuzione del Contratto; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; al fine di evitare contrasti interpretativi, ha in ogni caso il significato previsto dal Regolamento e dalle Leggi applicabili in materia di protezione dei Dati Personali;

"Diritti dell'Interessato" sono i diritti riconosciuti all'Interessato dalle Leggi applicabili in materia di protezione dei Dati Personali come, nei limiti di applicabilità del Regolamento, ad esempio, il diritto di chiedere al Titolare l'accesso, la rettifica o la cancellazione dei Dati Personali, il diritto alla limitazione del Trattamento dei dati dell'Interessato o il diritto di opposizione al Trattamento, nonché il diritto alla portabilità dei dati;

"Incaricato/i" il personale, dipendenti, collaboratori a qualsiasi titolo del Responsabile che abbiano accesso ai Dati Personali e agiscono sotto l'autorità del Responsabile del Trattamento ai sensi dell'art. 29 del Regolamento;

"Interessato/i" ha il significato previsto dal Regolamento;

"Leggi applicabili in materia di protezione dei Dati Personali" indica, negli Stati membri dell'Unione Europea, il Regolamento e le complementari legislazioni nazionali in materia di protezione dei Dati Personali, comprensivi di ogni orientamento e/o *code of pratice* emessi dalla competente Autorità di controllo all'interno dell'Unione Europea (inclusi i

provvedimenti e/o delle Autorizzazioni e/o Linee Guida del Garante per la protezione dei dati personali in quanto applicabili); e/o, negli Stati extra UE, ogni vigente legislazione in materia di protezione dei Dati Personali relativa alla tutela ed al legittimo Trattamento di Dati Personali;

"Regolamento" indica il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE;

"Responsabile del Trattamento" (anche solo "**Responsabile**") indica la persona fisica o giuridica, la pubblica autorità, l'organismo o altro ente che effettua un Trattamento dei Dati Personali per conto del Titolare. Ai fini del presente Accordo TDP, il Responsabile è **REGGIO EMILIA**"

"**SEE**" indica lo Spazio Economico Europeo;

"**Servizio**" indica i servizi **Manutenzione e Assistenza Soluzioni Software** , oggetto del Contratto;

"**Sub-Responsabile**" indica un organismo individuato dal Responsabile per assisterlo nel (o che intraprenda direttamente qualsivoglia) Trattamento dei Dati Personali nel rispetto delle obbligazioni previste dal Responsabile e di cui al presente Accordo TDP, che sia stato autorizzato dal Titolare ai sensi dell'Art. 5 del presente Accordo TDP;

"Titolare del trattamento" (anche solo **"Titolare"**) indica la persona fisica o giuridica, la pubblica autorità, l'organismo o altro ente che, da solo o congiuntamente con altri soggetti, determini le finalità e le modalità del Trattamento dei Dati Personali;

"Trattare" o "**Trattamento**" significa qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a Dati Personali o insiemi di Dati Personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

"**UE**" indica l'Unione Europea;

"Violazione dei Dati Personali" indica la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque trattati.

OBBLIGHI DEL RESPONSABILE

Il Responsabile è consapevole e accetta che, nella misura necessaria a consentire l'erogazione del Servizio, comunicherà i Dati Personali di cui è Responsabile in virtù del contratto stipulato con il Titolare, al Sub-responsabile o ne consentirà a quest'ultimo l'accesso.

Il Responsabile affida al Sub-responsabile tutte - ed esclusivamente - le operazioni di trattamento dei dati personali necessarie per dare piena esecuzione al Servizio. In caso di danni derivanti dal trattamento, il Sub-responsabile ne risponderà qualora non abbia adempiuto agli obblighi della normativa pro tempore vigente in materia di trattamento di dati personali specificatamente diretti ai responsabili del trattamento o abbia agito in modo difforme o contrario rispetto alle legittime istruzioni del Responsabile.

Il Responsabile si impegna a comunicare ufficialmente al Sub-responsabile qualsiasi variazione si dovesse rendere necessaria nelle operazioni di trattamento dei dati. Il Sub-responsabile o le persone autorizzate al trattamento non potranno effettuare nessuna operazione di trattamento dei dati al di fuori di quelle necessarie sopra ricordate.

Il Responsabile dichiara di aver ricevuto dal Titolare garanzia che i dati oggetto del trattamento e trasmessi al Sub-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 Sub-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.

OBBLIGHI DEL SUB RESPONSABILE

Il Sub-responsabile del Trattamento, per quanto di competenza, è tenuto, in forza di legge e di Contratto, per sé e per gli Incaricati e per qualunque soggetto collabori con la sua attività, al rispetto delle Leggi applicabili in materia di protezione dei Dati Personali.

Fatti salvi gli obblighi stabiliti da parte del presente Accordo TDP, il Sub-responsabile del trattamento è obbligato a:

a) trattare i Dati Personali solo per quanto strettamente necessario all'erogazione del Servizio e solo limitatamente alla conduzione tecnico funzionale dei sistemi/servizi oggetto del Contratto;
b) per quanto di propria competenza, è tenuto in forza di legge e del presente contratto, per sé e per le persone autorizzate al trattamento che collaborano con la sua organizzazione, a dare attuazione alle misure di sicurezza richieste dal Responsabile nonché previste dalla normativa pro tempore vigente in materia di protezione dei dati personali, fornendo assistenza al Responsabile nel garantire il rispetto della medesima.
c) Il Sub-responsabile, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, deve assicurarsi che siano adottate le misure di sicurezza richieste dal Responsabile e/o dal Titolare.

In assenza di indicazioni puntuali sulle misure di sicurezza da adottare e/o sul livello di rischio del trattamento, il Sub-Responsabile si impegna a garantire le misure di sicurezza previste da ENISA adeguate ad un rischio Medio del trattamento, come indicate nell'Allegato 2, al fine di garantire: - se del caso, 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.

d) Il Sub-responsabile implementerà una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento, trasmettendo tempestivamente al Responsabile la documentazione tecnica relativa sia alle misure di sicurezza in atto sia alle modifiche in seguito adottate.

e) Il Sub-responsabile mette a disposizione del Responsabile tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente contratto e della normativa applicabile, consentendo e contribuendo alle attività di revisione, comprese le ispezioni, realizzate dal Responsabile o da un altro soggetto da questi incaricato. A tale scopo il Sub-responsabile riconosce al Responsabile, e agli incaricati dal medesimo, il diritto di accedere ai locali di sua pertinenza ove hanno svolgimento le operazioni di trattamento o dove sono custoditi dati o documentazione relativa al presente contratto, purché il Responsabile informi il Sub-Responsabile dell'intenzione di effettuare l'accesso con un congruo preavviso non inferiore a 7 (sette) giorni lavorativi. In ogni caso il Responsabile si impegna per sé e per i terzi incaricati da quest'ultimo, a mantenere la riservatezza sulle informazioni raccolte durante le operazioni di verifica e pertanto a non comunicarle a soggetti terzi, salvo sia necessario in adempimento di un obbligo di legge o dal presente Accordo.

f) Il Sub-responsabile sarà, inoltre, tenuto a comunicare tempestivamente al Responsabile 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 effettuato per conto del Responsabile.

g) Il Sub-responsabile, nell'ambito della propria struttura aziendale, provvederà ad individuare le persone fisiche autorizzate al trattamento. Contestualmente alla designazione, il Sub-responsabile si fa carico di fornire adeguate istruzioni scritte alle persone autorizzate al trattamento circa le modalità del trattamento, in ottemperanza a quanto disposto dalla legge e dal presente contratto. A titolo esemplificativo e non esaustivo, il Sub-responsabile, nel designare per iscritto le persone autorizzate al trattamento, dovrà prescrivere che essi abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati. Dovrà, inoltre, verificare che questi ultimi applichino tutte le disposizioni in materia di sicurezza relativa alla custodia delle parole chiave (trattamenti elettronici) e che conservino in luogo sicuro i supporti non informatici contenenti atti o documenti con categorie particolari di dati (dati sensibili o giudiziari) o la loro riproduzione, adottando contenitori con serratura (trattamenti cartacei).

Il Sub-responsabile dovrà altresì verificare che gli incaricati implementino e utilizzino misure operative, tecniche e organizzative adeguate ai sensi dell'art. 32 del Regolamento per proteggere i Dati Personali (comprese le Categorie Particolari di Dati Personali, qualora presenti), in particolare contro:

- distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a Dati Personali trasmessi, conservati o comunque trattati.
- Trattamento dei Dati Personali non consentito o non conforme alle finalità delle operazioni di Trattamento;

Sarà cura del Sub-responsabile vincolare le persone autorizzate al trattamento alla riservatezza o ad un adeguato obbligo legale di riservatezza, anche per il periodo successivo all'estinzione del rapporto di collaborazione intrattenuto con il Sub-responsabile, in relazione alle operazioni di trattamento da esse eseguite.

h) Inoltre, ove occorrer possa e per quanto concerne i trattamenti effettuati per fornire il Servizio dalle persone autorizzate al trattamento con mansioni di "Amministratore di Sistema", il Sub-responsabile è tenuto altresì al rispetto delle previsioni pro tempore applicabili 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 Sub-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 Responsabile su richiesta del medesimo; a svolgere un'attività di verifica, con cadenza almeno annuale, sull'operato degli amministratori di sistema.

i) Il Sub-Responsabile, inoltre, qualora il Servizio sia erogato attraverso l'utilizzo dei suoi sistemi, si impegna ad adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi. Qualora l'obbligo di gestire l'access log sia in capo al Responsabile o al Titolare, il Sub-responsabile è tenuto a fornire l'elenco dei nominativi associati alle utenze che sono state rese disponibili dal Responsabile o dal Titolare.

j) Nel caso in cui il Sub-responsabile riceva istanze dagli interessati per l'esercizio dei diritti riconosciuti dalla normativa applicabile in materia di protezione dei dati personali dovrà:

- darne tempestiva comunicazione scritta al Responsabile allegando copia della richiesta;

- tenendo conto della natura del trattamento, assistere il Responsabile con misure tecniche e organizzative adeguate al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti degli interessati;

In particolare, ove applicabile e in considerazione delle attività di trattamento affidategli, il Sub-responsabile dovrà:

- permettere al Responsabile di fornire agli interessati i propri dati personali in un formato strutturato, di uso comune e leggibile da un dispositivo automatico, nonché di trasmettere i dati ad altro Responsabile;
- permettere al Responsabile di garantire in tutto o in parte i diritti di opposizione e limitazione del trattamento.

l) Il Sub-responsabile, su richiesta del Responsabile, coadiuva quest'ultimo nelle procedure davanti all'Autorità di Controllo competente e all'Autorità Giudiziaria in relazione alle attività rientranti nella sua competenza. Il Sub-responsabile comunica tempestivamente, senza indebito ritardo, ogni contatto o comunicazione ricevuta da un'Autorità di Controllo in relazione al Trattamento dei Dati Personali.

AUTORIZZAZIONE AL TRATTAMENTO DA PARTE DI SUB-RESPONSABILI

Col presente contratto, il Responsabile conferisce autorizzazione scritta generale al Sub-responsabile a poter ricorrere a eventuali ulteriori responsabili del trattamento ("Sub-responsabile/i") nella prestazione del servizio.

Nel caso in cui il Sub-responsabile faccia effettivo ricorso a ulteriori Sub-responsabili, il Sub-responsabile medesimo si impegna a selezionare ulteriori Sub-responsabili tra soggetti che per esperienza, capacità e affidabilità forniscano garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti di cui alla normativa pro tempore applicabile e garantisca la tutela dei diritti degli interessati. Il Sub-responsabile si impegna altresì a stipulare specifici contratti, o altri atti giuridici, con gli ulteriori Sub-responsabili a mezzo dei quali il Sub-responsabile descriva analiticamente i loro compiti e imponga a tali soggetti di rispettare i medesimi obblighi, con riferimento alla disciplina sulla protezione dei dati personali, imposti dal Responsabile sul Sub-responsabile ai sensi della normativa pro tempore vigente e degli applicabili provvedimenti speciali della competente Autorità di Controllo, prevedendo in particolare garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti della normativa applicabile e i provvedimenti emessi dall'Autorità di controllo.

Qualora gli ulteriori Sub-Responsabili omettano di adempiere ai propri obblighi in materia di protezione dei dati, il Sub-responsabile riconosce di conservare nei confronti del Responsabile l'intera responsabilità dell'adempimento degli obblighi degli ulteriori Sub-responsabili coinvolti, nonché si impegna a manlevare e tenere indenne il Responsabile da qualsiasi danno, pretesa, risarcimento, e/o sanzione possa derivare al Responsabile dalla mancata osservanza di tali obblighi e più in generale dalla violazione della applicabile normativa sulla tutela dei dati personali da parte del Sub-responsabile e dei suoi ulteriori sub-fornitori. Il Sub-responsabile si impegna altresì ad informare il Responsabile di eventuali modifiche o sostituzioni previste riguardanti gli ulteriori Sub-responsabili, dando così al Responsabile la possibilità di opporsi a tali modifiche. L'elenco dei Sub-responsabili ingaggiati è riportato **nell'Allegato 1.**

TRASFERIMENTO DATI PERSONALI

Il Sub-responsabile dovrà eseguire i trattamenti funzionali alle mansioni ad esso attribuite in relazione al Servizio o derivanti da istruzioni scritte del Responsabile, anche con riferimento all'eventuale trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale. Qualora sorgesse la necessità di trattamenti sui dati personali diversi ed eccezionali rispetto a quelli normalmente eseguiti, il Sub-responsabile dovrà informare preventivamente il Responsabile.

Laddove il Sub-responsabile intenda stipulare accordi con ulteriori Sub-responsabili stabiliti fuori dallo Spazio Economico Europeo, dovrà garantire che i trasferimenti dei dati avvengano previa comunicazione in tempo utile al Titolare, il quale avrà la possibilità di darne autorizzazione o di potersi opporre a tale modifica. L'eventuale trasferimento dei Dati Personali dovrà avvenire in conformità alle 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, chi si intendono qui interamente incorporate. 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".

OBBLIGHI IN TEMA DI COOPERAZIONE E RESPONSABILITÀ

Le Parti si impegnano a collaborare in buona fede per assicurare il rispetto delle previsioni di cui al presente Accordo TDP per conformarsi alle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali, tra cui, ma non solo, il dovere di assicurare il corretto e tempestivo esercizio dei diritti dell'Interessato, gestire incidenti di sicurezza/Violazioni dei Dati Personali al fine di mitigare i possibili effetti avversi da essi derivanti.

Le Parti collaborano in buona fede per rendere disponibile al Titolare del Trattamento, reciprocamente e verso l'Autorità di Controllo, le informazioni necessarie a dimostrare il rispetto delle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali.

VIOLAZIONE DEI DATI PERSONALI

Il Responsabile è consapevole e acconsente che il Sub-responsabile del trattamento non sarà ritenuto Responsabile in caso di Violazione dei dati personali che non sia imputabile a colpa di quest'ultimo.
Nel caso in cui il Sub-responsabile venga a conoscenza di una Violazione dei dati personali, dovrà adottare le misure tecniche e organizzative appropriate per contenere e mitigare tale Violazione dei Dati Personali.
Il Sub-responsabile si impegna ad informare il Responsabile entro e non oltre 24 (ventiquattro) ore dalla conoscenza di violazioni di dati personali e a fornire la più ampia collaborazione al Responsabile medesimo nonché alle Autorità di Controllo competenti e coinvolte al fine di soddisfare ogni applicabile obbligo imposto dalla normativa pro tempore applicabile (es. notifica della violazione dei dati personali all'Autorità Controllo compente; eventuale comunicazione di una violazione dei dati personali agli interessati).
Il Sub-responsabile, per quanto di competenza, tenuto conto delle attività di trattamento affidategli, assiste altresì il Responsabile nel garantire il rispetto degli obblighi relativi alla valutazione d'impatto sulla protezione dei dati nonché alla eventuale consultazione preventiva all'Autorità di Controllo.
Le parti definiscono nell'**Allegato 3** tutti gli elementi che devono essere forniti dal Sub-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 Sub-responsabile o del Servizio, il Sub-responsabile a discrezione del Responsabile sarà tenuto a: (i) restituire al Responsabile i dati personali oggetti del trattamento oppure (ii) 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.). In entrambi i casi il Sub-responsabile provvederà a rilasciare al Responsabile apposita dichiarazione per iscritto contenente l'attestazione che presso il Sub-responsabile non esista alcuna copia dei dati personali e delle informazioni di titolarità del Responsabile. Il Responsabile si riserva il diritto di effettuare controlli e verifiche volte ad accertare la veridicità della dichiarazione.
La presente nomina avrà efficacia fintanto che sia erogato il Servizio, salvi gli specifici obblighi che per loro natura sono destinati a permanere. Qualora il rapporto tra le parti venisse meno o perdesse efficacia per qualsiasi motivo o il Servizio non fosse più erogato, anche il presente contratto verrà automaticamente meno senza bisogno di comunicazioni o revoche, ed il Sub-responsabile non sarà più legittimato a trattare i dati del Responsabile.

DURATA E VALIDITÀ

Il presente Accordo TDP avrà la medesima durata del Contratto a cui si riferisce. Qualora questo venisse meno o perdesse efficacia e per qualsiasi motivo, anche il presente Accordo TDP verrà automaticamente meno, senza bisogno di comunicazioni o revoche, ed il Sub-responsabile non sarà più legittimato a trattare i dati personali, cessando lo status di Sub-responsabile.
Con il presente Accordo TDP, il Responsabile e il Sub-responsabile intendono espressamente revocare e sostituire ogni altra eventuale nomina e accordo tra le parti inerente al trattamento di dati personali.
Resta inteso che il presente contratto non comporta alcun diritto del Sub-responsabile ad uno specifico compenso e/o indennità e/o rimborso derivante dal medesimo.

COMUNICAZIONI TRA LE PARTI

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

- per il Responsabile del trattamento **REGGIO EMILIA.**- Reggio Emilia- **pec** comune.reggioemilia@cert.provincia.re.it
- per il Sub-Responsabile del Trattamento **MUNICIPIA SPA – TN - pec** municipia@pec.eng.it

SICUREZZA E PROTEZIONE DELLE INFORMAZIONI IN CLOUD SAAS (VALIDO SOLO PER L'EROGAZIONI DELLE SOLUZIONI IN CLOUD SAAS)

CONDIVISIONE DI RESPONSABILITA' PER LA SICUREZZA DELLE INFORMAZIONI

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

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

Si concorda che Cliente e Fornitore sono entrambi responsabili, ciascuno per le aree di propria competenza, che sono desumibili

contrattualmente.

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

PROTEZIONE DELLE INFORMAZIONI DEL CLIENTE NELL'AMBITO DEI SERVIZI CLOUD

GARANZIE

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

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

Si forniscono maggiori informazioni con particolare riferimento ai seguenti controlli:

Gestione delle vulnerabilità tecniche

Le vulnerabilità tecniche vengono gestite ciclicamente tramite un processo di individuazione strumentale delle vulnerabilità sugli asset (la frequenza è proporzionale al livello di esposizione degli asset stessi), gli input dei vendor e dei gruppi di interesse in contatto con i competence center tecnici oltre che da possibili inneschi provenienti da strumenti di monitoring o da segnalazioni utente.

La comunicazione ed il fixing delle vulnerabilità tecniche segue sempre un iter concordato tra le parti e da definire in fase di transition (change management) ed è comunque in funzione della gravità delle vulnerabilità stesse.

Hardening delle macchine virtuali

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

TRATTAMENTO DELLE INFORMAZIONI

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

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

Le informazioni risiedono:

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

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

DIFFUSIONE DELLE INFORMAZIONI

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

NOTIFICA DEGLI INCIDENTI

Il Fornitore, in armonia alla procedura di Gruppo per la gestione degli incidenti di tipo "data breach" si impegna a notificare

tempestivamente al Cliente gli incidenti di sicurezza informatica (data-breach) rilevati tramite strumenti di monitoraggio e controllo o da segnalazioni, che implichino o consistano in:

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

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

TRASFERIMENTO O RESTITUZIONE DELLE INFORMAZIONI O RIMOZIONE A FINE CONTRATTO

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

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

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

UTILIZZO DI SUB-FORNITORI

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

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

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

BACKUP E RESTORE

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

Il servizio di backup/restore è sempre dovuto dal Fornitore al Cliente tranne nei casi in cui, per natura del servizio o per esplicitazione contrattuale, è il Cliente stesso a provvedere autonomamente.

Il backup dei dati Cliente, qualora dovuto, viene garantito in duplice copia per tutti i dati. Eventuali deroghe richieste dal Cliente possono riguardare ambienti o dati "non di produzione". Originali e copie dei backup vengono conservati in locazioni (fisiche o logiche) differenti e il trasferimento dei dati in sede diversa avviene solo sotto protezione crittografica.

A meno di differenti accordi contrattuali, l'inizio dell'attività di restore dei dati in caso di incidente è sempre garantita, nel caso peggiore, nell'arco del giorno lavorativo successivo all'evento che rende necessario il ripristino. La durata complessiva dell'attività di restore è funzione del volume di dati da ripristinare.

LOGGING

La collezione e conservazione dei log a norma di legge è tipicamente effettuata dal Fornitore, sia direttamente, sia avvalendosi del servizio offerto dai propri sub-fornitori (IaaS e PaaS).

I log vengono resi disponibili al Cliente in forma di report "spot", effettuato su richiesta estemporanea del Cliente oppure, se concordato tra i servizi contrattualizzati, in forma di report periodico, o garantendo l'accesso in visione ai dati via rete. In tutti i casi viene garantita la riservatezza delle informazioni nel senso che ogni Cliente ha visibilità esclusivamente dei log relativi a sistemi/servizi di sua pertinenza.

PROPRIETÀ INTELLETTUALI

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

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

CAPITOLO 4

CONDIZIONI GENERALI DI VENDITA

Per quanto non espressamente previsto nel presente documento:

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

Allegato 1	**ELENCO SUB-RESPONSABILI** **MD14_PGT01_0_Allegato_Elenco_SubResponsabili**
Trattamento Dati	Assistenza e Manutenzione | Sviluppo Prodotto Prodotto: **jENTE** Erogazione: On Premises

Sezione Valida per l'erogazione delle soluzioni Municipia in SaaS
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.

Di seguito è riportato l'elenco dei sub-responsabili per le varie soluzioni Municipia.

Il trattamento oggetto del contratto è riferito al prodotto indicato sopra nella fascia arancione.

Paese cui è stabilito Sub-Responsabile	**Sub-Responsabili**	**Dati di contatto**	**Attività di trattamento affidata**	**Per il sub-responsabile indicato nella colonna sotto sono indicati i prodotti interessati.**
Italia	D-HUB Gruppo Engineering	info.dhub@eng.it	Service Provider (CSP qualificato AGID)	TRIBOX – GEIS – MERCURIO – GERI ARGO - GNOSIS
Lussemburgo	Amazon Web Services EMEA SARL	https://aws.amazon.com/it/contact-us/	Service Provider (CSP qualificato AGID)	JEnte – MUNIPAY – INES CLOUD

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**
Trattamento Dati	Assistenza e Manutenzione | Sviluppo Prodotto Prodotto: **jENTE** Erogazione: On Premises

Di seguito è riportato l'elenco delle varie soluzioni Municipia con l'indicazione delle caratteristiche del trattamento e le misure tecniche organizzative.

Il trattamento oggetto del contratto è riferito al prodotto indicato sopra nella fascia arancione.

ARGO è un Citizen Relation Management System, composto dai seguenti moduli:
- Front-End Cittadino: permette al cittadino la consultazione della propria situazione debitoria nei confronti dell'ente;
- Agenda: permette la gestione degli appuntamenti tra Cittadino ed Operatori preposti;
- Gestione Ticket: supporto al cittadino;

GEIS offre un supporto al comune per la riscossione e la gestione dell'imposta di soggiorno. Lato operatore fornisce un sistema per gestire le strutture, i gestori/rappresentanti legali, inserire dichiarazioni e versamenti, generazione di report. Lato gestore permette l'inserimento delle dichiarazioni e la gestione del bollettario elettronico.

TRIBOX è un Gestionale Tributi. È alimentato da fonti esterne eterogenee (catasto, demografici, SIATEL, 290, ecc), offre funzionalità puntuali e massive sulla situazione contributiva dei soggetti censiti nella banca dati dell'ente, relativamente ai tributi trattati.

GNOSIS è lo strumento software realizzato da Municipia a supporto del servizio di ricerca evasione TARI/IMU.

MERCURIO è uno strumento con funzione di spedizioniere. È in grado di recepire documenti da inviare attraverso diversi canali (export SIN, PEC, e-mail e notifiche AppIO. All'atto della spedizione è in grado di reperire informazioni PEC da Registro Imprese.

MUNIPAY è la soluzione di Municipia completa e modulare che supporta l'Ente nell'interazione con il mondo PagoPA.

JENTE jEnte in Cloud è la soluzione ERP rivolta all'Amministrazione locale e alle sue aziende. Semplice da usare, protetta e personalizzabile, è concepita per gestire, monitorare e razionalizzare tutti i processi connessi all'azione amministrativa secondo una visione sempre più orientata all'erogazione di servizi di qualità alla comunità.

INES CLOUD rappresenta la piattaforma per la gestione unificata della mobilità e della sosta urbana.

DETTAGLI DEL TRATTAMENTO

- Application Maintenance Management
- Customer Support
- Sviluppo Prodotto

CATEGORIE DI INTERESSATI

Categoria interessati	Prodotti
Cittadini e contribuenti	TUTTI I PRODOTTI
Clienti privati	INES Cloud
Dipendenti	JEnte
Minori	JEnte

TIPOLOGIA DI DATI PERSONALI

Dati Personali	Prodotti
Dati Personali Comuni (es. dati anagrafici, di contatto, relativi all'istruzione, stato civile/familiare, esperienza professionale)	TUTTI I PRODOTTI
Dati Finanziari (es. reddito, transazioni finanziarie, investimenti, carte di credito, fatture, ecc.)	TUTTI I PRODOTTI
Dati Particolari (es. sulla salute, genetici, biometrici, opinioni politiche, vita sessuale, ecc.)	JEnte / INES Cloud
Dati Giudiziari (es. dati relativi a condanne penali, ecc.)	JEnte / INES Cloud
Dati di Profilazione (es. dati di traffico telefonico, dati su preferenze personali ed abitudini, ecc.)	INES Cloud

CARATTERISTICHE DEL TRATTAMENTO

1. Full Outsourcing
   (per l'erogazione SaaS)

2. Traditional On-Premises IT - trattamento on site presso il Titolare con devices (laptop, desktop, ecc.) forniti dal Titolare/Cliente
   (per erogazione On-Premises)

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	Geis ARGO MuniPay	Tribox Gnosis Mercurio	JEnte INES Cloud
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.	X	X	X
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.	X	X	X
M	**Security Policy e procedure per la protezione dei dati personali**	**A.3**	L'organizzazione documenta una politica di sicurezza dedicata separata per quanto riguarda il trattamento dei dati personali. La politica approvata dalla Direzione e comunicata a tutti i dipendenti e alle parti esterne interessate.	N/A	X	X
M	**Security Policy e procedure per la protezione dei dati personali**	**A.4**	La politica di sicurezza fa riferimento a: i ruoli e le responsabilità del personale, le misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, per i responsabili del trattamento dei dati o	N/A	X	X

Risk Level	Categoria	ID	Descrizione	Geis ARGO MuniPay	Tribox Gnosis Mercurio	JEnte INES Cloud
			per le altre terze parti coinvolte nel trattamento dei dati personali.			
M	**Security Policy e procedure per la protezione dei dati personali**	**A.5**	È creato e mantenuto un inventario di politiche / procedure specifiche relative alla sicurezza dei dati personali, basato sulla politica generale di sicurezza.	N/A	X	X
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.	X	X	X
B	**Ruoli e responsabilità**	**B.2**	Durante le riorganizzazioni interne o le cessazioni e il cambio di impiego, sono chiaramente definite le modalità di revoca dei diritti e delle responsabilità con le rispettive procedure di passaggio di consegne.	X	X	X
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.	N/A	X	X
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.	N/A	N/A	X
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.	N/A	N/A	X
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.	X	X	X
M	**Policy per il controllo degli accessi**	**C.2**	Una politica di controllo degli accessi dettagliata e documentata. L'organizzazione dovrebbe determinare in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti nel contesto dei processi e delle procedure relative ai dati personali.	N/A	X	X
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.	N/A	X	X
A	**Policy per il controllo degli accessi**	**C.4**	I ruoli con diritti di accesso privilegiato sono chiaramente definiti e assegnati limitatamente a membri specifici dello staff.	N/A	N/A	X

Risk Level	Categoria	ID	Descrizione	Geis ARGO MuniPay	Tribox Gnosis Mercurio	JEnte INES Cloud
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).	X	X	X
B	**Gestione degli asset/risorse**	**D.2**	Le risorse IT sono riesaminate e aggiornate regolarmente.	X	X	X
M	**Gestione degli asset/risorse**	**D.3**	I ruoli che hanno accesso a determinate risorse sono definiti e documentati.	N/A	X	X
A	**Gestione degli asset/risorse**	**D.4**	Le risorse IT sono riesaminate e aggiornate su base annuale.	N/A	N/A	X
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.	X	X	X
B	**Gestione del cambiamento**	**E.2**	Lo sviluppo del software è eseguito in un ambiente speciale, non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire l test, sono utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non è possibile, sono previste procedure specifiche per la protezione dei dati personali utilizzati nei test.	X	X	X
M	**Gestione del cambiamento**	**E.3**	È presente una politica dettagliata e documentata di gestione dei cambiamenti. Dovrebbe includere: un processo per l'introduzione dei cambiamenti, i ruoli / utenti che hanno i diritti di cambiamento, le tempistiche per l'introduzione dei cambiamenti. La politica di gestione dei cambiamenti regolarmente aggiornata.	N/A	X	X
B	**Gestione degli incidenti / Data Breaches**	**G.2**	Le violazioni dei dati personali sono segnalate immediatamente alla Direzione. Sono in atto procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi dell'art. 33 e 34 GDPR.	X	X	X
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.	N/A	N/A	X
B	**Business Continuity**	**H.1**	L'organizzazione dovrebbe stabilire le procedure e i controlli principali da seguire al fine di garantire il livello richiesto di continuità e disponibilità del sistema informatico che elabora i dati personali (in caso di incidente / violazione dei dati personali).	X	X	X
M	**Business Continuity**	**H.2**	Un BCP dettagliato e documentato (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.	N/A	X	X

Risk Level	Categoria	ID	Descrizione	Geis ARGO MuniPay	Tribox Gnosis Mercurio	JEnte INES Cloud
M	**Business Continuity**	**H.3**	Un livello di qualità del servizio garantito definito nel BCP per i processi aziendali fondamentali che prevedono la sicurezza dei dati personali.	N/A	X	X
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.		N/A	X
B	**Riservatezza del personale**	**I.1**	L'organizzazione garantisce che tutto il personale comprenda le proprie responsabilità e gli obblighi relativi al trattamento dei dati personali. I ruoli e le responsabilità sono chiaramente comunicati durante il processo di pre-assunzione e / o inserimento.	X	X	X
M	**Riservatezza del personale**	**I.2**	Prima di assumere i propri compiti, il personale è invitato a riesaminare e concordare la politica di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione.	N/A	X	X
B	**Formazione**	**J.1**	L'organizzazione garantisce che tutto il personale sia adeguatamente informato sui controlli di sicurezza del sistema informatico relativi al suo lavoro quotidiano. Il personale coinvolto nel trattamento dei dati personali dovrebbe inoltre essere adeguatamente informato in merito ai requisiti in materia di protezione dei dati e agli obblighi legali attraverso regolari campagne di sensibilizzazione.	X	X	X
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.	N/A	X	X
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.	X	X	X
B	**Controllo degli accessi ed autenticazione**	**K.2**	L'uso di account generici (non personali) è evitato. Nei casi in cui ciò è necessario, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.	X	X	X
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.	X	X	X
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).	X	X	X
M	**Controllo degli accessi ed autenticazione**	**K.5**	Una politica specifica per la password è definita e documentata. La politica deve includere almeno la lunghezza della password, la complessità, il periodo di	N/A	X	X

Risk Level	Categoria	ID	Descrizione	Geis ARGO MuniPay	Tribox Gnosis Mercurio	JEnte INES Cloud
			validità e il numero di tentativi di accesso non riusciti accettabili.			
M	**Controllo degli accessi ed autenticazione**	**K.6**	Le password degli utenti sono archiviate in formato "hash".	N/A	X	X
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).	X	X	X
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.	X	X	X
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.	N/A	X	X
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.	N/A	X	X
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.	X	X	X
B	**Sicurezza desktop/laptop/mobile**	**N.2**	Le applicazioni anti-virus e le relative signatures sono configurate su base settimanale.	X	X	X
B	**Sicurezza desktop/laptop/mobile**	**N.4**	Il sistema dovrebbe avere timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.	X	X	X
B	**Sicurezza desktop/laptop/mobile**	**N.5**	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema sono installati regolarmente.	X	X	X
M	**Sicurezza desktop/laptop/mobile**	**N.6**	Le applicazioni antivirus e le signature sono configurate su base giornaliera.	N/A	X	X
B	**Network/Communication security**	**O.1**	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione è crittografata tramite protocolli crittografici (TLS / SSL).	X	X	X
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.	N/A	X	X
B	**Back-ups**	**P.1**	Le procedure di backup e ripristino dei dati sono definite, documentate e chiaramente collegate a ruoli e responsabilità.	X	X	X
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.	X	X	X
B	**Back-ups**	**P.3**	L'esecuzione dei backup monitorata per garantire la completezza.	X	X	X

Risk Level	Categoria	ID	Descrizione	Geis ARGO MuniPay	Tribox Gnosis Mercurio	JEnte INES Cloud
B	**Back-ups**	**P.4**	I backup completi sono eseguiti regolarmente.	X	X	X
M	**Back-ups**	**P.5**	I supporti di backup sono testati regolarmente per assicurarsi che possano essere utilizzati.	N/A	X	X
M	**Back-ups**	**P.6**	I backup incrementali programmati sono eseguiti almeno su base giornaliera.	N/A	X	X
M	**Back-ups**	**P.7**	Le copie del backup sono conservate in modo sicuro in luoghi diversi dai dati di origine.	N/A	X	X
B	**Sicurezza del ciclo di vita del software**	**R.4**	Sono seguiti standard e pratiche di codifica sicure.	X	X	X
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.	N/A	X	X
M	**Sicurezza del ciclo di vita del software**	**R.7**	Sono eseguiti penetration test periodici.	N/A	X	X
M	**Sicurezza del ciclo di vita del software**	**R.8**	Si ottengono informazioni sulle vulnerabilità tecniche dei sistemi IT utilizzati.	N/A	X	X
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.	N/A	X	X
B	**Sicurezza fisica**	**T.1**	Il perimetro fisico dell'infrastruttura IT non accessibile da personale non autorizzato.	X	X	X
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.	N/A	X	X
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	N/A	X	X
M	**Sicurezza fisica** (solo per Cloud SaaS)	**T.4**	I sistemi di rilevamento anti-intrusione sono installati in tutte le zone di sicurezza.	N/A	X	X
M	**Sicurezza fisica** (solo per Cloud SaaS)	**T.5**	Le barriere fisiche sono costruite per impedire l'accesso fisico non autorizzato.	N/A	X	X
M	**Sicurezza fisica** (solo per Cloud SaaS)	**T.6**	Le aree non usate sono fisicamente bloccate e periodicamente riesaminate.	N/A	X	X
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.	N/A	X	X
M	**Sicurezza fisica** (solo per Cloud SaaS)	**T.8**	Il personale di supporto esterno ha accesso limitato alle aree protette.	N/A	X	X

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)

_____

_____