Capital
Security

Capital Security Srls
Via Montenapoleone 8
20121 Milano

C.F. e P.IVA: 10835430967
Giancarlo.favero@capitalsecurity.it
capitalsecuritysrls@pec.it
Tel: 02.94750 267
Tel: +393355950674

A:
Pregiatissimo Dottore
Arch. Marcellino Arnoldi
Direttore
Ecoisola S.r.l.
Via Carso, 73
24040 Madone (BG)

Prot. CPSOFF230217GF1_EcoisolaArnoldiAnnuale

Milano, 17/02/2023

Oggetto:

- Assunzione del ruolo e responsabilità di Data Protection Officer, ai sensi degli artt. 37, 38 e 39 del GDPR – Regolamento Europeo 2016/679
- Gestione completa degli adempimenti previsti da GDPR – Regolamento Europeo 2016/679
- Gestione completa degli adempimenti previsti dal D.Lgs. 196/2003 così come modificato dal D.Lgs. 101/2018
- N. 36 Scansioni di vulnerabilità su Vostro sito web e su altri indirizzi ip direttamente raggiungibili da internet, ai sensi dell'art. 32 del GDPR
- Formazione specialistica a tutto il Vostro personale
- Garanzia assicurativa fino a 20.000,00 Euro in caso di sanzioni comminate per violazione del GDPR o del D.Lgs. 196/2003

Gentile Arch. Arnoldi,

come da accordi siamo lieti di sottoporre alla Vostra cortese attenzione la presente offerta relativa alla gestione di tutti gli adempimenti relativi a quanto in oggetto, per il periodo dal 01/01/2023 fino al 31/12/2023.

Rispetto alla precedente offerta, Vi abbiamo praticato uno sconto del 10%, triplicato il numero di scansioni di vulnerabilità, ed aggiunto una garanzia assicurativa fino a 20.000,00 Euro.

Rimanendo a Vostra disposizione per qualsiasi chiarimento si rendesse necessario, ringraziamo anticipatamente per l'attenzione e l'opportunità e rimaniamo in attesa di un Vostro graditissimo cenno di riscontro.

Cordialmente,

dott. Giancarlo Favero
Direttore
Capital Security Srls
Via Montenapoleone, 8
20121 Milano

1. **Assunzione ruolo e responsabilità di Responsabile della Protezione dei Dati (RDP o "Data Protection Officer"), ai sensi ed in ottemperanza a quanto previsto dagli artt. 37, 38 e 39 del Regolamento Europeo**

Si prevede lo svolgimento delle seguenti attività:

- adempiere a quanto previsto dall'art. 37 comma 1 lettera a) del Regolamento UE che prevede la nomina del **Responsabile della Protezione dei Dati** ("Data Protection Officer")
- vigilare sull'operato di responsabili ed incaricati del trattamento relativamente alla corretta esecuzione delle istruzione contenute in lettere di nomina, mansionari, regolamenti, disposizioni operative etc.
- fornire pareri tecnico – legali in merito all'impatto che le nuove tecnologie (es. dati in cloud) e le nuove procedure operative avranno sulla protezione dei dati
- affiancare il Titolare del trattamento al fine di informarlo e fornire consulenza specialistica relativamente agli obblighi derivanti dal Regolamento UE, da successivi Codici di Comportamento e Schemi di Certificazione emessi dall'Autorità Garante
- valutare la fondatezza e la liceità di richieste di accesso ai dati personali e di esercizio del diritto all'oblio esercitate dagli interessati
- fornire supporto in fase ispettiva, qualora l'Istituto fosse oggetto di ispezione o verifica da parte dell'Autorità Garante per la Protezione dei Dati Personali, della Guardia di Finanza, della Polizia Postale o più in generale delle Autorità competenti
- valutare se sussistano i presupposti per la notificazione di un evento di tipo "data breach"; se del caso, compilare il relativo modello e provvedere alla notificazione al Garante
- eseguire la valutazione dei rischi inerenti al trattamento dei dati personali
- informare il Titolare ed i referenti circa le previsioni normative e le procedure da adottare per non incorrere nelle violazioni e nelle conseguenti sanzioni.

2. **Gestione completa degli adempimenti previsti da GDPR – Regolamento Europeo 2016/679 e dal D.Lgs. 196/2003, così come modificato dal D.Lgs. 101/2018.**

Si prevede lo svolgimento delle seguenti attività:

- ricognizione della situazione attuale in termini di:
  - Struttura organizzativa
  - Banche dati trattate

  - Architettura hardware e software
- predisposizione del Registro dei trattamenti
- data Protection Impact Assessment, comprensivo di analisi dei rischi relativi a:
  - aspetti legali, normativi e organizzativi
  - luoghi fisici
  - risorse hardware
  - risorse logiche
  - accessi ad Internet
  - risorse dati (cartacei ed elettronici)
  - trattamenti effettuati mediante architetture in cloud
- individuazione delle misure di sicurezza
- stesura del piano di attuazione delle misure di sicurezza
- revisione processi, sistemi e modulistica in ottica di Privacy by Design e Privacy by Default
- predisposizione nuove informative
- predisposizione lettere di nomina per le varie figure previste dal GDPR e quelle ritenute comunque necessarie a fronte di analisi dei rischi e registro dei trattamenti (Titolare, Responsabile, Incaricato, Custode delle Password, Amministratore di Sistema, Azienda esterna, Consulenti o collaboratori esterni)
- predisposizione procedure operative:
  - Riscontro all'interessato
  - Diritto all'oblio
  - Gestione delle password
  - Profilazione degli utenti
  - Smaltimento e riutilizzo dei supporti di memorizzazione e strumenti elettronici
  - Gestione del salvataggio e ripristino dei dati
  - Altre procedure operative
- predisposizione del Regolamento per il corretto utilizzo degli strumenti informatici e telematici.

3. Trentasei scansioni di vulnerabilità su sito web e sugli indirizzi ip direttamente esposti su internet

Il servizio prevede l'esecuzione di tre scansioni di vulnerabilità con cadenza mensile, con uno strumento professionale di livello enterprise, al fine di individuare vulnerabilità e configurazioni poco sicure. Alla fine delle scansioni di vulnerabilità Vi verranno inviati i report dettagliati prodotti dalla piattaforma di vulnerability assessment, contenenti la descrizione dettagliata delle vulnerabilità riscontrate e le attività da svolgere per la loro risoluzione.

4. Corsi di formazione specialistica al personale

4.1 Caratteristiche e peculiarità degli interventi formativi

Si prevede di tenere ogni anno una sessione di formazione specialistica in presenza presso la Vostra sede oppure a distanza, della durata di circa tre ore.

Il taglio dell'intervento è molto interattivo e pratico, mantenendo al minimo l'esposizione della teoria e privilegiando l'esposizione di casi pratici e dando adeguato spazio alle importanti domande dei partecipanti

I corsi sono tenuti da relatori di adeguata seniority e standing, con profonda conoscenza della materia, in grado quindi di rispondere con precisione e cognizione di causa a qualsiasi quesito venga posto.

Alla fine dell'intervento viene rilasciato un regolare attestato di partecipazione, unitamente ad una relazione con l'esplicitazione di indicatori quantitativi e qualitativi di gradimento.

4.2 Possibilità di videoriprendere l'esposizione del relatore

Nel caso l'Ente lo ritenesse utile, viene data la possibilità di effettuare con mezzi propri riprese filmiche (con videocamere, smartphone etc.) dell'incontro formativo, in modo da poter permettere anche a chi era assente o impossibilitato a partecipare, di rivedere il corso e di maturare quindi una certa conoscenza delle problematiche trattate.

4.3 Cinque Ticket per quesiti successivi

Basandoci sulla nostra esperienza, abbiamo visto che spesso i quesiti più importanti e significativi da parte dei partecipanti sorgono qualche giorno dopo aver partecipato al corso e aver di conseguenza "assimilato" il materiale e le nozioni presentate.

Per questo motivo risulta particolarmente utile e gradita la possibilità di porre quesiti di qualsiasi tipo, ai quali viene data risposta in forma scritta nel tempo massimo di tre giorni lavorativi.

Nel costo dell'intervento formativo sono inclusi cinque Ticket.

4.4 Programma del corso

Fermo restando il taglio fortemente interattivo dell'intervento e lo spazio lasciato alle domande poste dai partecipanti, si prevede di seguire il seguente programma:

- Perché il nuovo Regolamento Europeo
- Come "lavora" il nuovo Regolamento: differenze con l'attuale quadro normativo
- Il principio di responsabilizzazione
- La figura del data protection officer
- Il registro dei trattamenti
- Il privacy impact assessment
- Protection by design e protection by default
- L'obbligo di notificazione del data breach
- Le misure di sicurezza
- I codici di condotta e le certificazioni
- Il quadro sanzionatorio.

5. Garanzia assicurativa fino a 20.000,00 Euro in caso di sanzioni comminate per violazione del GDPR o del D.Lgs. 196/2003

Il servizio prevede una garanzia assicurativa (erogata sotto forma di penale) con un massimale fino a 20.000,00 Euro in caso di sanzioni comminate dal Garante per la protezione dei dati personali per violazione del GDPR o del D.Lgs. 196/2003

Valutazione economica

Il servizio ha un costo di **Euro 1.935,00** + IVA 22% per il periodo da 1/1/2023 fino al 31/12/2023, comprensive di tempi e costi di trasferta.

Condizioni di fornitura e pagamento

Prezzi:	netti in Euro, IVA esente
Fatturazione:	In tre tranche: 30% all'ordine, 30% a primo SAL, e 40% saldo finale
Pagamento:	a 30 giorni dalla data di emissione della fattura, a mezzo bonifico bancario, con valuta fissa
Esclusioni:	

Capital
Security

Foro competente:	Per qualsiasi controversia riguardante l'interpretazione e/o l'applicazione delle presenti condizioni di fornitura sarà esclusivamente competente il Tribunale di Milano.
Trattamento dei dati personali:	Il fornitore nel trattamento dei dati di cui venga a conoscenza nello svolgimento della fornitura oggetto del presente ordine, si impegna ad osservare ed a far osservare ai propri dipendenti e collaboratori, le disposizioni di legge vigenti a livello nazionale ed europeo e quanto stabilito negli accordi che governano il rapporto.

Data, timbro e firma per accettazione:

ECOISOLA S.r.l.
24040 MADONE (BG)
Via Carso, 73
Tel. 035.991271 - Fax 035.4943437
Cod. Fisc. e P. IVA 02371570165

28 FEB 2023