

## Allegato 13 – Piano per la sicurezza informatica

Il Comune adotta la soluzione software di Gestione Protocollo e Documentale “hyperSIC Cloud” della società APKAPPA srl in modalità SaaS su piattaforma Cloud Service Provider Amazon Web Services, denominata AWS, così come qualificata nel Marketplace ACN <https://www.acn.gov.it/portale/w/sa-1740>.

Sotto il profilo della normativa in materia di protezione dei dati personali, si rileva che APKAPPA tratta i dati di cui il Comune è titolare in qualità di responsabile del trattamento e Amazon Web Services è stata nominata da APKAPPA quale sub-responsabile al trattamento dei dati, come previsto dall'art. 28 paragrafo 4 del Regolamento UE 679/2016 (GDPR).

In relazione ai profili relativi alla protezione dei dati personali, si forniscono le seguenti informazioni.

### **1. Localizzazione Data Center AWS**

L'Infrastruttura Globale di AWS offre la flessibilità per scegliere come e dove eseguire i carichi di lavoro, consentendo al cliente di scegliere la localizzazione dei dati.

APKAPPA ha scelto nelle configurazioni di AWS la Regione Italia - Milano come Data Center primario e la Regione Irlanda - Dublino e Germania - Francoforte come Data Center secondario, da utilizzarsi in caso di attivazione delle procedure di *disaster recovery*.

I dati non sono trasferiti o replicati al di fuori delle Regioni AWS scelte senza il consenso del cliente, salvo che ciò sia richiesto per legge o come conseguenza di un ordine vincolante da parte di un ente governativo.

La titolarità dei dati rimane in capo al cliente.

AWS, nella fornitura dei propri servizi, non accede né utilizza i contenuti dei Titolari per alcun motivo senza il loro consenso. Inoltre, AWS non utilizza i contenuti del Titolare né eventuali informazioni derivate per finalità differenti da quelle relative all'esecuzione del contratto, con esplicita esclusione di qualunque utilizzo per finalità pubblicitarie o di marketing.

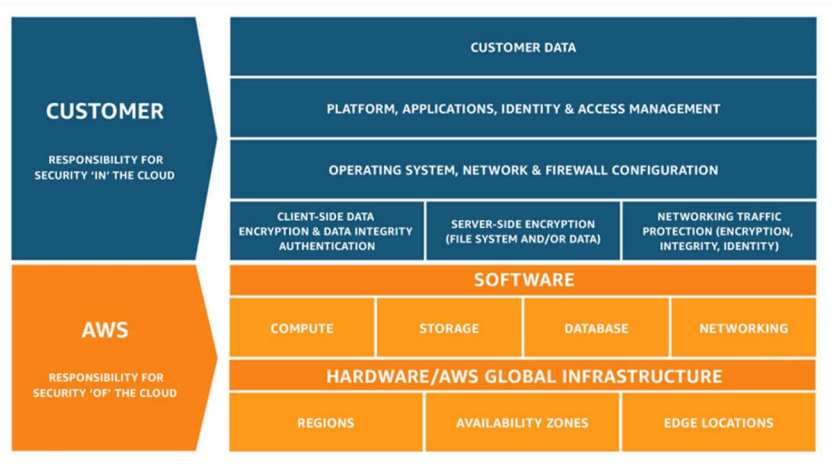
### **2. Sicurezza dei dati su piattaforma AWS**

Per quanto concerne il profilo della sicurezza, la soluzione in oggetto consente una integrazione tra le misure di sicurezza poste in essere dalla Società e quelle approntate da AWS, nel pieno rispetto della normativa applicabile e, in particolare, del dettato di cui all'art. 32 GDPR. Al riguardo, si segnala che AWS aziona, gestisce e controlla i componenti del sistema operativo host e il livello di virtualizzazione nonché gli aspetti relativi alla sicurezza fisica delle strutture in cui il servizio risiede. APKAPPA, che opera come responsabile esterno al trattamento dei dati per i propri clienti, si assume la responsabilità e la gestione del sistema operativo guest (inclusi gli aggiornamenti e le patch di sicurezza), di altro software applicativo nonché della configurazione del firewall del gruppo di sicurezza fornito da AWS.

In base al modello di responsabilità condivisa, AWS è responsabile della sicurezza dell'infrastruttura sottostante che supporta i servizi AWS (**Sicurezza DEL cloud**) e APKAPPA, in qualità di responsabile del trattamento dei dati, è responsabile di tutti i dati personali caricati sui servizi AWS (**Sicurezza NEL cloud**) di cui l'Ente è Titolare.

Nello schema sottostante evidenziano i ruoli del modello di responsabilità condivisa.

Per Customer si intende APKAPPA che agisce come Responsabile esterno al trattamento dei dati di cui l'Ente è Titolare.



Responsabilità di AWS "Sicurezza DEL cloud" – AWS si occupa di proteggere l'infrastruttura globale su cui vengono eseguiti tutti i servizi offerti nel cloud AWS. L'infrastruttura include hardware, software, rete e strutture in cui sono in esecuzione i servizi AWS, che forniscono a clienti potenti controlli quali la configurazione della sicurezza per gestire i contenuti dei loro clienti. AWS offre diversi report di conformità provenienti da enti di controllo di terze parti, che ne hanno verificato la conformità con numerosi standard e normative di sicurezza informatica. AWS è conforme alle norme ISO 27001, 27017 e 27018. La norma ISO 27018 contiene controlli di sicurezza volti alla protezione dei dati dei clienti.

### 3. Descrizione del trattamento

#### Categorie di interessati i cui dati personali sono trattati

- Cittadini
- Dipendenti
- Fornitori
- Utenti
- Amministratori

#### Categorie di dati personali trattati

- Dati comuni
- Dati particolari
- Dati giudiziari

#### Natura del trattamento

Trattamento di dati comuni, dati particolari e dati giudiziari

#### Finalità per le quali i dati personali sono trattati per conto del titolare del trattamento

Trattamento di dati relativi a:

- Gestione segreteria e affari generali
- Conservazione documenti informatici
- Cessazione del servizio di conservazione
- Gestione del servizio elettorale
- Gestione obblighi civili
- Gestione elezioni
- Gestione anagrafe

- Gestione Stato civile
- Gestione censimento
- Gestione Leva militare
- Gestione servizi scolastici
- Gestione altri servizi a domanda individuale
- Gestione servizi sociali
- Gestione servizi finanziari
- Servizi risorse umane
- Gestione servizi ufficio tecnico
- Gestione assistenza
- Gestione migrazione

#### Durata del trattamento

Conservazione fino al termine dell'erogazione del servizio.

#### **4. Misure tecniche organizzative per garantire la sicurezza dei dati.**

- Antivirus
- Autenticazione
- Autorizzazione
- Business continuity/disaster recovery
- Cambio password
- Firewall
- Intrusion detection
- Protocollo https
- Segregazione accessi
- Separazione ambienti
- Vulnerability assessment/penetration test
- Disaster recovery
- Cifratura dei protocolli di comunicazione
- Pseudonimizzazione
- Audit trail
- Accesso controllato
- Armadi chiusi
- Formazione
- Istruzioni per il trattamento
- Nomina per iscritto delegati, autorizzati
- Nomina per iscritto responsabili esterni
- Policy aziendali (regolamento IT)
- Istruzioni operative per il trattamento dei dati durante l'attività di assistenza
- Impianto di Videosorveglianza
- Istituzione Ufficio Privacy
- Registro delle richieste degli interessati
- Registro delle richieste di divulgazione e trasferimento dati

#### **5. Indicatori della qualità del servizio SaaS hyperSIC Cloud.**

Codice SLI	Indicatore	Descrizione	Valore Offerto
SLI1	Availability	<p>La percentuale di tempo in un dato periodo di riferimento in cui il servizio risulta essere accessibile e usabile.</p> <p>Quale periodo di riferimento si assume convenzionalmente il mese.</p> <p>Il tempo totale del periodo di riferimento, che funge da base di calcolo del dato percentuale, può tenere conto dei fermi programmati del servizio (in tal caso il CSP deve esplicitare questa circostanza).</p>	<p>Piattaforma Cloud APKSer.Cloud: <b>99.5</b></p> <p>Piattaforma Cloud AWS: <b>99.5</b></p>
SLI2	Support hours	<p>L'orario in cui il servizio di supporto tecnico è operativo (eventualmente differenziato per "support plan" sottoscrivibile).</p>	<p><b>Telefono:</b> Disponibile Ore supporto: dal lunedì al venerdì, dalle 8.30 alle 17.30 (escluso festivi) – opzionale sabato dalle 8:30 – 14:00</p> <p><b>Sistema di on-line ticketing:</b> Disponibile Ore supporto: dal lunedì al venerdì, dalle 8.30 alle 17.30 (escluso festivi) – opzionale sabato dalle 8:30 – 14:00</p> <p><b>Assistenza on-site:</b> Disponibile Ore supporto: dal lunedì al venerdì, dalle 8.30 alle 17.30 (escluso festivi) – opzionale sabato dalle 8:30 – 14:00</p> <p><b>Assistenza remota:</b> Disponibile Ore supporto: dal lunedì al venerdì, dalle 8.30 alle 17.30 (escluso festivi) – opzionale sabato dalle 8:30 – 14:00</p>
SLI3	Maximum First Support Response Time	<p>Il tempo massimo che intercorre tra la segnalazione di un inconveniente da parte del cliente e la risposta iniziale alla segnalazione da parte del CSP.</p>	<b>120 minuti</b>
SLI4	Cloud Service Bandwidth	<p>La quantità di dati che può essere trasferita in un determinato periodo di tempo.</p> <p>Da intendersi rispetto all'interfaccia Client (laddove applicabile) oppure nell'ambito della virtual network.</p>	<p>La suite hyperSIC10, su cui si basa il servizio SaaS hyperSIC Cloud proposto necessita di una banda minima di circa 2Mbit/sec sia in upload che in download (preferibilmente con basse latenze); ogni valore superiore</p>

Codice SLI	Indicatore	Descrizione	Valore Offerto
			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), l'applicativo hyperSIC10 in tecnologia Web non produce consumo costante ma di tipo request/response, minimizzando e rendendo efficiente l'uso di banda trasmissiva.
SLI5	Limit of Simultaneous Cloud Service Connections	Numero massimo di connessioni simultanee supportate dal servizio.	L'architettura web native della suite hyperSIC10 e la scalabilità del servizio SaaS hyperSIC Cloud consente un numero illimitato di connessioni simultanee
SLI6	Cloud Service Throughput	Il numero di input o insieme di input correlati tra di loro (transazione) che possono essere processati in ciascuna unità di tempo dal servizio.	
SLI7	Elasticity Speed	Descrive quanto velocemente reagisce il servizio alla richiesta di nuove risorse allorquando: <ul style="list-style-type: none"> <li>• viene effettuata una richiesta di riallocazione (nel caso di elasticità manuale), oppure</li> <li>• il carico di lavoro cambia (in caso di elasticità automatica).</li> </ul>	Il servizio proposto utilizza l'Elasticità Manuale. Il monitoraggio è costante e ciò consente di prevedere la necessità di espansione e di mantenere elevati standard di servizio scalabile in ogni sua componente.
SLI8	Maximum Time to Service Recovery	Il massimo tempo che intercorre tra l'indisponibilità del servizio dovuta a malfunzionamento di una delle sue componenti e il ripristino della sua normale operatività.	A parte casi di Disaster Recovery definiti in SLI12, in caso di malfunzionamento di una componente, poiché il sistema è in High Availability, in ogni sua componente, il Time to Service Recovery è pressoché nullo (failover istantaneo)
SLI9	Backup Interval	Il tempo che intercorre tra un backup e l'altro.	<b>24 ore</b> per i dati meno critici <b>3 ore</b> per i dati critici (DB incrementale)
SLI10	Retention period of backup data	Il periodo di tempo in cui vengono mantenuti i backup da parte del CSP.	Ultimi 7 gg Ultime 4 settimane Ultimi 12 mesi Ultimo anno
SLI11	Backup restoration testing	Il numero di test di restore	Sono effettuati Report periodici ogni 4 mesi, all'interno dei quali

Codice SLI	Indicatore	Descrizione	Valore Offerto
		(a partire dai dati di backup) eseguiti durante un determinato periodo di tempo.	vengono eseguite da 10 a 20 azioni di restore
SLI12	Recovery Time Objective (RTO)	Il tempo massimo necessario a ripristinare completamente il servizio dopo un'interruzione dovuta ad un "evento catastrofico" che ha innescato l'attivazione di un ambiente di erogazione secondario (disaster recovery).	<b>RTO massimo di 3 ore</b>
SLI13	Recovery Point Objective (RPO)	L'intervallo massimo di tempo che precede un "evento catastrofico" rispetto al quale si può verificare la perdita delle modifiche ai dati come conseguenza delle attività di ripristino del servizio (disaster recovery).	<b>RPO massimo di 24 ore</b>
SLI14	Data retention period	Il periodo di tempo in cui i dati del cliente vengono mantenuti dal CSP dopo la notifica di cessazione del servizio.	<b>30 giorni</b>
SLI15	Log retention period	Il periodo di tempo in cui i file di log relativi al servizio vengono conservati dopo la notifica di cessazione del servizio.	Tempo minimo di conservazione dei log di servizio: <b>90 gg</b> Tempo massimo di conservazione dei log di servizio: <b>180 gg</b>