**CSI PIEMONTE**

**SERVIZIO PER SUPPORTO ALL’ESECUZIONE DI AUDIT GDPR DI FORNITORI TERZI**

**(APIM22\_010)**

**REQUISITI TECNICO - FUNZIONALI E MODALITÀ DI FORNITURA**

**[***Indicare qui il nome dell’operatore economico partecipante***]**

# INTRODUZIONE

Nel contesto della presente manifestazione il CSI Piemonte ha interesse ad individuare per sè e per i propri Enti Consorziati, una soluzione di supporto che permetta di ottimizzare ed efficientare il processo di verifica di compliance alla normativa GDPR di fornitori terzi nominati sub-responsabili.

Per soddisfare tale esigenza si intende verificare la possibilità di usufruire di un servizio che venga espletato tramite la fruizione di una soluzione che permetta di gestire in modalità efficace la gestione di checklist /questionari da sottoporre ai fornitori terzi e che sia di supporto per la gestione dell’analisi dei riscontri ottenuti agevolando in tal modo il processo di controllo, la verifica ed il tracciamento delle evidenze raccolte.

Si evidenziano di seguito le caratteristiche principali (funzionali e non funzionali) della soluzione desiderata:

* **Articolazione:** la soluzione individuata deve essere estremamente flessibile e personalizzabile
* **Dispiegamento della soluzione**: la soluzione deve essere fruibile in modalità SAAS. In alternativa si chiede di valutare eventualmente il dispiegamento on premises su Cloud CSI
* **Durata del servizio:** la soluzione deve poter essere fruita per una durata minima pari a 12 mesi

Il presente documento – che costituisce l’allegato 1 *all’Avviso pubblico per la manifestazione di interesse per l’acquisizione a titolo di sperimentazione -e successiva eventuale acquisizione a titolo oneroso- di una soluzione software a supporto per l’esecuzione di Audit GDPR di Fornitori Terzi* – ha l’obiettivo di verificare la presenza sul mercato di soluzioni dotate – in tutto o in parte – di caratteristiche funzionali e tecniche atte a soddisfare le esigenze del CSI-Piemonte, conoscendone anche le relative modalità di fornitura/distribuzione oltre che le stime di massima su costi e tempi di messa a disposizione.

# Nota bene: Si segnala che, gli operatori partecipanti sono invitati a non inserire tra le informazioni fornite partecipando alla presente Consultazione elementi protetti da segreto industriale , know-how, proprietà intellettuale e/o industriale o analoga normativa ovvero segnalare quali informazioni siano da considerare protetti da segreto industriale, know-how, proprietà intellettuale e/o industriale o analoga normativa, di cui si vuole inibire l’uso ulteriore.

#

# DESCRIZIONE IN SINTESI DELLA SOLUZIONE PROPOSTA

*Inserire qui una breve descrizione (max 2 pagine) della soluzione proposta e delle tecnologie di riferimento adottate dalla soluzione (system software, linguaggi di sviluppo e middleware).*

# SODDISFACIMENTO DEI REQUISITI

Nel seguito sono elencati i requisiti individuati per la soluzione sulla base delle esigenze espresse anche dagli Enti fruitori del servizio

Si distinguono in tabelle separate:

* i requisiti funzionali (RF),
* i requisiti non funzionali (RNF),
* la modalità di fornitura del software (MF)

Nel seguito si descrive il significato delle colonne:

* **Gruppo di requisiti**: per i requisiti non funzionali e le modalità di fornitura descrive il raggruppamento logico del requisito. (NON MODIFICARE) non è un campo presente nella tabella
* **ID**: descrive il codice univoco del requisito (NON MODIFICARE)
* **Requisito**: descrive il singolo requisito individuato (NON MODIFICARE)
* **Obbligatorio (O) / Informativo (I):** i requisiti contrassegnati con la
	+ **O** sono considerati essenziali/imprescindibili. La loro assenza non permette di prendere in considerazione la soluzione proposta;
	+ **I** sono utili a comprendere elementi alternativi o utili ma non rappresentativi ai fini della valutazione in termini quantitativi della soluzione valutata
* **Requisito soddisfatto:** indica la disponibilità del requisito da parte della soluzione proposta nella versione attualmente disponibile (COMPILARE). La disponibilità/non disponibilità deve essere indicata con “SI/NO”.
* **Note** (DA COMPILARE OPZIONALMENTE E/O OVE RICHIESTO): spazio da utilizzare per fornire precisazioni esplicative rispetto al soddisfacimento del requisito.

**Requisiti funzionali**

| **ID** | **Requisito funzionale (RF)** | **Obbligatorio (O)** **Informativo(I)** | **Requisito soddisfatto****(SI/NO)**  | **Note** |
| --- | --- | --- | --- | --- |
| **RF1** | La soluzione permette la predisposizione di check list di controllo basate sulle evidenze richieste dalla normativa privacy | **O** |   |  |
| **RF2** | Il sistema permette di ottenere dei report di sintesi dei risultati | **O** |  |  |
| **RF3** | La soluzione permettere la compilazione direttamente da form web  | **O** |   |  |
| **RF4** | La soluzione è accessibile solo dopo autenticazione | **O** |   |  |
| **RF5** | La soluzione può inviare notifiche, quando la check list e stata compilata | **O** |  |  |
| **RF6** | La soluzione permette di salvare in bozza prima di invio completo della check list | **O** |  |  |
| **RF7** | La soluzione permette di avere degli indicatori in automatico in baseal livello dei rischi individuati dalla compilazione  | **O** |   |  |
| **RF8** | Lo strumento prevede funzionalità per la creazione/gestione di profili distinti, la definizione dei permessi granulari di ogni profilo e l'attribuzione puntuale dei profili alle risorse degli attori della soluzione (almeno 2: Admin e compilatore) | **O** |  |  |
| **RF9** | La soluzione permette di gestire eventuali parametrizzazioni  | **O** |   |  |
| **RF10** | Lo strumento traccia chi ha fatto una determinata operazione e deve mantenere i log per un tempo predefinito (configurabile) | **I** |  |  |
| **RF11** | Lo strumento mette a disposizione funzionalità di ricerca all’interno delle informazioni censite | **O** |  |  |
| **RF12** | La soluzione prevede la generazione di reportistica  | **O** |  |  |
| **RF13** | La soluzione prevede funzionalità di back office ad uso di un utente amministratore per la gestione delle informazioni  | **O** |  |  |
| **RF14** | La soluzione permette di personalizzare le check list in base a gruppi di fornitori/forniture | **O** |  |  |
| **RF15** | La soluzione prevede un cruscotto/report con la vista per il DPO | **I** |  |  |
| **RF16** | La soluzione prevede di verificare se ci sono compilazioni in pendig | **O** |  |  |
| **RF17** | Il fornitore garantisce la gestione sistemistica del servizio (installazioni di patch, rilasci, monitoraggio del corretto funzionamento applicativo) compresa la gestione del Sistema Operativo tramite  | **O** |  |  |

**Requisiti non funzionali**

I requisiti “non funzionali” includono requisiti tecnici o di servizio.

| **Classe del Requisito** | **ID** | **Requisito tecnico, architetturale, infrastrutturale e non funzionale (RNF)** | **Obbligatorio (O)** **Informativo(I)** | **Requisito soddisfatto**  | **Note** |
| --- | --- | --- | --- | --- | --- |
| **Portability** | **RNF1** | La soluzione garantisce lo stesso tipo di funzionamento su dispositivi client di diverso tipo: PC Desktop, Laptop, Tablet, Smartphone. | **I** |  |  |
| **Portability** | **RNF2** | La soluzione garantisce lo stesso tipo di funzionamento su diverse tipologie di dispositivi client (ad esempio PC Desktop, Laptop, Tablet, Smartphone) attraverso modalità web responsive. | **I** |  |  |
| **Portability** | **RNF3** | La Soluzione è fruibile da parte dell’utente finale attraverso l’utilizzo di web browser (anche in coesistenza) di comune diffusione alle versioni stabili e supportate (ad es. Internet Explorer dalla vers. 10, Edge, Mozilla Firefox dalla v.30, Chrome dalla v.54, ecc.) ed a quelle future, senza la necessità di prevedere l’installazione di applicativi o plug-in ad hoc sulla macchina client dell’utente finale. | **O** |  |  |
| **Standardisation** | **RNF4** | La soluzione prevede l’esportazione di dati e report per più strumenti di produttività individuale alternativi (MS Office, Open Office, Libreoffice, ecc.). | **I** |  | specificare quali |
| **Standardisation** | **RNF5** | La soluzione è in grado di esportare, nell’ambito di ciascuna delle funzionalità offerte, documenti in formato OpenDocument (ODF) | **I** |  |  |
| **Standardisation** | **RNF6** | La soluzione è in grado di esportare documenti in formato PDF e PDF/A | **I** |  |  |
| **Security** | **RNF7** | La comunicazione tra i sistemi (compreso il client web, sia con i sistemi esterni, sia le componenti interne alla soluzione) avviene in modalità sicura, adottando politiche di cifratura del canale e securizzando le comunicazioni proteggendo i servizi con meccanismi idonei (https/ssh). | **O**  |  |  |
| **Security** | **RNF8** | Sono disponibili i risultati dei test di vulnerabilità della soluzione, effettuati periodicamente, per le istanze già installate. | **I** |  |  |
| **Security** | **RNF9** | È garantito il monitoraggio e controllo della sicurezza applicativa del sistema (vulnerability assessment e patching di sicurezza). | **O** |  |  |
| **Security** | **RNF10** | Sono prontamente evidenziate le situazioni legate ad anomalie di sicurezza (accessi anomali, brute force attack, ecc.). | **I** |  |  |
| **Performance & Availability** | **RNF11** | La soluzione continua ad essere disponibile indipendentemente dalla quantità di accessi, senza soluzione di continuità né decadimento apprezzabile delle prestazioni. | **I** |  |  |
| **Backup** | **RNF12** | Sono previste delle procedure di backup dei dati gestiti dalla soluzione. | **O** |  |  |
| **Usability** | **RNF13** | La soluzione adotta lo standard HTML 5 per la implementazione del Presentation Layer nel caso di fruizione via web browser | **I** |  |  |
| **Usability** | **RNF14** | Il look and feel dell’interfaccia utente deve essere personalizzabile con elementi grafici del committente | I |  |  |
| **Monitoring** | **RNF15** | La soluzione adotta un sistema di traceability delle attività degli utenti, assicurando il monitoraggio attraverso la fruizione dei log di audit,  | **I** |  |  |
| **Quality** | **RNF16** | I dati gestiti dalla soluzione sono mantenuti e storicizzati, ovvero la soluzione mantiene e storicizza i dati necessari almeno per 12 mesi | **I** |  |  |
| **Quality** | **RNF17** | La documentazione della soluzione è corredata di manuale utente e/o altro strumento di supporto all’uso a beneficio dell’utente (es. FAQ). | **I** |  |  |
| **Quality** | **RNF18** | La soluzione garantisce l’univocità dei Master Data presenti nella Base Dati (ovvero non esistono duplicazioni non necessarie dei dati) all’interno di tutto il sistema. | **I** |  |  |
| **Compliance** | **RNF19** | La soluzione rispetta i requisiti previsti dal Regolamento UE 2016/79 noto come GDPR (General Data Protection Regulation).In particolare sono presi in considerazione i seguenti articoli del regolamento:• art 25 – privacy by design. La soluzione garantisce che gli aspetti legati all’implementazione della privacy sono tenuti in considerazione sin dalla fase di progettazione.• art 32 – Misure di sicurezza. In particolare, almeno: - integrazione con sistema di autenticazione centralizzato, - gestione della profilazione utenti, - gestione degli audit log (poter ricostruire a posteriori “chi ha fatto che cosa, come e quando”), - tracciamento degli accessi; - storicizzazione dei dati; - cifratura di canale- gestione delle sessioni e dei cookies. | **O** |  |  |

**Modalità di fornitura della soluzione**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Business support** | **L1** | Il fornitore può erogare giornate di formazione e training on the job al personale della stazione appaltante | **I** |  |  |
| **Business support** | **L2** | Il software è messo a disposizione attraverso modalità Cloud computing o "SaaS" (software as a service, in cui il software viene erogato come servizio da remoto sui sistemi del fornitore o di terzi accreditati).  | **O** |  |  |
| **Business support** | **L3** | Il software è messo a disposizione on premises sul Cloud del CSI Piemonte  | **I** |  |  |

**DIMENSIONAMENTO DELLA SOLUZIONE**

Per consentire al fornitore una stima dei costi e dei tempi si riportano di seguito alcuni dati indicativi di dimensionamento:

| **ID** | **Descrizione** | **Q.tà** |
| --- | --- | --- |
| **1** | Numero di audit (invio di check list e analisi) previsti per la fase di sperimentazione del servizio | **20** |
| **2** | Numero di audit (invio di check list e analisi) previsti per la fase di erogazione del servizio | **100** |

**COSTI E TEMPI INDICATIVI DELLA MESSA A DISPOSIZIONE DELLA SOLUZIONE**

Si richiede di compilare le seguenti tabelle relative a costi e tempi per la messa a disposizione e per la gestione della soluzione desiderata. Si ricorda che si tratta di stime di massima, non impegnative (non costituiscono offerta), ma saranno utilizzate quale ausilio al dimensionamento degli importi da porre a base d’asta ed i requisiti tecnici acquisiti saranno utilizzati per strutturare il capitolato tecnico per una eventuale successiva procedura di approvvigionamento finalizzata all’acquisizione della soluzione dal mercato.

In particolare, le stime riguardano:

* i requisiti funzionali e non funzionali;
* la messa in esercizio della soluzione.

**Costo delle componenti**: costo complessivo stimato della messa a disposizione delle caratteristiche funzionali e non funzionali.

I valori economici stimati verranno considerati oneri fiscali esclusi.

Compilare la seguente tabella in base alla metrica proposta.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Costo stimato** | **Sperimentazione di 20 audit\*** | **Erogazione di servizio di supporto per 50 audit** | **Erogazione di servizio di supporto per 100 audit** | **Costo pacchetti aggiuntivi di 10 audit** |
| Costo del supporto complessivo (fase di predisposizione, invio, ricezione ed analisi delle check list) \* |  |  |  |  |
|  |  |  |  |  |
| Assistenza all’analisi di secondo livello (indicare il costo di una singola giornata) |  |  |  |  |
|  |  |  |  |  |

\*Indicare il costo complessivo stimato per la sperimentazione ovvero la possibilità di effettuare la sperimentazione a titolo gratuito.

Firma digitale

*(Legale rappresentante o Persona autorizzata alla firma)*