IQC S.r.l.
Sede Legale: Via Domenico Morelli, 4/A - 40137 Bologna (BO)
Sede Operativa: Via di Corticella, 181/3 - 40128 Bologna (BO)
P.I. e C.F.: 03332011208 - www.itaqua.it - info@itaqua.it

Bologna, 2019-03-11

Rif. Codice Offerta O1898-19

Spett.le **ASSOCIAZIONE NAZIONALE MEDICI DIREZIONI OSPEDALIERE**
Via Ciro Menotti, 5
40126 - Bologna

C. att.ne Dott. Gianfranco Finzi

OGGETTO: **Offerta per l'attività di consulenza e assistenza tecnica per l'aggiornamento del sistema di gestione della *Privacy*, *Data protection e Cyber Security* in ottica di adeguamento al Regolamento Europeo UE 679/2016**

PREMESSA

IQC è espressione della lunga esperienza che i Soci Fondatori hanno maturato a supporto di istituzioni pubbliche, organizzazioni di produzione e di servizio, per affiancarle nel loro percorso di qualificazione del sapere, saper essere e saper fare italiano sul mercato nazionale ed estero.

IQC offre alle **Imprese di Servizi, alle PP.AA ad alle Organizzazioni Sanitarie**, soluzioni volte alla valorizzazione dei processi interni ed esternalizzati, delle performance prestazionali e delle competenze professionali. L'esperienza del personale IQC garantisce efficienza organizzativa e soddisfazione dell'utente finale privilegiando il coinvolgimento delle parti interessate.

In particolare nel **Settore Sanità**, i professionisti IQC hanno profonda conoscenza del Sistema di Accreditamento Istituzionale della Regione Emilia Romagna, avendo contribuito alla definizione della sua prima edizione oltre ad aver contribuito alla definizione dei Sistemi di Accreditamento Istituzionale delle seguenti regioni: Regione Toscana, Regione Liguria e Regione Umbria. In particolare IQC già dal 2016 ha avviato un percorso tuttora in corso di rivisitazione del procedimento di Accreditamento della Regione Umbria alla luce dei nuovi requisiti delle Inteste Stato-Regione che prevede attività di formazione e assistenza rivolta anche alle strutture sanitarie regionali per il progressivo avvicinamento ai nuovi orientamenti assunti.

Il **4 maggio 2016** è entrato ufficialmente in vigore il **Regolamento 2016/679**, che diventerà definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal **25 maggio 2018**.

Numerose sono le novità introdotte dal Regolamento UE 2016/679, dal principio di ***Accountability*** alla nomina del ***Data Protection Officer***, dall'obbligo di redazione del ***registro dei trattamenti*** alla valutazione di impatto, dall'***obbligo di notifica delle violazioni*** di sicurezza all'obbligo di ***formazione degli incaricati*** al trattamento di dati personali.

Uno degli obiettivi del nuovo Regolamento è quello di introdurre o rafforzare garanzie e diritti per i cittadini, anche grazie alla definizione di responsabilità specifiche previste per imprese e enti.

Il Regolamento è direttamente applicabile e vincolante in tutti gli Stati membri dell'Unione europea e non richiede una legge di recepimento nazionale e tra le organizzazioni che saranno impattate dai nuovi requisiti vi sono le **Strutture sanitarie e relativi fornitori**, che rappresentano contesti critici in cui vengono trattati su larga scala categorie particolari di dati personali (ad esempio dati genetici, biometrici o dati relativi alla salute)

La seguente proposta ha l'obiettivo di:

- Identificare gli eventuali punti di debolezza dell'organizzazione su cui intervenire in maniera prioritaria. Coadiuvando nella definizione di procedure e regole finalizzate al rispetto dei requisiti introdotti dal nuovo Regolamento.

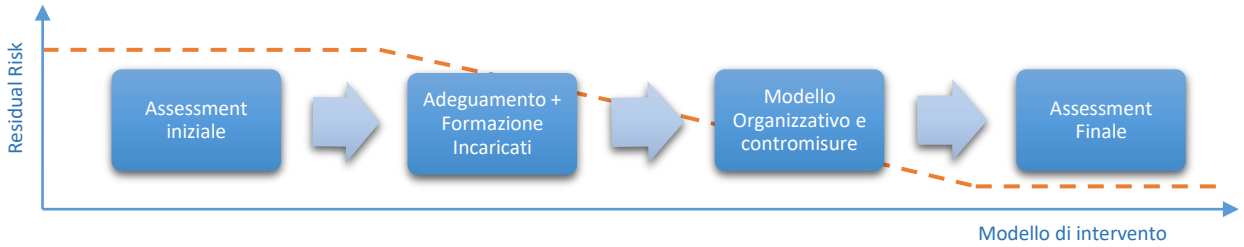
- Creare la opportuna consapevolezza nelle figure identificate dal nuovo Regolamento (es Responsabile della protezione dei dati) oltre che in tutta l'organizzazione.

Dati del cliente:

Ragione Sociale:	**A.N.M.D.O**
Attività:	Attività associativa con finalità scientifica, di tutela legale e sindacale
Addetti:	1 + 500 soci ca.
Incaricati:	2 addetti
ADS:	no

ASPETTI TECNICI e METODOLOGICI

IQC srl propone un modello di intervento che integra elementi di ***compliance legale*****,** di ***data management*** e ***cyber security***-attraverso i seguenti step:



L'intervento mira al riesame del sistema di protezione dei dati, delle infrastrutture IT e delle tecnologie di Cyber *Security* . Verranno valutate le condizioni in essere per attuare procedure di DPIA (Valutazione di impatto) e/o provvedere alla nomina del DPO (**Data Protection Officer**) ove tali adempimenti risultino obbligatori o consigliati in ragione dei trattamenti posti in essere dal Titolare.

In particolare si propone:

- ## Assessment iniziale:

  Intervento mirato e condotto attraverso un confronto con il Referente Privacy e/o IT Manager con la finalità di evidenziare i punti su cui sono presenti carenze tecniche e organizzative. L'intervento è suggerito alle imprese consapevoli di adottare già misure organizzative (e.i DPS aggiornato e un buon

governo sui sistemi informatici) rispetto alle quali è opportuno in maniera mirata valutare i Gap da colmare. L'attività comporterà l'emissione di specifico rapporto di valutazione.

- ## Modello Organizzativo Privacy (MOP)

Apparato procedurale proattivo, in conformità alle disposizioni del Reg.Ue 2016/679, realizzato mediante la verifica, la revisione e l'aggiornamento del Documento Programmatico della Sicurezza se esistente o in alternativa pensato in maniera mirata al contesto organizzativo e ai rischi connessi.

La messa a punto MOP comporterà:

- **Analisi, riesame e classificazione dei dati** oggetto di trattamento;
- **Verifica e aggiornamento delle nomine delle funzioni preposte** al trattamento del dati tra le quali: *Responsabile del Trattamento, Amministratore di Sistema, incaricati al trattamento, DPO (se richiesto);*
- **Verifica ed aggiornamento della valutazione del rischio privacy** mediante l'analisi delle aree e dei locali e degli asset nei quali si svolgono i trattamenti. Verifica delle misure di sicurezza adottate fisica e sicurezza informatica (richiamo al manuale delle contromisure);
- **Adeguamento delle informative** al trattamento dei dati (dipendenti/clienti/fornitori) e verifica/introduzione di criteri per stabilire il periodo di conservazione dei dati;
- **Riesame/Predisposizione dei contratti** con i Responsabili del Trattamento e /o soggetti esterni indirettamente coinvolti
- **Verifica della legittimità del trattamento** dei dati on line mediante siti web (informativa e raccolta del consenso), redazione della policy privacy ed informativa al trattamento dei dati;
- **Verifica/aggiornamento Mansionario Privacy** e **predisposizione dei registri** delle attività di trattamento (Titolare e Responsabile) se necessari;
- **Formazione delle funzioni aziendali preposte al trattamento dei dati** (incaricati) presso impresa. Rilascio di Digital Badge (www.iqcbox.com);
- **Formazione e affiancamento al DPO** (*Data Protection Officer*); con rilascio di Digital Badge;
- **Creazione della procedura per il riscontro delle istanze degli interessati**;
- **Predisposizione della procedura di violazione (data breach)** e della eventuale comunicazione della violazione ai soggetti interessati
- **Verifica e implementazione delle policy di utilizzo di dispositivi portatili** (notebook, Tablet, smartphone ecc) se presenti;

- ## Manuale delle Contromisure (MC)

Analisi del sistema informativo, del flusso dei dati e delle misure di sicurezza adottate**,** con il coinvolgimento della funzioni interessate (i.e. IT manager, amministratore di sistema, responsabile del trattamento, ecc).

L'analisi e le contromisure verranno condotte, per quanto applicabile alla organizzazione, seguendo le disposizioni della norma ISO/IEC 27001:2014 in particolare si porrà particolare attenzione a:

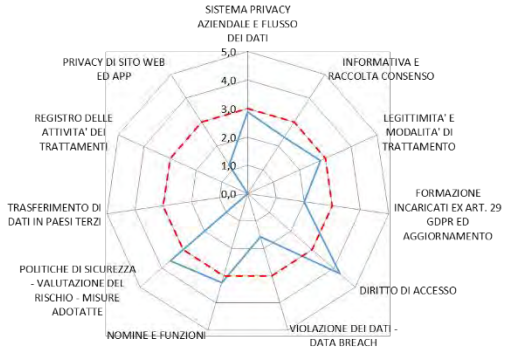
- Gestione degli Asset (HW, SW e Licenze)

- Classificazione delle informazioni
- Controllo degli accessi
- Crittografia
- Sicurezza fisica e ambientale della infrastruttura HW e SW
- Sicurezza delle informazioni nella gestione della continuità operativa (Antivirus, Firewall ecc)
- Sicurezza delle comunicazioni interne ed esterne IDS (Intrusion detection systems)/IPS(Intrusion prevention systems),
- Gestione dei sistemi HW e SW
- Sicurezza delle informazioni nelle relazioni con i fornitori
- Gestione degli incidenti relativi alla sicurezza delle informazioni e dei miglioramenti

Verranno valutate eventuali azioni di *Vulnerabily Assessment*, *Penetretion Test*, *Stress Test*

- **Assessment finale.**

Verifica della efficacia delle soluzioni proposte e della loro corretta implementazione e applicabilità attraverso con rilascio di apposito **rapporto di valutazione**



- **Mantenimento del Sistema Privacy**

In vista delle future disposizioni dell'Autorità Garante, IQC si rende disponibile a seguirvi nella gestione e mantenimento del Sistema Privacy e Data Protection prevendendo interventi quali:

- Formazione alle eventuali nuove figure di **Incaricati;**
- Adeguamento delle procedure a tutela del cliente;
- Formazione al Responsabile Privacy e Data Protection Officer (nel caso la figura si rendesse in futuro necessaria);
- Valutazione e aggiornamento e corretta applicazione delle procedure, Trattamenti e gestione dei rapporti con **Responsabili del trattamento esterni;**
- Valutazione della efficacia delle misure di sicurezza tecnico-organizzative/funzionali adottate;
- Eventuale assistenza nei rapporti con **l'Autorità Garante;**
- Assessment annuale;

- **Mantenimento con servizio di Responsabile della protezione dei dati (DPO) – (opzionale)**

  Oltre agli interventi di cui sopra, IQC, su richiesta del cliente si propone di assumere il ruolo di DPO, in osservanza di quanto previsto dall'art. 39, paragrafo 1, del Regolamento, con il mandato di svolgere, in piena autonomia e indipendenza, i seguenti compiti e funzioni:

  - informare e fornire consulenza al Titolare, ai Responsabili del Trattamento ed agli incaricati, in merito agli obblighi derivanti dal Reg. UE 2016/679, dalla normativa vigente in materia di protezione dei dati personali nonché dai provvedimenti e pareri dell'Autorità Garante;
  - fornire un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Reg.UE 2016/679;
  - cooperare con il Garante per la Protezione dei Dati Personali, interagendo in caso di richieste di informazioni o effettuazione di controlli ed accessi da parte dell'Autorità;
  - fungere da punto di contatto con il Garante per la Protezione dei Dati Personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Reg.UE 2016/679, ed effettuare, se del caso, consultazioni relativamente a qualsivoglia altra questione rilevante in materia di protezione dei dati personali;
  - informare prontamente il Titolare di ogni questione rilevante ai fini della legge vigente in materia di protezione dei dati personali;
  - coadiuvare il Titolare nell'attività di aggiornamento del Registro delle Attività di Trattamento tenuto dal Titolare. Tale attività di aggiornamento dovrà essere svolta da soggetti terzi sotto l supervisione del DPO, non essendo la stessa oggetto del presente incarico.
  - gestire tempestivamente i reclami degli interessati e le eventuali istanze del Garante nel rispetto della "Procedura di Riscontro delle Istanze degli Interessati" predisposta dal Titolare;
  - verificare che i dati personali oggetto del trattamento non siano comunicati o diffusi in Italia o che non siano trasferiti, comunicati, diffusi o altrimenti trattati all'estero (Paesi Ue ed extra Ue), senza la preventiva autorizzazione del Titolare;
  - comunicare prontamente e per iscritto al Titolare il verificarsi di una violazione dei dati personali ai sensi e per gli effetti degli artt. 33 s.s. Reg. UE 2017/679 e provvedere, qualora se ne ravvisi l'obbligo, ad eseguire la notifica all'Autorità Garante ed alle eventuali comunicazioni ai soggetti interessati così come prescritto dalla relativa "Procedura di Data Breach", adottata dal Titolare;
  - supervisionare la conservazione della documentazione predisposta dal Titolare in adempimento degli obblighi vigenti in materia di privacy;

PROFESSIONISTI IQC

Le attività saranno condotte sotto la responsabilità di IQC prevedendo il coinvolgimento di professionisti altamente qualificati con competenze specifiche nel settore di intervento della Struttura e con ampia esperienza in materia di sistemi di gestione per privacy e sicurezza delle informazioni, accreditamento e certificazione.

RISERVATEZZA

Quanto verrà a nostra conoscenza in merito alla Vostra organizzazione ed attività sarà da ritenersi strettamente riservato. IQC srl si impegna a mettere in atto le dovute cautele al fine di mantenere la completa riservatezza. IQC srl si riserva comunque il diritto di pubblicizzare a scopo promozionale l'attività svolta.

CONDIZIONI CONTRATTUALI

Qualora l'Impresa decidesse di recedere dal presente contratto prima della conclusione delle attività previste, dovrà darne avviso a IQC srl, mediante lettera raccomandata AR, almeno 15 giorni prima della data in cui il recesso deve avere esecuzione. Resta inteso che in caso di esercizio del diritto di recesso, IQC srl avrà diritto ad un compenso proporzionale all'attività effettivamente svolta sino al momento del recesso e non ancora retribuita.

ATTIVAZIONE DEL SERVIZIO

Il servizio potrà essere attivato a fronte delle sottoscrizione della presente offerta controfirmata per accettazione.

Ringraziando fin d'ora per la cortese attenzione, manifestiamo piena disponibilità per ogni necessità di chiarimento e/o approfondimento anche nell'ambito di un incontro da organizzare presso la Vostra sede.

Cordiali Saluti

L'Amministratore Unico

(Ing. Rodolfo Trippodo)

Timbro e firma per accettazione

A.N.M.D.O. Associazione Nazionale dei Medici delle Direzioni Ospedaliere.