SMART TECHNOLOGIES

Spett.le **FONDAZIONE PICCOLO TEATRO DI MILANO TEATRO D'EUROPA**
Via Rovello 2
20121 - MILANO (MI)

Magenta, 11 ottobre 2023
Rif. ID OPPORT. 42284B

OGGETTO: UPGRADE DEL SISTEMA INFORMATIVO DELL'ENTE ALLE WEB APP PRIVATE HYPERSIC 10 PER LA GESTIONE DEL PROTOCOLLO INFORMATICO IN CLOUD CON CSP APKAPPA QUALIFICATO ACN E CONSERVAZIONE DIGITALE A NORMA.

PROGETTO TECNICO E OFFERTA.

In relazione a quanto concordato con la vostra Amministrazione abbiamo il piacere di sottoporre alla vostra cortese attenzione la nostra migliore proposta tecnico ed economica per i prodotti e servizi richiesti ed in particolare la fornitura dei seguenti prodotti e servizi:

- **Web App private**
- Area Protocollo
- Area Conservazione
- **Conservazione Digitale a norma**
- **Cloud procedurale** (erogazione in saas) hyperSIC Cloud, come servizio SaaS (Software as a Service) qualificato ACN (Agenzia per la Cybersicurezza Nazionale) **hyperSIC Cloud**, erogato da APKAPPA tramite il servizio di Cloud computing **AWS (Amazon Web Services)** qualificato come servizio PaaS per il Cloud della PA
- **Migrazione dati protocollo da precedente software di PA DIGITALE**
- **Formazione e Supporto all'Avviamento**
- **Messa a disposizione dei nostri WS che verranno richiamati da Digital PA**

Certi di un favorevole accoglimento della presente comunicazione, l'occasione è gradita per porgere cordiali saluti.

APKAPPA srl
Il **Funzionario Commerciale**
Dr. Alessandro Viganò

FONDAZIONE PICCOLO TEATRO DI MILANO TEATRO D'EUROPA

Offerta Tecnico Economica

Commerciale di Riferimento
Dr. Alessandro Viganò

UPGRADE WEB APP HYPERSIC® 10

APKAPPA S.r.l.
sede operativa e amministrativa
via M.K.Gandhi, 24/A I-42123 **Reggio Emilia**
sede operativa via Milano 89/91 I-20013 **Magenta** (Mi)
sede legale via F.Albani, 21 I-20149 Milano

Tel. +39 02.91712.000
Fax +39 02.91712.339
apkappa@apkappa.it
(PEC) apkappa@legalmail.it
www.apkappa.it

Iscr. Reg. Impr. Milano
REA1232455
C.F. e P.IVA IT-08543640158
Reg.Produttori AEE
IT08020000002166

Capitale sociale
Euro 600.000,00 i.v.
Società soggetta all'attività
di direzione e coordinamento
di Maggioli S.p.A.

Sommario

hyperSic® 10

hyperSIC10 è una **Web APP**, progettata secondo il principio del *mobile first*, ovvero una applicazione mobile che può essere utilizzata su smartphone, tablet o personal computer attraverso un browser per la navigazione in internet, **senza nessuna componente applicativa installata sui device**. La **Web App in versione pubblica** è utilizzabile dai cittadini sui propri smartphone o tablet rendendo fruibile in tempo reale il contenuto ed i servizi messi a disposizione dall'Ente su dispositivi mobile.

Vantaggi di una WEB APP sono:

- Non necessita di installazione sul smartphone o tablet. Questo è un importante punto di forza per cui:
- Non necessita di aggiornamenti da parte dei cittadini
- Non necessita di un supporto (Help Desk) ai cittadini
- Disponibilità di nuovi servizi e contenuti in tempo reale
- Non occupa ulteriore memoria dello smartphone o tablet in esecuzione dell'applicazione
- Funziona su tutte le versioni di smartphone o tablet
- Bassi costi di sviluppo e di manutenzione.
- Unico ambiente e linguaggio di sviluppo.

Vantaggi di HyperSic®10:

- Integra nativamente il front-0ffice dei servizi online
- **Sviluppato in modalità *mobile first*** con design responsive che consente un automatico adattamento dei contenuti al device durante la navigazione
- Permette di **disporre di tutte le funzionalità operative di back-office su smartphone o tablet**
- Permette di disporre di una integrazione con funzionalità di terzi parti attraverso web service su smartphone o tablet
- Disponibilità immediata di ogni nuovo servizio attivato
- Integrazione nativa di servizi quali **SPID, CNS/CRS, Timbro Digitale, PagoPA**
- **Integrazione nativa con firma remota** da smartphone o tablet

Protocolli e standard

hyperSIC10® utilizza:

- architettura conforme allo standard SOA (Service Oriented Architetture)
- protocolli web standard come TCP/IP, HTTP/HTTPS per la trasmissione delle informazioni;
- protocollo standard LDAP per la consultazione dei servizi di directory;
- linguaggio standard ANSI SQL per l'interazione con l'RDBMS
- tecnologie WEB Service (XML, WDSL, etc) per la definizione e interscambio dei dati;
- formati PDF - PDF/A - Portable Document Format, .p7m per il formato dei documenti gestiti dal sistema;
- formati per i documenti informatici che si sottopongono a conservazione come:
  - PDF - PDF/A
  - JPEG con estensione .jp2
  - OOXML – Open Office XML conforme allo standard ISO/IEC 29500:2008
  - ODF – Open Document Format
  - eXtensible Markup Language Extensible Markup Language (XML). Su XML si basano numerosi linguaggi standard utilizzati nei più diversi ambiti applicativi. ad esempio:
    - SVG usato nella descrizione di immagini vettoriali
    - XBRL usato nella comunicazione di dati finanziari
    - ebXML usato nel commercio elettronico
    - SOAP utilizzato nello scambio dei messaggi tra Web Service

Rispetto delle linee guida di design per i servizi web della PA

La piattaforma hyperSIC10® rispetta le linee guida di design per i servizi web della PA indicati dall'Agenzia per l'Italia Digitale AgID e dal Team per la Trasformazione Digitale.

Rispetto normativa sulla privacy (Regolamento UE 2016/679)

La piattaforma applicativa hyperSIC10® prevede adeguati strumenti di sicurezza dell'accesso che garantiscono tutti i principi di sicurezza e di privacy, in conformità alle normative vigenti, primo fra tutte il **General Data Protection Regulation (GDPR)**; in particolare la sicurezza degli accessi è garantita attraverso un sistema di autenticazione informatica ed un sistema di autorizzazione e tracciabilità degli utenti gestiti in maniera centralizzata dal modulo Amministratore per tutti i moduli verticali della piattaforma, garantendo così l'accesso alle funzioni ed ai dati dei cittadini esclusivamente ai soggetti aventi le abilitazioni necessarie. Rispetta inoltre gli standard europei del Regolamento 2016/679.

Aderenza alle raccomandazioni del World Wide Web Consonrtium (W3C)

Per quanto riguarda l'accessibilità, le regole ed i principi adottati per la progettazione degli strati di presentazione di hyperSIC® si fondano sugli aspetti di accessibilità informatica, coerenti con la normativa nazionale ed internazionale vigente e in particolare in conformità alle raccomandazioni per l'accessibilità fornite da W3C Raccomandazioni del World Wide Web Consortium (W3C): HTTP 1.1, HTML 4.01 e CSS 2.0, XHTML 1.0, XML 1.0 e WAI.

Compatibilità browser

hyperSIC10® è compatibile con i più comuni browser, ad esempio: **Internet Explorer, Edge, Mozilla Firefox, Google Chrome in ambiente Microsoft Windows; Safari; Opera in ambiente Mac OS; Mozilla Firefox, Opera e browser nativo in ambiente Android**.

Compatibilità Sistemi Operativi

Il sistema proposto è indipendente dal sistema operativo e funziona su ambienti operativi server standard **OpenSource (Linux Distribution RedHat, Centos) e/o standard di mercato come MicrosoftTM (MS Windows Server)**.

Design Responsivo

hyperSIC10® è sviluppato in modalità ***mobile first*** con **design responsive** che consente un automatico adattamento dei contenuti al device utilizzato durante la navigazione e quindi consente l'utilizzo, senza perdita di funzionalità, sia da PC desktop, che da dispositivi mobili quali **smartphone e tablet rendendo inutile il ricorso ad applicazioni ad hoc per questi dispositivi**.

Accesso sicuro a pagine web secondo gli standard SSL/TSL

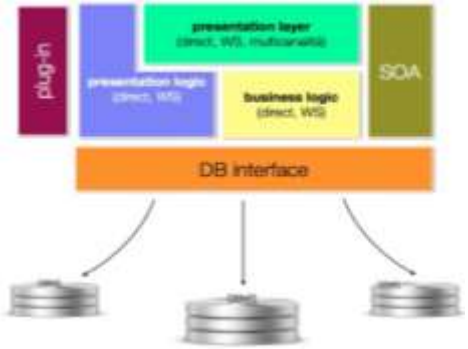
hyperSIC10® inoltre utilizza tecnologie che consentono di dotare tutte le risorse web di un canale sicuro e protetto creato dal protocollo HTTPS (protocollo HTTP che utilizza autenticazione e crittografazione del protocollo SSL/TLS per la costruzione delle connessioni), grazie all'impiego di certificati digitali. **hyperSIC10® sfrutta metodi di crittografazione al livello più elevato possibile di tutti i dati trattati in sede di scambio anche con altri sistemi, al fine di proteggere non solo sé stesso, ma anche la riservatezza delle informazioni trasmesse**. Anche la comunicazione tra webservices, oltre che essere completamente crittografata, è costituita quindi da servizi protetti, con accesso limitato e controllato.

Tecnologia e manutenibilità

Dal punto di vista tecnologico, hyperSIC10® è basata su tecnologie Open, in particolare è interamente realizzato in .NET e Java e utilizza i webservice come modalità standard di interoperabilità. Supporta soluzioni open source quali: Sistema Operativo Linux; Web Server Apache; Application Server Mono/Tomcat; RDBMS MySql/MariaDB; Browser Internet come Firefox e Chrome; Strumenti di produttività individuale quali Open Office e Libre Office e il Sistema di gestione della reportistica Jasper Reports. Il software applicativo proposto inoltre è stato realizzato rispettando le specifiche di controllo di qualità certificate, sulla produzione e sviluppo dello stesso, contenute nella Norma ISO 9126 e quindi anche la manutenibilità.

Modularità e scalabilità

La piattaforma applicativa hyperSIC10® si presenta con una struttura modulare, con un'unica interfaccia grafica ed unico DB dove i dati e le applicazioni sono pienamente e nativamente integrati. hyperSIC10® può essere visto come un sistema distribuito di processi, intercomunicanti tra loro. hyperSIC10® copre tutte le aree funzionali del Comune con moduli verticali specializzati per ciascuna di esse e, al tempo stesso, cooperanti tra loro per offrire sempre e comunque un ambiente produttivo unico ed informazioni univoche. I moduli verticali possono essere attivati anche in tempi diversi, in funzione delle esigenze di progetto.



La natura 3-Tier di hyperSIC10® permette un'elevata scalabilità: è infatti possibile la suddivisione in bilanciamento e ridondanza dei tre strati applicativi che consentono a loro volta l'organizzazione di Server Farms in forma "scalabile".

Questa caratteristica ha i seguenti due aspetti:

- Scalabilità Orizzontale intesa come capacità di aggiungere componenti hardware o software in grado di interagire con quelle già esistenti come un'unica entità logica
- Scalabilità Verticale intesa come capacità di aggiungere risorse alle componenti hardware o software già esistenti per il loro potenziamento.

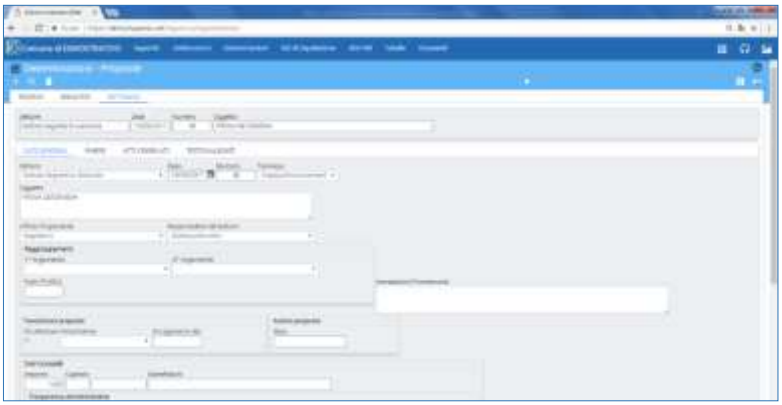
Usabilità e accessibilità

Uno degli obiettivi principali del progetto hyperSIC10® e quindi di tutti i moduli che costituiscono la suite, compresi quelli che costituiscono la proposta di questa offerta tecnica, **è fondato sulle caratteristiche di qualità per l'utilizzo da parte degli utenti, quindi usabilità ed accessibilità**. Al fine di garantire l'usabilità del sistema sono state effettuate specifiche scelte di progettazione, sia per quanto riguarda le caratteristiche di presentazione delle pagine che di realizzazione delle funzionalità, disponibili per l'esecuzione delle specifiche attività dell'utente. Ad esempio, è stata effettuata la scelta di standardizzazione delle pagine, sia per quanto riguarda l'utilizzo dei colori che la struttura, e quindi la disposizione nella pagina sia delle informazioni che dei comandi, che consentono una scelta immediata delle azioni necessarie al raggiungimento di quanto desiderato.

L'interfaccia utente inoltre garantisce:

- la comprensibilità, in quanto le informazioni i comandi presenti nell'interfaccia sono semplici da comprendere e da utilizzare;
- la consistenza e coerenza in quanto i tab e i pulsanti generali presenti nelle pagine hanno in tutto il sistema lo stesso significato;
- la facilità di apprendimento anche grazie alla presenza dell'Help in linea selezionabile su ciascuna scheda. Tale help è contestualizzato alla specifica funzionalità relativa alla maschera da cui viene attivato e consente la visualizzazione della **manualistica ipertestuale e di videocorsi** ove disponibili;
- la completezza funzionale, in quanto sono presenti tutte le operazioni necessarie per la realizzazione della funzionalità attivata;

- la flessibilità, in quanto è possibile personalizzare, attraverso il modulo Amministratore, i menù e i profili di utenza.



La presenza di un'interfaccia omogenea e standard per le Web App private, unita alla possibilità di gestire, tramite il CMS, templates per le pagine web delle Web App pubbliche, permette di garantire, anche in fase di modifica delle pagine e dei loro contenuti, livelli idonei di usabilità ed accessibilità.

Tutti i moduli applicativi di back office hyperSIC10® propongono un'interfaccia grafica che rispetta un unico standard grafico.

Cloud computing (oggetto di fornitura)- erogazione in saas dell'applicativo hyperSIC

La proposta prevede la fruizione, da parte del Comune di Luino della piattaforma applicativa hyperSIC Cloud, come servizio SaaS (Software as a Service) qualificato ACN (Agenzia per la Cybersicurezza Nazionale) hyperSIC Cloud, erogato da APKAPPA tramite il servizio di Cloud computing AWS (Amazon Web Services) qualificato come servizio PaaS per il Cloud della PA. Ciò consente all'Ente di avvalersi di servizi SaaS e Cloud in linea con le più stringenti regole sulla sicurezza, business continuity e disaster recovery imposte dalle linee guida e circolari AgID, direttive europee e Piano Triennale per l'Informatica nella PA e dal PNRR Piano Nazionale di Ripresa e Resilienza.

AWS è uno dei service provider con livelli e stabilità reale leader di mercato con una struttura standard dei Datacenter secondo Regions che è una composizione di >= 3 Datacenter separati da diverse decine di Km e totalmente ridondati in ogni loro parte, quindi già molto sicuri singolarmente e estremamente sicuri utilizzati in HA.

APKAPPA dopo un complesso processo ha ottenuto la Partnership AWS.

Saranno erogati i servizi tecnologici necessari alla definizione ed all'applicazione delle policy di sicurezza e al service management conformi ai modelli, alle metodologie e alle procedure definite da APKAPPA.

Il service management è costituito dai servizi di: monitoraggio delle risorse e capacity planning.

L'infrastruttura del CSP AWS per il servizio SaaS hyperSIC Cloud è composta da 2 Siti:

- Sito Primario in Italia presso Region Milan / eu-south-1 (Milano)
- Sito di Disaster Recovery presso Region Ireland / eu-west-1 (Dublino - Irlanda)

Oltre alla già collaudata architettura di servizio impiegata per tutti i Datacenter supportati (ad esempio quello di Magenta - CSP di tipo B), sono sfruttate le potenzialità messe a disposizione da Amazon AWS (Availability Zones, ecc.), per la costituzione di architetture in alta disponibilità e in sicurezza.

Il servizio proposto comprende tutti i servizi necessari e previsti per la qualificazione SaaS Cloud per la PA: ►attivazione, ►backup, ►recovery, ►service management (monitoraggio delle risorse e capacity planning), ►disattivazione entro i termini previsti, ►reversibilità per la restituzione dei dati.

a. Disponibilità del sistema ed elementi prestazionali

La piattaforma Cloud AWS garantisce SLA per servizio riportati al link AWS Service Level Agreements (SLAs), in particolare una disponibilità all'interno di una Region pari ad almeno il 99,99%.

Il servizio SaaS hyperSIC Cloud offerto, utilizzabile 24 ore al giorno per 365 giorni all'anno, salvo finestre di manutenzione concordata, garantisce una disponibilità del 99.5%.

Nell'ambito della soluzione di Disaster Recovery, descritta nel paragrafo che segue, sono garantiti valori di Recovery Time Objective - RPO massimo di 24 ore e Recovery Point Objective - RTO massimo di 3 ore.

hyperSIC Cloud necessita di una banda minima di circa 2Mbit/sec sia in upload che in download (preferibilmente con basse latenze); ogni valore superiore accelererà le fasi di carico e scarico di documenti ed allegati. In particolare per singolo client, per funzioni applicative, la banda di occupazione è di circa 1 KByte/s. Tale valore non è un valore costante ma Burst (di picco), hyperSIC Cloud in tecnologia Web non produce consumo costante ma di tipo request/response, minimizzando e rendendo efficiente l'uso di banda trasmissiva.

L'architettura web native della suite proposta e la scalabilità del servizio SaaS hyperSIC Cloud consente di supportare un numero illimitato di connessioni simultanee.

Per quanto riguarda il periodo di tempo in cui vengono mantenuti i backup (Periodo di Retention) si rimanda al paragrafo successivo.

b. Politiche di sicurezza adottate sull'infrastruttura

Ogni Datacenter AWS fornisce gli stessi livelli di qualità e sicurezza. I dati e le risorse utilizzate sono tutte crittografate a basso livello con chiavi di crittografazione note solo a APKAPPA. Questo garantisce livelli elevatissimi di sicurezza del dato, ovunque esso sia posizionato. Tutti gli ambienti su infrastruttura Amazon Web Service sono dedicati e gestiti totalmente da tecnici APKAPPA. Le attività di provisioning e deployment vengono eseguite automaticamente con tecnologie IaC (Infrastructure as Code), a garanzia di infrastrutture e servizi con caratteristiche di alta disponibilità e sicurezza. Sono mantenuti ambienti eseguiti all'interno di VPC (Amazon Virtual Private Cloud) dedicati, ogni ambiente: sviluppo, staging (pre-produzione), produzione è totalmente separato dagli altri. Il servizio SaaS hyperSIC.Cloud rispetta tutte le Best Practice di sicurezza e disponibilità suggerite dal fornitore Cloud. Il deployment è totalmente ridondato. La disponibilità dei dati a seguito di eventuale distruzione o danneggiamento dei dati stessi e/o degli strumenti elettronici utilizzati per il trattamento è garantita da opportune politiche di backup e disaster recovery contenute nelle specifiche procedure interne a norma ISO/IEC 27001:2013 di APKAPPA.

Le politiche di backup implementate garantiscono:

- un Backup Interval pari a 24 ore per i dati meno critici e 3 ore per i dati critici (DB incrementale).
- il Retention period definito come: ultimi 7 gg, ultime 4 settimane, ultimi 12 mesi, ultimo anno

Le tecnologie adottate e i piani di Disaster Recovery, di seguito DR, sono basate su repliche di tutte le componenti critiche, presso il sito secondario. L'architettura di DR e le tecnologie impiegate, consentono l'attivazione dei servizi protetti, presso il sito di Disaster Recovery, in tempi molto brevi e con operazioni automatizzate (IaC) e estremamente semplici. Grazie all'architettura impiegata, è possibile eseguire test di DR frequenti, senza alcun impatto sull'ambiente di produzione. Il piano di DR prevede soluzioni tecnologiche ed organizzative tali da permettere di continuare ad operare, nelle sue attività critiche, durante l'emergenza e fino al ritorno a condizioni di normalità.

Tutti i processi organizzativi e tecnologici, indispensabili per decidere e intervenire in caso di disastro, sono definiti in uno specifico piano di Disaster Recovery contenuto all'interno del Business Continuity Plan, sottoposti entrambi a certificazione di sicurezza, come il resto dei processi e dell'infrastruttura.

Sono assicurati nell'ambito della soluzione di DR, valori di RPO massimi di 24 ore e RTO massimo di 3 ore.

Le principali soluzioni previste per garantire i requisiti di sicurezza di hyperSIC Cloud sono di seguito riportate:

Controllo Accessi - hyperSIC Cloud prevede, sia per i moduli di back office che di front office, adeguati strumenti di sicurezza nell'accesso che garantiscono tutti i principi di sicurezza e di privacy, in conformità alle normative vigenti (GDPR). La sicurezza degli accessi è garantita attraverso un sistema di autenticazione informatica ed un sistema di autorizzazione e tracciabilità degli utenti gestiti in maniera centralizzata per tutti i moduli verticali della piattaforma, garantendo così l'accesso alle funzioni ed ai dati esclusivamente ai soggetti aventi le abilitazioni necessarie.

hyperSIC Cloud permette l'identificazione ed autenticazione univoca degli utenti con meccanismi semplificati come login (utente e password), integrabile in modo efficace con un sistema di autenticazione Active Directory, o con meccanismi più complessi quali l'identificazione tramite Sistema Pubblico di Identificazione Digitale (SPID), Carta d'Identità Elettronica CIE, Carta Nazionale dei Servizi CNS ed eIDAS.

Inoltre la piattaforma, al fine di aumentare il livello di sicurezza dell'accesso agli applicativi, implementa meccanismi di autenticazione a due livelli 2FA (two factor authentication).

Tracciabilità - hyperSIC Cloud dispone delle funzioni di registrazioni e tracciabilità delle attività effettuate attraverso la componente di logging, come descritto nel paragrafo § 2g, che consente di registrare in forma storica le operazioni svolte dagli utenti, anche in accordo alle misure di cui al Provvedimento del 27 novembre 2008 e s.m.i. del Garante della Privacy e al Regolamento UE 2016/679 GDPR.

Accesso sicuro a pagine web secondo gli standard SSL/TLS - hyperSIC Cloud utilizza tecnologie che consentono di dotare tutte le risorse web di un canale sicuro e protetto creato dal protocollo HTTPS grazie all'impiego di certificati digitali. Sfrutta metodi di crittografazione al livello più elevato possibile di tutti i dati trattati in sede di scambio anche con altri sistemi, al fine di proteggere non solo sé stesso, ma anche la riservatezza delle informazioni trasmesse secondo la normativa vigente (GDPR). Anche la comunicazione tra web services, oltre che essere completamente crittografata, è costituita quindi da servizi protetti, con accesso limitato e controllato.

Rispetto delle Misure minime di sicurezza ICT per le Pubbliche Amministrazioni e del GDPR - La suite hyperSIC Cloud di APKAPPA aderisce alle indicazioni della Circolare AgID n.2/2017 del 18 aprile 2017 in relazione alle «Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)», con un livello di attuazione superiore A. e garantisce inoltre il pieno rispetto di quanto previsto dal GDPR - Reg. UE 2016/679 e dalle disposizioni d'adeguamento contenute nel D.Lgs 2018/101.

Si riporta di seguito l'elenco delle principali misure adottate ed aderenti al GDPR: ►Sicurezza dei dati - la soluzione proposta, tramite l'infrastruttura applicativa, garantisce la disponibilità e l'integrità di tutti i dati nel caso in cui si verifichino errori, assicurando l'isolamento e limitando la propagazione delle anomalie nei diversi moduli applicativi; ►Gestione Utenti e accessi – come già indicato il sistema di autenticazione degli utenti a hyperSIC Cloud permette di integrarsi in modo efficace con un sistema di autenticazione Active Directory oppure di operare in autonomia. L'autenticazione degli utenti è prevista una sola volta, al momento dell'accesso all'applicazione. L'applicazione prevede funzionalità di tipo amministrativo, tali da consentire una profilazione centralizzata e granulare degli utenti. hyperSIC Cloud recepisce inoltre le indicazioni previste nella Circolare AgID n.2/2017 in relazione alla gestione delle credenziali; ►Cifratura dei dati - Il sistema hyperSIC Cloud adotta misure di sicurezza a protezione dei dati particolari quali la "pseudonimizzazione" che garantisce l'assenza di identificabilità diretta del soggetto interessato;

c. Metodologia di aggiornamento dell'infrastruttura di base

L'aggiornamento dell'infrastruttura di base è garantita dal Service Management previsto che è costituito dai servizi di Monitoraggio delle risorse e Capacity planning. I servizi di Service Management sono erogati così come previsto e documentato nel Sistema di Gestione della Qualità Aziendale ed in conformità a ISO/IEC 27001.

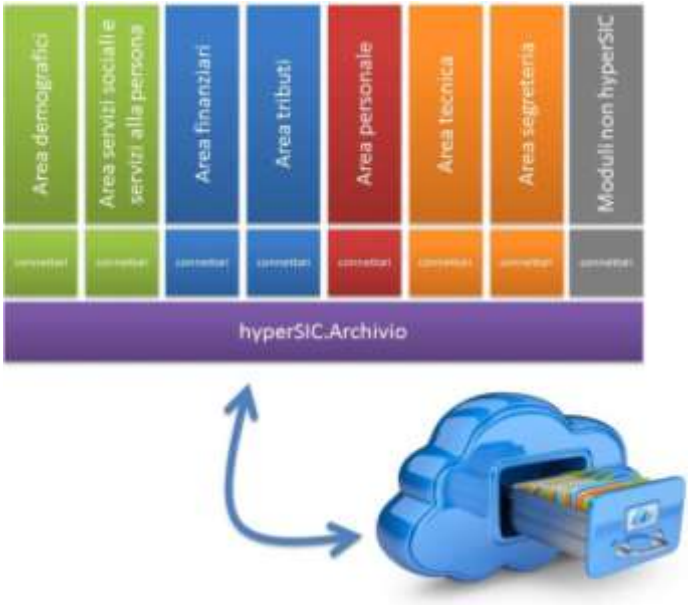
Monitoraggio delle risorse - Il monitoraggio delle risorse è effettuato in maniera automatica con differenti strumenti di monitoraggio e notifica di alert operanti sui diversi componenti della infrastruttura di erogazione del servizio e sul servizio stesso. In particolare il monitoraggio eseguito dal Cloud Team, avviene attraverso: ►consultazione interattiva di dati Real-Time e dati di Trend prodotti ed elaborati da opportuni strumenti di monitoraggio delle diverse componenti infrastrutturali quali ad esempio: utilizzo delle CPU, consumo di banda in ingresso e uscita, operazioni di scrittura/lettura su dischi, etc; ►meccanismi pro-attivi di Alert, nel caso di superamento di limiti stabiliti, prodotti dagli strumenti utilizzati e sulla base delle soglie impostate per le risorse (occupazione spazi, numero di processi, utilizzo delle risorse dell'infrastruttura utilizzo dei servizi, etc.); ►consultazione, manuale o a seguito di notifiche automatiche, dei log generati dai sistemi infrastrutturali;

Capacity planning - Il Capacity Planning è realizzato con l'analisi dei valori Real-Time resi disponibili dagli strumenti di monitoraggio utilizzati, ma soprattutto con quelli di Trend (report periodici). Almeno quadrimestralmente, in occasione delle rilevazioni periodiche ISO27001, sono prodotti e analizzati diversi report dei sistemi definiti nelle opportune checklist di verifica

Conservazione digitale a norma integrata con APKSer.Archivio (oggetto di fornitura)

Il servizio di conservazione a norma qui proposto è **APKSer.Archivio, servizio erogato e svolto direttamente da APKAPPA** srl, con le proprie strutture cloud, e con il quale ha ottenuto l'accreditamento ai sensi art. 44-bis D.Lgs. 82/2005 dall'Agenzia per l'Italia Digitale (i.e. AgID) come servizio del più elevato livello in termini di qualità e sicurezza.
Il valore aggiunto di utilizzare APKSer.Archivio è dato dal fatto che esso è anche nativamente interoperabile con la piattaforma applicativa hyperSIC® diversamente da altri sistemi di conservazione digitale seppur a norma; infatti esso consente all'utente di accedere sempre e comunque a qualsiasi documento gestito dal sistema, anche quando esso è conservato, direttamente dal proprio ambiente applicativo (i.e. dalla propria scrivania digitale). Si mantiene quindi l'accesso e la consultazione, tramite il proprio ambiente di lavoro, in cooperazione applicativa anche dopo l'avvio in conservazione dei documenti; tale opportunità supporta l'utente soprattutto in quei procedimenti il cui ciclo di vita è molto lungo ma dove alcuni documenti, per adempimenti normativi come le fatture elettroniche, devono comunque essere avviati in conservazione anche se non conclusi. L'utente hyperSIC® viene allertato che sta consultando un documento conservato ma non gli viene assolutamente inibito l'accesso o imposto un procedimento di accesso diverso da quello previsto per i documenti non ancora avviati in conservazione.
APKSer.Archivio mette a disposizione un servizio di conservazione del più elevato livello in termini di qualità e sicurezza, acquisisce i pacchetti di documenti informatici per via telematica, anche con canali di accesso protetti e privilegiati, e li conserva nel pieno rispetto delle regole tecniche stabilite dal DPCM 3/12/2013, dalle linee guida dell'Agenzia per l'Italia Digitale e dal codice per l'amministrazione digitale (D.Lgs. 82/2005 e s.m.i.).
Avvalersi di APKSer.ARCHIVIO è semplice: è possibile avviare in conservazione pacchetti di versamento con flussi telematici oppure in cooperazione applicativa con il back office hyperSIC. Grazie alla loro composizione, conforme alle regole tecniche attualmente in vigore, APKSer.Archivio li prende in carico e, dopo aver effettuato dei controlli preliminari, li inserisce in conservazione nello spazio dedicato al Cliente, gestendone da quel momento il processo nel tempo.
Con APKSer.Archivio il processo di esibizione viene soddisfatto in modalità semplice ed immediata grazie al collegamento autorizzato e sicuro via internet.
Il documento/fascicolo informatico, insieme ai suoi dati di registrazione e classificazione originari, affidato ad APKSer.ARCHIVIO per la sua conservazione preserva le sue caratteristiche di autenticita', integrita', affidabilita', leggibilita' e reperibilita' ed è protetto con misure di sicurezza conformi al D.Lgs. 196/2003 e ISO 27001:2013.

Per rendere ancor più proattiva l'attività di individuazione ed avvio in conservazione dei documenti/fascicoli informatici, l'utente hyperSIC® si avvale del modulo hyperSIC.Archivio grazie al quale viene supportato nell'individuare gli oggetti da conservare (tipicamente in base allo stato di conclusione dell'affare a cui si riferiscono, come previsto dalla sezione V del DPR 28 dicembre 2000 n. 445) per mezzo di funzioni di cooperazione applicativa con i moduli gestionali hyperSIC che li hanno prodotti o, ricorrendo all'uso di webservices, con moduli gestionali di altro produttore.



hyperSIC.Archivio assiste, inoltre, l'operatore nelle fasi di preparazione dei pacchetti di versamento, associandovi i metadati in accordo a quanto previsto dalle regole tecniche ed assicurando, attraverso una funzione a procedimento assistito, che allo stesso venga apposta la firma digitale ed il riferimento temporale UTC da parte del responsabile della conservazione dell'Ente prima che il pacchetto stesso venga versato nel sistema di conservazione APKSer.Archivio.

Con hyperSIC.Archivio è possibile impostare un procedimento che rispetti i seguenti passaggi:

- acquisizione automatica o manuale dei documenti da archiviare,
- creazione dei pacchetti di versamento,
- apposizione firma digitale e/o impronta,
- apposizione del riferimento temporale UTC,
- chiusura pacchetti di versamento,
- versamento pacchetti di versamento

Processo di Esibizione

Tramite hyperSIC.Archivio, l'utente può richiedere l'esibizione di un documento conservato accedendo all'opportuno servizio; in tal caso, diversamente dall'accesso in cooperazione applicativa, APKSer.Archivio restituisce in un pacchetto di esibizione, costituito in forma analoga a quello di versamento, il documento digitale conservato richiesto. Rimane in capo all'Ente consegnarlo al richiedente nella forma da esso richiesta (es. copia conforme analogica all'originale digitale conservato).

Cruscotto di monitoraggio

hyperSIC.Archivio offre al responsabile della conservazione un ambiente di monitoraggio grazie al quale può tenere sotto controllo varie informazioni legate all'archivio conservato, alla sua conservazione ed alle quote di occupazione nel sistema.

Assistenza telefonica e supporto

La qualità del servizio offerto ai propri cittadini dalla PAL è direttamente proporzionale alla qualità del proprio sistema informativo, vale la pena pertanto soffermarsi sulle caratteristiche importanti che una suite applicativa deve avere:

- Aggiornamenti normativi, migliorativi e di sicurezza tempestivi
- Automatismi per facilitare il lavoro quotidiano
- Estrema facilità di attivazione e utilizzo
- Percorsi formativi completi
- **Assistenza tecnica e normativa**

Desideriamo mettere l'accento proprio su questo ultimo aspetto il quale, per esperienza, riteniamo fondamentale per far si che tutto il resto funzioni alla perfezione.

Una **squadra di oltre 50 professionisti, costantemente aggiornati e verticalizzati su aree tematiche** come la Finanziaria, Demografici, Tributi, Affari Generali, Ufficio Tecnico, ecc… sono a vostra disposizione negli orari d'ufficio per risolvere problematiche tecniche e normative legate all'utilizzo delle Web App. Potrete raggiungere i tecnici, chiamando direttamente il centralino di APKAPPA o aprendo una segnalazione (ticket) direttamente dalla procedura o dal sito internet e **lo specialista più competente in materia vi ricontatterà nel giro di breve per risolvere la problematica** sottoposta.

Oltre ai normali format APKAPPA ha realizzato una **piattaforma di e-learning** nella quale in modo organizzato potrete trovare brevi video che vi guideranno nelle pratiche, magari quelle che si fanno più di rado, raggiungendo in modo semplice e veloce il vostro obiettivo.

Riteniamo **l'Help Desk una componente molto importante di una Web App** tecnologica, pratica e snella che permette agli operatori di lavorare in completa serenità e sicuri di raggiungere obiettivi e i più elevati standard di operatività richiesti dalle moderne Pubbliche Amministrazioni.

Formazione e avviamento sistema informativo

La formazione riveste un ruolo importante all'interno di questo cambiamento per questo motivo siamo a proporvi un percorso formativo di alto livello tramite tutti i più moderni strumenti tecnologici.

APKAPPA a seconda delle esigenze formative e operative dei responsabili e dipendenti dell'Ente è in grado di studiare una piano che può comprendere

- Giornate di formazione e/o consulenza in loco
- Sessioni formazione e/o consulenza tramite strumenti interattivi Webinar©
- Corsi normativi, formativi e operativi sulla nostra piattaforma di FAD (Formazione a Distanza) disponibili 24 ore su 24 e 365 giorni all'anno.

Nel caso di specie siamo a proporvi un piano operativo così strutturato, che naturalmente potrà essere ampliato in funzione delle vostre esigenze:

- Installazione, attivazione, parametrizzazione
- conversione dati da PA DIGITALE
- **3 gg on site** di formazione per protocollo, atti, conservazione
- **2 pacchetti da 10 ore via web** di formazione
- **Test ws con DIGITAL PA**

Le sessioni formative saranno effettuate in funzione dell'esigenza dell'ente ON SITE e VIA WEB.

Oltre a queste sessioni sarà messa a vostra disposizione tutta la nostra biblioteca multimediale per la formazione a distanza che completa il progetto con nozioni normative e gestionali.

Riteniamo che **4 GIORNATE ON SITE** e 2 pacchetti da **10 ORE VIA WEB** di formazione siano sufficienti per un ottimo startup completo del sistema per la gestione informatica dell'Ente ma riteniamo altresì indispensabile una fattiva collaborazione da parte del protagonista del cambiamento ovvero il personale dipendente della vostra amministrazione.

Per ulteriori giornate di formazione eventualmente ritenute necessarie per l'ente il prezzo A VOI RISERVATO sarà di

600,00€ + IVA per interventi ON SITE

550,00€ + IVA per pacchetti da 10 ore VIA WEB (fatturazione oraria- ovvero 50,00 €/ora)

Conversione degli archivi

APKAPPA vanta una esperienza ultra trentennale sulle conversioni di basi dati e nei fatti riteniamo di vitale importanza questo passaggio.

Al fine di rendere l'attività quanto più indolore vi informiamo che per una corretta trasposizione dei dati dal vostro attuale sistema Datamanagement alla nuova piattaforma HyperSic10 è indispensabile avere gli archivi in formato elettronico, leggibile (non criptato e non protetto da password) e una **fattiva collaborazione da parte di tutti i dipendenti e responsabili coinvolti**.

Nel dettaglio APKAPPA trasmigrerà i dati con conversione i seguenti dati:

PROTOCOLLO:

- La fattibilità è subordinata alla consegna dei dati in formato leggibile: DB non criptato o protetto da password (o esportazione analoga) documentato da apposito dizionario dati. Di ogni archivio saranno convertiti i dati identificabili presenti nelle procedure. Recupero archivi attualmente presenti relativamente ai dati di "segnatura dell'atto" (numero, data, interlocutore ed oggetto), destinatario interno (settore, ufficio, persona), classificazione ed altri dati descrittivi presenti in origine.

Costi e investimenti

Di seguito riportiamo i prezzi di fornitura dei prodotti e servizi offerti.

Quadro Economico

SERVIZIO	PREZZO
Servizio SaaS Cloud del software APKAPPA per le aree di protocollo fino al **31/12/2024 max 800 GB** **(ovvero canone biennale SAAS comprensivo di canone cloud + assistenza telefonica+ manutenzione continuativa)** • assessment, pianificazione, esecuzione. • trasferimento patrimonio informativo (dati e documenti) • licenze d'uso SAAS hyperSIC aree **back office** di: - **protocollo,** - **conservazione,** *dal 1/1/2025 il canone annuo SAAS (assistenza, manutenzione, cloud) per 800 GB sarà pari a 3.500,00	**€ 3.500,00*+ IVA******
Sigillo elettronico (attivazione e canone annuale)* *dal 1/1/2025 il canone annuale sarà pari a 100,00 euro/anno	**€ 200,00*+ IVA***
• Attivazione ambiente conservazione (avviamento) • Conservazione digitale a norma **(SPAZIO 10 GB)** fino al **31/12/2024** *dal 1/1/2025 il canone annuo per la conservazione digitale sarà pari a 890,00 euro/anno + iva	**€ 1.000,00*+ IVA****
Conversione dati protocollo da **PA DIGITALE nella seguente modalità: conversione di tutti i dati forniti, conversione degli allegati SOLO DELL'ULTIMO ANNO (2023)**	**€ 1.000,00*+ IVA***
Test dei WS con DIGITAL PA* ***Messa a disposizione dei WS di APKAPPA che verranno richiamati da Digital PA**	**€ 550,00*+ IVA***
Formazione: • 3 giornate ON SITE (600,00 euro + iva cadauna) • 2 pacchetti da 10 ore web (550,00 euro + iva per ogni pacchetto da 10 ore web)	**€ 2.900,00 *+ IVA***
TOTALE FORNITURA	**€ 9.150,00 *+ IVA***
Dal 1/1/2025 i canoni (SAAS + Sigillo Elettronico +Conservazione) saranno pari a:	**€ 4.490,00 *+ IVA***

Condizioni generali di fornitura

Evasione Ordini	***60 giorni dall'ordine formale di acquisto***
Consegna Software e garanzia collegamenti	*Secondo un piano concordato con l'ente.*
Sessioni formative	*Le giornate di formazione come le sessioni formative saranno pianificate secondo le esigenze di attivazione delle procedure*
IVA	*I prezzi su esposti si intendono al netto dell'IVA in vigore alla data della fatturazione.*
Fatturazione	*Il pagamento a mezzo mandato a 30gg fm df.*

Garanzia Software

APKAPPA S.r.l. garantisce il software applicativo per un periodo di dodici mesi dalla data di consegna o installazione. In tale periodo APKAPPA si impegna a rimuovere o correggere gratuitamente eventuali malfunzionamenti che gli fossero segnalati per iscritto dall'utente.

Per malfunzionamenti si intendono errori o anomalie di funzionamento riproducibili e che non dipendano da malfunzionamenti dell'hardware, del software di base o comunque da problemi esterni al software applicativo. Eventuali limitazioni o casi particolari non previsti dai programmi non possono considerarsi malfunzionamenti. APKAPPA non sarà tenuto a rispondere di problemi dovuti a manomissioni, negligenze o cattivo uso dei Sistemi Software.

Licenza d'Uso

Tutti i programmi forniti dallo APKAPPA oggetto dell'offerta sono erogati in modalità saas dal nostro CSP qualificato AGID.
Al termine del servizio i dati dell'ente vengono riconsegnati su supporto fisico.

MARCHI E DEPOSITI

Si fa presente che hyperSIC® e APKAPPA® sono marchi registrati presso l'Ufficio Italiano Marchi e Brevetti del Ministero dello Sviluppo Economico:
hyperSIC10, attestazione di registrazione n. 0001507309
APKAPPA, attestazione di registrazione n. 0001404561
Il codice sorgente dell'intera suite hyperSIC10® è depositato presso il Registro Pubblico Speciale per i Programmi ed Elaboratori tenuto dal SIAE, n. progressivo 008289 ordinativo D007487.

CLAUSOLA DI RISERVATEZZA dell'offerta tecnica

Questo documento non può essere utilizzato in qualsiasi forma in tutto o in parte, per scopi diversi da quelli per i quali è stato prodotto. In caso di violazione della presente clausola, APKAPPA tutelerà i propri diritti in termini di legge in sede civile e/o penale.

Validità dell'Offerta

La proposta in oggetto ha validità di 30 giorni dalla data di emissione.

OFFERTA N. /2023
FONDAZIONE PICCOLO TEATRO DI MILANO TEATRO D'EUROPA
NOMINA A RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI PERSONALI EX ART. 28 REGOLAMENTO (UE) 2016/679 (DI SEGUITO, IL "REGOLAMENTO")

In virtù del rapporto in essere, il Titolare del trattamento dei dati personali (di seguito, il "Titolare") ai sensi dell'articolo 4, par. 1, n. 7 del Regolamento, nomina APKAPPA S.r.l. quale Responsabile del trattamento dei dati personali (di seguito, il "Responsabile") ai sensi degli articoli 4, par. 1, n. 8 e 28 del Regolamento in relazione ai trattamenti effettuati e per le finalità del trattamento relative all'erogazione dei servizi in esecuzione e secondo le diverse modalità definite nel contratto.
Per quanto riguarda i trattamenti dei dati personali (anche particolari) effettuati per conto del Titolare, per le attività inerenti l'adempimento delle obbligazioni assunte, APKAPPA deve attenersi, in qualità di Responsabile ed in relazione a ogni aspetto disciplinato dal Regolamento, alle finalità, modalità e requisiti di sicurezza, alle istruzioni di seguito enunciate.
Con la sottoscrizione del presente atto, il Responsabile accetta la nomina e si dichiara disponibile e competente alla piena attuazione di quanto nella stessa previsto.
Il Responsabile si doterà di una procedura per i casi di violazione dei dati personali e provvederà a darne opportuna comunicazione al Titolare secondo quanto espressamente previsto all'articolo 33, par. 2, del Regolamento.
I servizi erogati da APKAPPA possono essere così brevemente riassunti:

1) Licenza d'uso, assistenza, servizi di outsourcing e manutenzione di applicazioni licenziate da APKAPPA installate sui sistemi informativi del Titolare (di seguito, le "Applicazioni").
2) Servizi di assistenza, servizi di outsourcing e manutenzione di applicazioni erogate da APKAPPA in cloud computing.
3) Servizio di conservazione digitale dei documenti informatici.

Nell'esecuzione del rapporto in essere, qualora la fornitura del servizio riguardi le attività di cui al punto 1 APKAPPA S.r.l. potrà accedere ai dati di soggetti terzi (quali ad esempio i dati personali degli utenti dei servizi) trattati dal Titolare tramite le Applicazioni con le seguenti modalità:

a) accesso ai Sistemi con privilegi idonei all'effettuazione dell'intervento mediante rete interna o connessioni protette, sotto la supervisione del Responsabile dei Sistemi Informativi o Amministratori di Sistema del Titolare;
b) intervento tecnico (a seconda dei casi installazione, aggiornamento, parametrizzazione, personalizzazioni dell'applicazione ecc.);
c) chiusura della sessione di lavoro sui Sistemi con contestuale comunicazione di fine intervento al Responsabile dei Sistemi Informativi o Amministratori di Sistema del Titolare.

Resta inteso che, nell'ambito delle attività di cui al punto 1:

a) l'intervento tecnico non prevede l'assegnazione di credenziali ad uso esclusivo ai tecnici di APKAPPA S.r.l.
b) gli incaricati di APKAPPA S.r.l. rispetteranno le misure tecniche e organizzative comunicate dal Titolare per garantire un livello di sicurezza adeguato ai sensi dell'articolo 32 del Regolamento;
c) gli incaricati di APKAPPA S.r.l. sono tenuti alla riservatezza nell'esecuzione dell'intervento e tale obbligo perdura anche successivamente allo svolgimento dello stesso;
d) l'incaricato di APKAPPA S.r.l. indicherà nel modulo in uso la descrizione dell'attività effettuata.

Qualora l'esecuzione del contratto riguardi le attività di cui al punto 2 e/o 3 APKAPPA S.r.l., in relazione all'attuazione del Provvedimento Generale del Garante del 27 novembre 2008 e s.m.i., relativo alla figura

professionale dell'Amministratore di Sistema, conferma di essersi adeguata al predetto provvedimento e di aver proceduto, tra l'altro, a:

- conservare direttamente e specificamente, gli estremi identificativi delle persone fisiche preposte quali Amministratori di Sistema che dovranno essere comunicati al Titolare;
- svolgere inoltre attività di verifica, con cadenza almeno annuale, sul loro operato anche attraverso la gestione, in conformità al richiamato Provvedimento, di un access log;
- provvedere all'osservanza di quanto stabilito dal Provvedimento del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" (G.U. n. 300 del 24 dicembre 2008) e successive modifiche, emesso dall'Autorità Garante per la protezione dei dati personali. In particolare dovrà garantire l'adozione delle misure tecniche e organizzative prescritte dal sopracitato provvedimento.
- In ogni caso APKAPPA S.r.l. dovrà conformarsi alle seguenti istruzioni:
- per quanto di sua competenza, garantire che i trattamenti svolti dai suoi incaricati avvengano nel rispetto delle norme del Regolamento e della normativa di attuazione;
- informare immediatamente il Titolare qualora, a suo parere, un'istruzione ricevuta dal Titolare violi il Regolamento o altre disposizioni relative alla protezione dei dati;
- comunicare prontamente al Titolare il verificarsi di situazioni anomale o di emergenza in relazione ai Sistemi, che possano comportare una violazione di dati personali in termini di perdita di integrità, disponibilità o riservatezza.

Il Responsabile si impegna a trattare i dati personali del Titolare solo per le finalità strettamente necessarie all'esecuzione del Contratto, e in conformità alle istruzioni ricevute per iscritto dal Titolare e nel rispetto di ogni obbligo di legge. Sarà espressamente vietato al Responsabile, e ai soggetti che con esso eventualmente collaborano, divulgare, ovvero utilizzare in qualsiasi altro modo, dati personali di terzi dei quali sia venuto a conoscenza nello svolgimento del proprio incarico, al di fuori delle indicazioni espressamente riportate nella presente nomina o successivamente ricevute dal Titolare.

Il Responsabile avviserà immediatamente, e comunque entro 48 ore, il Titolare di ogni richiesta, ordine o attività di controllo di cui venga fatto oggetto da parte del Garante, dell'Autorità Giudiziaria o di altra Pubblica Autorità. Il Responsabile, fin d'ora si impegna a eseguire senza ritardo quanto disposto dal Garante, dall'Autorità Giudiziaria o da altra Pubblica Autorità, con il supporto del Titolare.

Il Titolare avrà diritto di richiedere supporto al Responsabile per qualunque istanza formulata nei suoi confronti, ai sensi degli artt. 15, 16, 17, 18, 19, 20, 21, 22 del Regolamento, da parte degli interessati delle operazioni di trattamento connesse all'esecuzione del Contratto di cui in premessa. Il Responsabile non gestirà direttamente richieste provenienti dagli interessati ma ne darà notizia al Titolare ogniqualvolta riceva una richiesta di esercizio dei diritti.

Nel caso in cui il Responsabile si avvalga di terzi sub-appaltatori o sub-fornitori nella prestazione dei servizi forniti al Titolare, quest'ultimo concede ora per allora al Responsabile ex articolo 28, par. 2, del Regolamento il consenso generale alla nomina di tali soggetti quali sub-responsabili del trattamento dei dati personali trattati dal Responsabile nell'esecuzione del contratto, secondo quanto previsto dall'articolo 28, par. 4, del Regolamento e alle condizioni che seguono.

Nel caso in cui il Responsabile ricorresse a un altro soggetto per l'esecuzione di specifiche attività di trattamento per conto del Titolare, sarà tenuto ad imporre su tale altro Responsabile del trattamento, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nella presente nomina, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento.

Il Responsabile dovrà, altresì, comunicare al Titolare l'avvenuta nomina del sub-responsabile. Qualora l'altro Responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi dell'altro Responsabile.
APKAPPA tratterà e conserverà i dati per il periodo necessario al fine di adempiere agli obblighi e perseguire le finalità relative al Contratto, e comunque per un periodo non superiore a quello della durata del Contratto e sue eventuali estensioni e proroghe. Successivamente consegnerà i dati al Cliente secondo quanto previsto all'interno del sopracitato contratto, salvo la necessità di conservare copia dei dati ora detti per ragioni di natura normativa, regolamentare o giudiziale. Inoltre APKAPPA sarà autorizzata a trattare i dati per conto del Titolare – anche ai fini dell'erogazione del servizio - nel periodo intercorrente tra la cessazione di un Contratto e le conseguenti attività di migrazione, per un periodo non superiore a 12 mesi dalla cessazione degli effetti del Contratto.

La presente nomina non è a titolo oneroso e si intenderà revocata all'atto dello scioglimento del Contratto in essere tra le parti, per qualsiasi causa ciò avvenga.
Il Titolare potrà compiere ai sensi dell'articolo 28, par. 3, lettera h) del Regolamento verifiche periodiche sull'adempimento da parte del Responsabile di quanto sopra previsto, secondo modalità e costi che verranno concordati tra le parti. Tali verifiche potranno tuttavia essere condotte solo nei normali orari di ufficio, con preavviso di almeno 20 (venti) giorni lavorativi e potranno avere ad oggetto i soli documenti non confidenziali necessari a verificare il rispetto da parte del Responsabile delle istruzioni qui impartite.
Il Responsabile si impegna ad adottare e implementare le misure tecniche e organizzative di sicurezza (di seguito, le "Misure") che – ai sensi dell'art. 32 RGPD siano adeguate a eliminare o comunque a ridurre al minimo qualsiasi rischio di distruzione o perdita, anche accidentale dei dati trattati, di accesso non autorizzato o di trattamento non consentito o non conforme, con l'obbligo di documentarle se richiesto dal Titolare.
In base all'attività svolta dal Responsabile, varranno le Misure di seguito elencate.

Per le Applicazioni installate sui sistemi informativi del Titolare di cui al punto 1, APKAPPA in conformità all'Art. 32 del Regolamento, e nel rispetto dei principi Privacy by Design e Privacy by Default, adotta le seguenti misure tecniche ed organizzative:

- Sistema di autenticazione
- sistema anti malware
- firewall
- sicurezza perimetrale

Per le Applicazioni installate sui sistemi informativi del Responsabile di cui al punto 2 e/o 3, lo stesso, in conformità all'Art. 32 del Regolamento, e nel rispetto dei principi Privacy by Design e Privacy by Default, adotta le seguenti misure tecniche ed organizzative articolate sui tre livelli:

1) LIVELLO 1: Sistema di autenticazione, sistema anti malware, firewall e sicurezza perimetrale;
2) LIVELLO 2: Cifratura completa dei protocolli per l'accesso alle applicazioni e delle credenziali;
3) LIVELLO 3: Sistema AUDIT TRAIL per la gestione dei log sia di sistema che applicativi.

Per ulteriori specifiche relative all'attività di cui al punto 3) si rimanda al manuale di conservazione così come pubblicato sul sito dell'AGID essendo APKAPPA un conservatore accreditato.

Le parti stabiliscono che i referenti per l'esecuzione della Nomina sono:

Per il Responsabile del Trattamento: email: ufficio.privacy@apkappa.it, tel. 02 94454.000.
Qualsiasi modifica relativa le sopra menzionate persone o la responsabilità delle persone di contatto deve essere immediatamente notificata all'altra parte.

lì, 11/10/2023

APKAPPA SRL
Il Responsabile del Trattamento

Il TITOLARE