Amet SPA

" Manifestazione di Interesse per la Fornitura di Servizi di Supporto Specialistico in ambito GDPR per Amet SPA "

CAPITOLATO SPECIALE D'ONERI

Allegato 1

CAPITOLATO TECNICO

INDICE

1 Ambito di riferimento

Il contesto macroeconomico e competitivo del mercato richiede un forte impegno operativo da parte di AMET S.p.A. volto ad assicurare l'erogazione di Servizi integrati e innovativi, offerti ad una clientela sempre più esigente e differenziata, con riguardo al miglioramento continuo della qualità ed al contenimento dei costi.

Nello specifico, nell'ambito di tali direttive deve soddisfare i seguenti punti:

- Gap Analysis sia tecnologica che procedurale per essere conforme all'art.35 del nuovo regolamento europeo GDPR Regolamento (UE) n. 2016/679

- Inserire nell' Organizzazione una figura di DATA PROTECTION OFFICER – DPO (Art. 37)

2 Oggetto della Gara

Oggetto della presente Gara è l'impegno alla Fornitura di questi Servizi di Supporto Specialistico:

- Servizi di GAP Analysis relativi all'art 35 del Regolamento Europeo GDPR n. 2016/679
- Figura del DPO - DATA PROTECTION OFFICER (Art. 37) da inserire nell' Organizzazione del Cliente.

La fornitura si compone di un unico Lotto.

Lotto 1	Fornitura dei Servizi di Supporto Specialistico	Servizi di GAP Analysis
		Fornitura di 1 figura Data Protection Officer (DPO)

Tabella 1 — Composizione dei Servizi Richiesti

Per ciò che concerne la Fornitura di Servizi di Gap Analysis, le attività previste andranno suddivise in Type-of-Work; Nella Tabella che segue vengono indicati i fabbisogni in termini percentuali di ciascun Type-of-Work (d'ora in avanti TOW) nel periodo di validità contrattuale.

TOW	Descrizione	Peso % (effort)
TOW 1	GAP Analysis Tecnologica	40%
TOW 2	GAP Analysis Procedurale	60%

Tabella 2 — Type-of-work (TOW) e relativo peso percentuale

Il Data Protection Officer sarà una persona esterna all' Azienda e coprirà questo ruolo per la durata di 12 Mesi.

La stazione appaltante si riserva, per il solo servizio di DPO, ai sensi dell'art. 106, la facoltà di prorogare per un ulteriore anno il solo servizio di Data Protection Officer (DPO).

I servizi dovranno essere erogati nel mese successivo alla data di stipula contrattuale con AMET SpA.

2.1 Utilizzo apparecchiature

Nell'erogazione dei servizi oggetto di gara, è richiesto che l'Impresa utilizzi proprie apparecchiature (PC), che dovranno essere dotate (o predisposte per l'utilizzo) degli strumenti progettuali indicati nel successivo paragrafo.

L'accesso ai sistemi di AMET SpA per svolgere le attività previste nel presente documento sarà regolato dalle procedure vigenti in azienda che saranno messe a disposizione dell'Impresa dal responsabile della Funzione di GAP Analysis.

2.2 Strumenti progettuali

Attività/prodotto	Strumento
Documenti	Microsoft Word @ 2003 e successive
Tabelle	Microsoft Excel @ 2003 e successive
Rappresentazioni grafiche	Microsoft PowerPoint @ 2003 e successive
Elaborazione	Qualys Vulnerability management Checkmarx Vulnerability Code

Tabella 3 — Strumenti progettuali

L'uso di tali strumenti non dovrà comunque comportare oneri aggiuntivi per AMET SpA.

La proprietà delle licenze rimarrà dell'Impresa.

Al termine delle attività, tali strumenti dovranno essere eliminati dagli ambienti di AMET SpA, senza che ciò comporti alcun impatto sull'operatività.

3 Requisiti minimi obbligatori della fornitura

Vengono di seguito illustrati i requisiti minimi e obbligatori che devono essere soddisfatti dai servizi oggetto della fornitura.

Le caratteristiche si intendono minime e obbligatorie, pena la risoluzione del contratto.

3.1 Gap Anaysis

Le Attività di Gap Analysis devono essere erogate con le modalità riportate in tabella.

TOW	Denominazione	Descrizione	Risultato
TOW 1	GAP Analysis Tecnologica	Assessment tecnologico volto a individuare il livello di adeguamento e le azioni da intraprendere per soddisfare i requisiti di sicurezza richiesti dal regolamento europeo sulla privacy General Data Protection Regulation (GDPR) Regolamento (UE) n. 2016/679. Particolare attenzione dovrà essere dedicata a documentare, ai fini della prova del rispetto della norma, quanto sarà realizzato.	Definizione di un percorso (attività/priorità/massimo sfruttamento di semplificazioni normative) per colmare i gap tecnologici individuati ed essere conformi al Regolamento o aver definito le opportune strategie definite dal Regolamento.
TOW 2	GAP Analysis Procedurale	Assessment Procedurale volto a individuare il livello di adeguamento e le azioni da intraprendere per soddisfare i requisiti di sicurezza richiesti dal regolamento europeo sulla privacy General Data Protection Regulation (GDPR) Regolamento (UE) n. 2016/679. Particolare attenzione dovrà essere dedicata a documentare, ai fini della prova del rispetto della norma, quanto sarà realizzato.	Definizione di un percorso (attività/priorità/massimo sfruttamento di semplificazioni normative) per colmare i gap procedurali individuati ed essere conformi al Regolamento o aver definito le opportune strategie definite dal Regolamento.

Tabella 4 — Gap Analysis – Modalità Procedurali

Nei paragrafi successivi, vengono elencate le attività che l'Impresa dovrà svolgere per ogni singola iniziativa del TOW di riferimento.

3.1.1 TOW 1: Gap Analysis Tecnologica

Scopo dell'assessment è la definizione di un percorso (attività/priorità/massimo sfruttamento di semplificazioni normative) per colmare i **gap tecnologici** individuati ed essere conformi al Regolamento o aver definito le opportune strategie definite dal Regolamento.

Nella Tabella sono riportate le macro attività previste all'interno del TOW 1 e saranno dettagliate nel seguito del paragrafo.

Modalità Operativa	MacroAttività
TOW1: GAP Analysis Tecnologica	Audit conoscitivo
	Verifica degli Adempimenti delle attività e della documentazione
	Verifica del livello di sicurezza dell' infrastruttura informatica del Cliente

Tabella 5 — Gap Analysis Tecnologica – MacroAttività

In sede di **Audit conoscitivo** verranno affrontati i seguenti argomenti:

- Verifica del sito;
- Verifica delle misure di sicurezza fisica;
- Verifica delle misure di sicurezza logica;
- Colloqui con interessati;
- Videosorveglianza e geolocalizzazione;
- Infrastruttura IT.

Si procederà con la **Verifica degli adempimenti delle attività già svolte e della documentazione presente**, allo scopo di:

- accertare lo stato dell'arte;
- individuare eventuali non conformità;
- definire le tipologie ed il livello di eventuali azioni correttive che si ritenessero necessarie;
- individuare le disposizioni normative del Regolamento che risultino non applicabili e documentarne le relative motivazioni, allo scopo di rendere il più agevole possibile l'adeguamento dell'azienda.

Tale attività da svolgere sul campo con personale della AMET S.p.A. sarà finalizzata ad arricchire il documento rilasciato con attestazioni tese a portare in evidenza le modalità di gestione dei dati ed eventuali punti critici.

In particolare per la verifica dei gap tecnologici verranno analizzate approfonditamente le seguenti aree di adempimenti:

- Valutazione del rispetto dei principi di data protection
- Individuazione di eventuali processi/trattamenti che necessitano di Valutazione d'impatto sulla protezione dei dati e suggerimenti su quando/come realizzarla
- Definizione delle misure di sicurezza delle informazioni in linea con le best practices internazionali
- Policy sull'utilizzo degli strumenti informatici, di Internet ed e-mail e devices mobili
- Verifica Diritto alla portabilità dei dati
- Stato compliance complessiva dei siti web aziendali
- Stato compliance complessiva dei sistemi di videosorveglianza in essere

Per quanto riguarda la **Verifica del livello di sicurezza dell' infrastruttura informatica del cliente** (gap tecnologico) si procederà con l'analisi dei rischi e delle vulnerabilità e con un particolare focus nell'individuare e descrivere:

- Le modalità operative sicure per correlare e collegare i dati con altre basi di dati;
- Le regole per lo sviluppo sicuro del codice sorgente degli applicativi;
- I Business Requirement per l'IT Department che saranno utilizzati per la software selection delle soluzioni informatiche e per l'evoluzione delle applicazioni;
- I requisiti tecnici, (supportando l'IT Department del committente nella definizione degli stessi) per il rafforzamento delle misure di sicurezza poste a presidio dei trattamenti di dati personali;

Le attività saranno erogate nelle seguenti modalità:

- Definizione del perimetro di azione e analisi dell'as is.
- Hardware & Software Assessment attraverso un Asset Inventory ed analisi delle risorse definite al punto a) con un particolare focus a quelle coinvolte nel processo di risk management.
- Analisi delle vulnerabilità dei sistemi, delle applicazioni coinvolte e identificazione del livello di conformità allo scopo di un aggiornamento dei processi di gestione dei flussi.

In questa fase verranno identificate le vulnerabilità ad alto rischio, comprese quelle che derivano da una combinazione di vulnerabilità a basso rischio, mediante procedure automatiche e mediante procedure che richiedono conoscenze specifiche. A questo scopo, saranno utilizzati dei tool automatici, obbligatoriamente i **software Qualys e Checkmarx pena esclusione** , i quali, effettuando una lunga serie di controlli su ogni singolo sistema o applicazione, permettono di conoscere dettagli riguardanti la loro configurazione e l'eventuale presenza di vulnerabilità

Rilasci

Nella tabella sottostante vengono elencati i rilasci necessari per la suddetta attività.

Rilasci per la Gap analysis Tecnologica	Descrizione
Documento Gap analysis tecnologica	esposizione delle interviste effettuate e l'evidenza delle criticità.

Documento di Valutazione rischi tecnologica	Serve a valutare non solo per gli aspetti generali di sicurezza, ma anche per implementare le tecniche di Backup, di Business Continuity.
Documento dei Requisiti IT	• Garantire modalità operative sicure per correlare e collegare i dati con altre basi di dati • Garantire lo sviluppo sicuro del codice sorgente degli applicativi • Garantire modalità sicure di comunicazione dei dati personali tra le direzioni aziendali coinvolte nel trattamento • Supportare l'IT Department nella software selection delle soluzioni informatiche e per l'evoluzione delle applicazioni in ottica adeguamento al GDPR • Supportare l'IT Department del committente nel rafforzamento delle misure di sicurezza poste a presidio dei trattamenti di dati personali

Tabella 6 — Gap Analysis Tecnologica – Rilasci

Il team

Il team di professionisti coinvolto nell'operazione dovrà essere composto come in tabella, a pena esclusione:

Figura Richiesta	q.tà	Descrizione Ruolo	Certificazioni Richieste
Tecnici specializzati nell'area ICT Security	➢ = 2	Almeno due tecnici specializzati nell'area ICT Security per la gestione di tutte le attività di security assessment. i tecnici certificati Qualys sono in grado di analizzare ed indirizzare tutte le strategie e politiche di sicurezza al fine di fornire un quadro completo anche sullo stato di adeguamento alle disposizioni tecniche della legge, delle misure adeguate di sicurezza e delle policy/procedure di sicurezza locali e - ove necessario - internazionali/corporate.	Qualys Vulnerability Management (VM);

Tabella 7 — Gap Analysis Tecnologica – Profilo Risorse

Andrà allegate nella Busta B - Offerta Tecnica I Curriculum Vitae dei componenti il Team.

3.1.2 TOW 2: Gap Analysis Procedurale

Scopo dell'assessment è la definizione di un percorso (attività/priorità/massimo sfruttamento di semplificazioni normative) per colmare i gap procedurali individuati ed essere conformi al Regolamento o aver definito le opportune strategie definite dal Regolamento.

Nella Tabella sono riportate le macro attività previste all'interno del TOW 1, sono riportate nella tabella e saranno dettagliate nel seguito del paragrafo

Modalità Operativa	MacroAttività
TOW 2: GAP Analysis Procedurale	Audit conoscitivo
	Verifica degli Adempimenti delle attività e della documentazione

Tabella 8 — Gap Analysis Procedurale – MacroAttività

In sede di **Audit conoscitivo** verranno affrontati i seguenti argomenti:

- Soggetti che effettuano il trattamento;
- Analisi documentale (informative, incarichi, ruoli, competenze);
- Verifica delle misure di sicurezza organizzativa;
- Colloqui con interessati;
- Raccolta e tipologia dei dati trattati;

Partendo dall'analisi dei trattamenti di dati personali, si procederà con la **verifica degli adempimenti delle attività** già svolte e della documentazione presente, allo scopo di:

- accertare lo stato dell'arte;
- individuare eventuali non conformità;
- definire le tipologie ed il livello di eventuali azioni correttive che si ritenessero necessarie;
- individuare le disposizioni normative del Regolamento che risultino non applicabili e documentarne le relative motivazioni, allo scopo di rendere il più agevole possibile l'adeguamento dell'azienda.

Tale attività da svolgere sul campo con esponenti della AMET S.p.A. dovrà essere finalizzata ad arricchire il documento

che verrà rilasciato con attestazioni tese a portare in evidenza le modalità di gestione dei dati ed eventuali punti critici.

In particolare per la verifica dei gap procedurali andranno analizzate approfonditamente le seguenti aree di adempimenti:

- Classificazione dei Trattamenti di dati personali
- Valutazione del rispetto dei principi di data protection
- Progettazione servizi/device/applicazioni nel rispetto della privacy by design e privacy by default
- Individuazione di eventuali processi/trattamenti che necessitano di Valutazione d'impatto sulla protezione dei dati e suggerimenti su quando/come realizzarla
- Valutazione di effettiva necessità di dotarsi di un Data Protection Officer (DPO)
- Definizione delle misure di sicurezza delle informazioni in linea con le best practices internazionali
- Policy sull'utilizzo degli strumenti informatici, di Internet ed e-mail e devices mobili
- Verifica Registro delle attività di trattamento (registro privacy)
- Verifica Trasferimento di dati all'estero
- Analisi della contrattualistica e rapporti in essere per definire la corretta ripartizione delle responsabilità con le terze parti (clienti/fornitori/appaltatori di servizi)
- Verifica Informative privacy e consensi privacy
- Verifica Modalità di esercizio dei diritti degli interessati
- Verifica Diritto alla portabilità dei dati
- Verifica Obblighi privacy in materia di profilazione
- Stato compliance complessiva dei siti web aziendali
- Stato compliance complessiva dei sistemi di videosorveglianza in essere
- Verifica Responsabili/incaricati del trattamento.

Rilasci

Nella tabella sottostante vengono elencati i rilasci necessari per la suddetta attività.

Rilasci per la Gap analysis Procedurale	Descrizione
Documento Gap analysis Procedurale	Esposizione delle interviste effettuate e l'evidenza delle criticità.

Tabella 9 — Gap Analysis Procedurale – Rilasci

Il team

Il team di professionisti coinvolto nell'operazione sarà così composto, a pena esclusione:

Figura Richiesta	q.tà	Descrizione Attività	Certificazioni Richieste
Esperto privacy	➢ = 1	un esperto privacy per il coordinamento ed il controllo delle attività, valutazione di	Comprovata esperienza nel campo della privacy di 5 anni

		profili di responsabilità derivanti dalla non corretta applicazione delle normative e degli adempimenti previsti dalla legge	

Tabella 10 — Gap Analysis Procedurale – Profilo del Team

Andrà allegate nella Busta B - Offerta Tecnica I Curriculum Vitae dei componenti il Team.

3.2 DPO

Il Fornitore dovrà fornire una figura di DPO da inserire nell' organizzazione di AMET SpA, al fine di essere conformi all ' Articolo 37.

La figura dovrà coprire le seguenti funzioni:

- informa e fornisce consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati.

- sorveglia l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo.

- fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento, coopera con l'autorità di controllo, funge da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva, considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo

Figura Richiesta	q.tà	Descrizione Attività	Certificazioni
DPO	1	Data Protection Officer	5 anni di comprovata esperienza nel campo della Privacy

Tabella 11 - Profilo del DPO

La durata del servizio di questa figura sarà di 12 mesi la presenza in AMET S.p.A. sarà di almeno 10 giorni annui.

4 Figure Professionali

L' Impresa deve garantire, per ciascuna Figura Professionale, il rispetto di tutti i requisiti minimi obbligatori, pena la risoluzione del contratto.

Visto il RUP

L'Amministratore Delegato