Risposte alle richieste di chiarimento pervenute da parte degli operatori economici prima della data di presentazione delle offerte.

Estremi della gara:

Oggetto: Procedura negoziata previa consultazione di elenco operatori su MEPA ai sensi e per gli effetti della L 120/2020, art. 1, co. 2 lett. b) per Acquisizione di una soluzione di GRC (Governance, Risk Management e Compliance) e servizi connessi - CIG 9521342BF8

Domanda 1:

Il capitolo parla di un'attività di popolamento della basedati tramite l'importazione dei dati presenti negli attuali strumenti (fogli di calcolo e Utopia – NSI Nier).
E' possibile avere esempi dei fogli di calcolo utilizzati e dei file di esportazione prodotti da Utopia?

Risposta 1:

Per motivi di riservatezza dei dati, i file non possono essere resi disponibili.
In ogni caso l'attività riguarda sostanzialmente l'importazione di dati strutturati, resi disponibili attraverso formati standard, relativi a: registro dei trattamenti dei dati, registro istanze degli interessati, organizzazione, anagrafica dei soggetti esterni responsabili dei trattamenti.

Domanda 2:

Si chiede di confermare che le funzionalità della soluzione GRC debbano prevedere la valutazione dei rischi 231 e 190 direttamente mediante l'applicativo, attraverso l'attivazione di flussi automatizzati (campagne di assessment) che prevedano il coinvolgimento dei risk owner (cd. key officer), o che la soluzione sia esclusivamente funzionale all'integrazione delle diverse dimensioni di analisi del rischio così come rappresentato nelle schede indicate di riferimento.

Risposta 2:

Si conferma che funzionalità della soluzione GRC devono prevedere la valutazione dei rischi 231 e 190 direttamente mediante l'applicativo, con flussi automatizzati che coinvolgano i risk owner.

Domanda 3:

Si chiede di confermare che la valutazione degli altri rischi 50/16, trasparenza, privacy, 262/05, sicurezza delle informazioni, sicurezza fisica, AML, rischio operativo sia effettuata extra sistema ed unicamente importata nella soluzione GRC.

Risposta 3:

Non si conferma. Le funzionalità della soluzione GRC devono prevedere la valutazione degli altri rischi direttamente mediante l'applicativo, con flussi automatizzati che coinvolgano i risk owner.

Domanda 4:

Si chiede di confermare che il servizio di assistenza deve prevedere disponibilità 5 giorni su 7 dal lunedì al venerdì per 10 ore al giorno (fascia oraria 8-18), escludendo i giorni festivi.

Risposta 4:

Si conferma.

Domanda 5:

Si chiede di confermare che l'applicazione delle penali di cui al paragrafo 8 del capitolato tecnico, punti 2, e 4 non siano previste qualora i ritardi siano ascrivibili direttamente a CONSIP.

Risposta 5:

Al paragrafo 3.2 del Capitolato tecnico è riportato "*Il Piano di Lavoro, in accordo e previa autorizzazione della Committente, potrà essere soggetto a modifiche e ripianificazioni, secondo le esigenze che emergeranno in corso di svolgimento delle attività contrattuali.*", pertanto il Fornitore è tenuto ad aggiornare tempestivamente il Piano di Lavoro, sottoponendolo all'accettazione della Committente, ogni qualvolta si manifestino eventi tali da poter causare ritardi che non siano ascrivibili al Fornitore stesso.
Solo per eventuali ritardi non prevedibili e ascrivibili direttamente a Consip non è prevista l'applicazione delle penali.

Domanda 6:

Nel Capitolato Tecnico al par. 2, pag. 4, è riportato che:
"I servizi di assistenza e manutenzione dovranno prevedere:

- costante allineamento della soluzione all'evoluzione normativa di riferimento"

Ciò è da intendersi unicamente come fine tuning alla metodologia esistente o come riprogettazione strutturale della soluzione in funzione di cambiamenti radicali apportati dall'evoluzione alla normativa di riferimento?

Risposta 6:

Si conferma che la soluzione, da erogarsi in modalità SaaS, dovrà garantire il costante adeguamento all'evoluzione normativa di riferimento.

Domanda 7:

Nel Capitolato Tecnico al par. 2, pag. 4, è riportato che

"I servizi di assistenza e manutenzione dovranno prevedere:

- adeguamento della soluzione alle evoluzioni tecnologiche"

Ciò è da intendersi unicamente in riferimento ad eventuali modifiche richieste sull'interfacciamento con sistemi terzi? In caso negativo, potreste esplicitare l'elenco dei potenziali adeguamenti delle funzionalità/dinamiche applicative che dovranno essere previste?

Risposta 7:

Si conferma che l'adeguamento della soluzione è da intendersi indirizzato a garantirne l'interfacciamento e il colloquio con servizi terzi.

Domanda 8:

Nel Capitolato Tecnico al par. 2, pag. 5, è riportato che

"I servizi di assistenza e manutenzione dovranno prevedere:

- supporto tecnico e applicativo tramite email e/o contatto telefonico."

Analogamente a quanto specificato per i servizi di formazione/consulenza, è possibile prevedere un quantitativo massimo di giornate e/o numero massimo di ticket di supporto, eventualmente basato su un periodo temporale predefinito (es. base mensile o trimestrale), anche per i suddetti servizi di assistenza e manutenzione?

Risposta 8:

Trattandosi di manutenzione e assistenza di una piattaforma software erogata in modalità SaaS, non è possibile per la Committente determinare "a priori" la quantità di richieste che potranno essere inviate al Fornitore.

Domanda 9:

Nel Capitolato Tecnico al par. 2.1, pag. 5, è riportato che:

"Per quanto riguarda le funzionalità di Privacy, il sistema deve avere funzionalità e caratteristiche analoghe a quelle del sistema attuale"

È possibile avere l'elenco dettagliato delle funzionalità Privacy e processi applicativi del sistema attuale che la piattaforma GRC dovrà prevedere?

Risposta 9:

La componente privacy della soluzione, oltre alle funzionalità generali condivise con gli altri moduli deve avere almeno le seguenti funzioni principali:

- Gestione anagrafica risorse, ruoli e funzioni aziendali (inclusa storicizzazione per gestire i cambiamenti organizzativi);
- Tenuta e gestione del Registro dei Trattamenti coerentemente con organigramma aziendale e sue evoluzioni nel tempo;
- Tenuta e gestione del registro istanze degli interessati;
- Valutazione d'impatto DPIA (Data Protection Impact Assessment) con catalogo Minacce e Misure di Sicurezza;
- Gestione ruoli privacy: DPO, Soggetti autorizzati ai trattamenti, Responsabili del Trattamento, Titolari autonomi, Contitolari;
- Configurazione e gestione degli Audit (controlli di conformità) con la produzione di evidenze di verifica:

- Tenuta del Registro delle Violazioni (Registro Data Breach) comprensivo di Tool per la determinazione della gravità della violazione utile per decidere se notificare al Garante e generazione del registro e dei report per la notifica al Garante;
- Censimento e gestione degli Asset (applicazioni, database, etc) in cui sono allocati i dati personali.

Domanda 10:

Si chiede di specificare se le istanze e le licenze della piattaforma di supporto alla soluzione GRC, dovranno essere intestate alla committente o al fornitore.

Risposta 10:

Come specificato al paragrafo 2.1 del Capitolato tecnico, la soluzione richiesta è una piattaforma software qualificata come servizio SaaS da AGID (e successivamente dalla Agenzia per la Cybersecurity) e deve essere presente nel Marketplace Cloud della PA. Pertanto non è prevista la fornitura di licenze da intestare alla Committente.

Firma del responsabile
approvazione

Vale la firma digitale
del documento

Il Responsabile
Divisione Sourcing Operation
(Gianandrea Greco)

GIANANDREA
GRECO
CONSIP S.P.A
13.12.2022
08:37:37 UTC