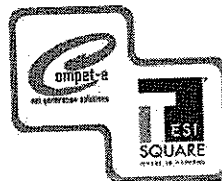


Rif. Ns. Protocollo Interno: OUT/2018/041		 SERINT GROUP consulenza e progetti	Codice documento Allegato Tecnico	
N° Edizione 1	N° Revisione 2		Data Emissione 16/04/2018	Pagina 1/5



Consulenza in materia di
Sicurezza per le Informazioni e
supporto alla Certificazione
ISO/IEC 27001 ed integrazione
degli adempimenti di cui al
Regolamento Europeo GDPR

Allegato Tecnico
Versione di Aprile 2018

Rif. Ns. Protocollo Interno: OUT/2018/041		 SERINT GROUP consulenza e progetti	Codice documento Allegato Tecnico	
N° Edizione 1	N° Revisione 2		Data Emissione 16/04/2018	Pagina 2/5

1 Oggetto della fornitura

Oggetto della fornitura sono le attività di consulenza in materia di sicurezza per le informazioni e supporto alla Certificazione ISO/IEC 27001 ed all'adeguamento al Regolamento UE 2016/679 (per brevità indicato anche come GDPR).

Il Progetto verrà condotto da professionisti Serint Group assieme al partner Compet-e che, assieme, rappresentano il Gruppo di Lavoro.

2 Requisiti della fornitura

- Vincoli temporali: il Gruppo di Lavoro si strutturerà, da parte propria, per erogare i propri servizi di consulenza e supporto nell'arco delle due annualità (2018 e 2019) come già indicato nell'offerta. Nel caso in cui il cliente incontrasse maggiori difficoltà per sviluppare le attività di propria competenza (ad esempio le implementazioni necessarie che emergeranno dopo la prima fase di analisi dei rischi dopo la quale sarà possibile effettuare un piano di maggiore dettaglio) il Gruppo di Lavoro si strutturerà per erogare i propri servizi adattandosi a queste nuove esigenze.
- GDPR: l'adeguamento in tale ambito richiederà almeno 2 mesi di lavoro continuativi
- Localizzazione dei siti: le attività saranno svolte sia presso i vostri che i nostri uffici.

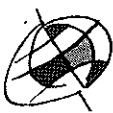
3 Oggetto della consulenza

L'intervento consulenziale si propone di supportarvi nelle tematiche inerenti la Sicurezza delle Informazioni e la relativa Certificazione ISO/IEC 27001 da parte di Ente terzo Accreditato, nonché nelle tematiche inerenti l'adeguamento al GDPR.

Se utile/necessario siamo disponibili a controfirmare appositi accordi di riservatezza (NDA) cui le parti si riferiranno nel corso del Progetto.

4 Modalità di erogazione della consulenza

Le parti definiranno un Piano di Lavoro nel quale verranno definite le attività sviluppate ed il relativo calendario di incontri. Ogni incontro genererà un report (riesame del progetto) delle attività svolte e degli impegni reciproci in modo da tracciare l'evoluzione del Progetto e monitorarne l'andamento. Qualsiasi variazione a tali impegni sarà concordata. All'interno del costo del Progetto è inclusa la licenza per il primo anno di utilizzo del tool informatico (di proprietà del partner Compet-e) per l'elaborazione della Valutazione dei Rischi ma non è incluso il costo della licenza per gli eventuali anni successivi (se di interesse).

Rif. Ns. Protocollo Interno: OUT/2018/041		 SERINT GROUP consulenza e progetti	Codice documento Allegato Tecnico	
N° Edizione 1	N° Revisione 2		Data Emissione 16/04/2018	Pagina 3/5

5 Pianificazione di massima

La pianificazione prevede uno sviluppo nelle due annualità con un piano di lavoro di dettaglio che riguarderà le prime attività del 2018 che sarà confermato o rivisto a seguito della valutazione degli eventuali Gap emersi dopo la prima valutazione dei rischi.

L'inizio lavori è previsto dopo 15 gg. lavorativi dalla data di accettazione della presente offerta. Il progetto sarà articolato in incontri (della durata massima di una giornata lavorativa) nel corso dei quali saranno affrontate almeno le seguenti tematiche:

- obiettivi progettuali;
- attività da svolgere per il raggiungimento degli obiettivi;
- verifica degli obiettivi e delle attività svolte in relazione alle scadenze progettuali;
- verifica dei risultati ottenuti e l'avanzamento del progetto;
- identificazione di eventuali problematiche/varianti rispetto al Progetto iniziale.

6 Fase di implementazione ISO/IEC 27001

Il Gruppo di Lavoro ha stimato un impegno di circa 20gg/u a fronte delle informazioni in nostro possesso. Nel caso in cui nel corso del Progetto dovessero emergere ulteriori necessità condivideremo come procedere.

Nei primi 7 mesi di lavoro verranno svolte almeno le seguenti attività (nei successivi mesi si riprogrammeranno le attività seguenti in funzione dell'avanzamento di Progetto):

Requisiti di riferimento	Pianificazione di massima (mesi)						
	1	2	3	4	5	6	7
1. Contesto							
4.1 Comprendere l'organizzazione e il suo contesto	X						
4.2 Comprendere le necessità e le aspettative delle parti interessate	X						
4.3 Determinare il campo di applicazione del sistema di gestione per la sicurezza delle informazioni	X						
4.4 Sistema di gestione per la sicurezza delle informazioni	X						
2. Leadership e impegno							
5.1 Leadership e impegno	X						
5.2 Politica	X						
5.3 Ruoli, responsabilità e autorità nell'organizzazione	X						
3. Pianificazione							
6.1 Azioni per affrontare rischi e opportunità	X						
6.2 Obiettivi per la sicurezza delle informazioni e pianificazione per conseguirli	X						

Rif. Ns. Protocollo Interno: OUT/2018/041		 SERINT GROUP consulenza e progetti	Codice documento Allegato Tecnico	
N° Edizione 1	N° Revisione 2		Data Emissione 16/04/2018	Pagina 4/5

ALLEGATO TECNICO 27001 + GDPR

Requisiti di riferimento	Pianificazione di massima (mesi)						
	1	2	3	4	5	6	7
4. Supporto							
7.1 Risorse		X					
7.2 Competenza		X					
7.3 Consapevolezza		X					
7.4 Comunicazione		X					
7.5 Informazioni documentate		X					
5. Attività operative							
8.1 Pianificazione e controllo operativi					X		
8.2 Valutazione del rischio relativo alla sicurezza delle informazioni					X		
8.3 Trattamento del rischio relativo alla sicurezza delle informazioni					X		
6. Controlli organizzativi e decisionali							
A.5 Security Policy		X					
A.15 Compliance		X					
A.6 Organization of Information Security		X					
A.8 Human resources security		X					
A.7 Asset management		X					
7. Controlli sistemici							
A.12 Information systems acquisition, development and maintenance					X	X	
A.13 Information Security Management					X	X	
A.14 Business Continuity Management					X	X	
8. Controlli tecnici							
A.9 Physical and environmental security						X	X
A.11 Access control						X	X
A.10 Communications and operations management						X	X
9. Valutazione delle prestazioni							
9.1 Monitoraggio, misurazione, analisi e valutazione							
9.2 Audit interno							
9.3 Riesame di direzione							
10. Miglioramento							
10.1 Non conformità e azioni correttive							
10.2 Miglioramento continuo							
Stage 1 e Stage 2 di certificazione							

Rif. Ns. Protocollo Interno: OUT/2018/041		 SERINT GROUP consulenza e progetti	Codice documento Allegato Tecnico	
N° Edizione 1	N° Revisione 2		Data Emissione 16/04/2018	Pagina 5/5

7 Fase di implementazione GDPR

Il Gruppo di Lavoro ha stimato un impegno di circa 7gg/u a fronte delle informazioni in nostro possesso. Nel caso in cui nel corso del Progetto dovessero emergere ulteriori necessità condivideremo come procedere.

Nei 2 mesi di lavoro verranno svolte almeno le attività illustrate qui di seguito (con eventuale riprogrammazione delle attività seguenti in base all'avanzamento di Progetto):

Requisiti di riferimento	Pianificazione di massima (mesi)	
	1	2
1. Censimento delle attività di trattamento e redazione dell'apposito registro		
1.1 Individuazione dei responsabili dei processi aziendali	X	
1.2 Censimento delle attività di trattamento effettuate in qualità di TITOLARE	X	
1.3 Censimento delle attività di trattamento effettuate in qualità di RESPONSABILE	X	
2. Informative ed acquisizione consenso		
2.1 Verifica perimetro di applicazione / processi ed elaborazione standard	X	
3. Diritti dell'interessato		
3.1 Verifica modalità di gestione e redazione istruzioni per la gestione		X
4. Governance		
4.1 Definizione delle responsabilità relative alla protezione dei dati degli interessati		X
5. Protezione dei dati		
5.1 Risk assessment (valutazione di impatto)		X
5.2 Gap Analysis		X
5.3 Data Breach		X
6. Formazione		X