DPR. 1-

Sistema Socio Sanitario
Regione Lombardia
ASST Valtellina e Alto Lario

ALLEGATO ALLA DETERMINAZIONE
N. 638 DEL 26 GIU 2019
COMPOSTO DA N. 16 PAGINE

Direzione Amministrativa
Tel. 0342/521223 – Fax 0342/521914 – e-mail: *direzione.amministrativa@asst-val.it*
PEC: *protocollo@pec.asst-val.it*

01.01.02

Al Direttore
U.O.C. Approvvigionamenti
Dott. Renato Paroli
SEDE

OGGETTO: incarico di Data Protection Officer

L'Azienda ha necessità di conferire un incarico esterno, almeno biennale, per l'attività di Data Protection Officer e l'attività di consulenza.

Si invita la S.V. a procedere nel modo più celere possibile.

Cordiali saluti

Il Direttore Amministrativo
Dr. Andrea De Vitis

A.S.S.T. Valtellina e Alto Lario D.G.R. n. 4497 del 18/12/15

LCG LECIS CANNELLA GRASSI
STUDIO LEGALE ASSOCIATO

DPR. 2

Ugo Lecis
Giuseppe M. Cannella
Matteo Grassi
Maria Chatzikonstanti
Marco Romanelli
Paolo De Martino
Alberto Capitani
Maria Benedetta Agus
Benedetta Colombo
Gabriella Isgrò
Antonio Bambino
Ilaria Gandini
Carlo Ferrucci
Giuliana Sonzogni
Giulia Garavana
Barbara Barbarino
Luigi Colantuoni
Vinna Lodi
Edoardo Asta
Alessandra Coletti
Federica Catalano
Alessia Lipari
Teresa Breschi
Caterina Panzeri
Francesco Spanò
Rebecca Minini
Camilla Gregori
Andrea Randazzo

Milano, 6 giugno 2019

Spett.le
ASST DELLA VALTELLINA E ALTO LARIO
Via Stelvio, 25
23100 Sondrio

Proposta per l'affidamento dell'incarico di DPO e dei servizi di consulenza finalizzata a garantire l'adeguamento dell'ASST Valtellina e Alto Lario al nuovo Regolamento Europeo sulla privacy n. 679/2016.

PROGETTO GESTIONALE E ORGANIZZATIVO DEL SERVIZIO

Egregi Signori,

facendo seguito alla Vostra richiesta del 3 giugno u.s. sottoponiamo alla Vostra attenzione la proposta per l'attività di consulenza *Data Protection Officer*.

1. OGGETTO DELLA PROPOSTA

La presente proposta ha per oggetto lo svolgimento dell'incarico di DPO ai sensi del Regolamento Europeo n. 679/2016 (di seguito "GDPR"), e precisamente:

1.1 Attività di Data Protection Officer (DPO)

In qualità di DPO, lo scrivente svolgerà le prestazioni previste dall'art. 39 GDPR, come di seguito specificate:

- pianificazione e gestione di un Piano di attività annuale;
- definizione di un piano di flussi informativi con scadenza trimestrale;

20122 Milano
Viale Bianca Maria, 23
Tel. +39 02.76398404
Fax +39 02.76006457

00193 Roma
Via M. Clementi, 18
Tel. +39 06.69352804
Fax +39 06.69352791

e-mail: lcg@lexlecis.com

Part. IVA 05127440963

www.lexlecis.com

- informazione e consulenza al Titolare del trattamento, nonché al Referente privacy interno, in merito agli obblighi derivanti dal GDPR e da altre disposizioni nazionali in materia di protezione dei dati personali, attraverso l'invio di un report trimestrale e rapporti interpersonali;
- partecipazione a riunioni e incontri di pianificazione aziendale nei quali è utile la sua presenza, anche al fine di reperire informazioni inerenti alle attività con impatto sui dati personali trattati;
- vigilanza sull'osservanza del GDPR, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati, nonché delle politiche del Titolare 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;
- svolgimento di audit periodici, definiti all'interno di un piano annuale, al fine di verificare l'osservanza del GDPR e di altre disposizioni nazionali in materia;
- supporto dell'ASST nella gestione documentale in materia di protezione dei dati anche ai fini di esibizione a terzi e allo scopo di dimostrare le attività poste in essere dal Titolare in linea con il principio di "accountability";
- cooperazione con il Garante italiano per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva, il supporto nell'accesso da parte del Garante ai documenti e alle informazioni necessarie per l'adempimento dei suoi compiti, nonché ai fini dell'esercizio dei suoi poteri d'indagine, correttivi, autorizzativi e consultivi;

- consultazione del Garante italiano per la protezione dei dati personali relativamente ad ogni altra questione;
- relazione periodica almeno semestrale circa le attività del Garante della privacy italiano d'interesse per l'Azienda (es. pareri, provvedimenti, linee guida, ecc.);
- punto di contatto per gli Interessati in merito al trattamento dei loro dati personali, anche particolari, e all'esercizio dei diritti previsti dal GDPR;
- supporto nella tenuta del registro delle richieste degli Interessati, nonché gestione dei riscontri agli Interessati;
- cooperazione e supporto del Responsabile della Prevenzione della Corruzione, Trasparenza e Internal Auditing, dei singoli RUP aziendali e delle altre strutture organizzative nella valutazione delle richieste che dovessero pervenire da parte degli Interessati;
- disponibilità a partecipare a gruppi di lavoro o organismi aziendali in ambito compliance con impatto sugli aspetti privacy;
- analisi dei rischi inerenti al trattamento e definizione di un ordine di priorità nella risoluzione delle problematiche relative ai trattamenti che presentino maggiori rischi tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo;
- redazione, se richiesto, di pareri in merito alla valutazione d'impatto sulla protezione dei dati, supporto nello svolgimento della stessa ai sensi dell'articolo 35 del GDPR ed eventuale riesame;
- disponibilità a svolgere accessi, almeno una volta al mese, presso la sede dell'Azienda e a evadere le richieste di natura giuridica in materia di privacy provenienti dall'ASST entro le 48 ore dalla

ricezione di e-mail o telefonate. A tal fine, sarà istituito un canale di comunicazione privilegiato al fine di garantire pronta e tempestiva assistenza, secondo quanto previsto nel Piano di attività, tenuto conto che il DPO sarà supportato da una struttura organizzativa composta da due professionisti;

- redazione di informative, indicazioni, report e relazioni mensili sull'attività svolta e sul livello di adeguamento al GDPR raggiunto di volta in volta nell'ambito delle sue funzioni;
- supporto nella predisposizione e gestione di specifici audit interni ed esterni;
- programmazione dell'attività di formazione e aggiornamento annuale degli operatori dell'ASST;
- definizione di un flusso informativo sulla formazione erogata;
- analisi dei flussi inviati dal Titolare e/o dai suoi Referenti in relazione alle nuove attività aziendali con impatto sui dati personali;
- supporto al Titolare nella tenuta e nell'aggiornamento del Registro delle attività di trattamento.

Inoltre, nel corso dell'anno solare la fine dell'anno, sarà svolta una simulazione di Data Breach, supportati dalla vostra funzione IT interna, al fine di testare il livello attuale delle misure di sicurezza presenti in Azienda.

1.2 Requisiti del DPO

Lo scrivente, socio fondatore dello Studio LCG, opera, già a far data dal 2000 a favore di enti sanitari e socio-sanitari per quanto riguarda l'adozione dei modelli comportamentali (avendo peraltro supportato 2 progetti pilota), l'analisi dei rischi e il risk management, la sicurezza e salute nei luoghi di lavoro, nonché la *compliance* in materia di privacy.

A titolo esemplificativo, il medesimo è stato nominato DPO del Gruppo Italdesign (Italdesign Giugiaro SpA, Italdesign Giugiaro SI.U, Italdesign Giugiaro GmbH), dell'Ospedale San Pellegrino di Castiglione delle Stiviere, dell'Ospedale Civile di Volta Mantovana e dell'ASST dei Sette Laghi (Varese).

Lo Studio LCG, sotto il suo coordinamento, ha implementato – e sta implementando – numerosi sistemi privacy in favore di soggetti pubblici (non economici), strutture sanitarie accreditate con il Servizio Sanitario Nazionale alla luce del nuovo regolamento n. 2016/679/UE (GDPR).
Tra le più importanti attività, si segnalano:

- ASST dei Sette Laghi;
- Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico di Milano;
- Fondazione Regionale per la Ricerca Biomedica (F.R.R.B.);
- Fondazione Lombardia per l'Ambiente;
- Fondazione Sviluppo Ca' Granda;
- Ospedale San Pellegrino di Castiglione delle Stiviere;
- Ospedale Civile di Volta Mantovana;
- RINA S.p.a.
- R.S.A. Beata Paola;
- R.S.A. San Pietro;
- R.S.A. Villa Azzurra;
- R.S.A. Fondazione Don Pozzoli Onlus;
- Gemini RX Srl – Diagnostica per immagini;
- Centro Politerapico – Polidiagnostico di Monza;
- CRP – Centro Radiologico Polispecialistico Srl;
- Curie Srl – Diagnostica per immagini e terapia;
- Studio Radiologico Carroccio Dr. Bossi Giuseppino;

- Studio Radiologico Città di Parabiago;
- Ospedale Casa di Cura Villa Esperia;

Lo stesso professionista è attualmente Presidente del Comitato scientifico dell'Associazione *Data Protection Officer* (Asso-DPO), che riunisce diversi esperti di privacy a livello europeo.

Svolge, inoltre, attività di docente in Master universitari e corsi di formazione nelle materie sopra indicate.

Lo scrivente possiede un'ampia conoscenza dei sistemi di gestione attualmente adottati in ambito sanitario.

Sotto il profilo personale si segnala l'elevato standard deontologico che lo contraddistingue, nonché la correttezza, lealtà e integrità di condotta riconosciutagli diffusamente.

Si esclude ogni situazione, anche potenziale, di conflitto di interessi che potrebbe generarsi dallo svolgimento dell'attività di DPO.

Lo scrivente è esperto in materia di anticorruzione e trasparenza e accesso generalizzato. Inoltre, lo stesso ha collaborato a progetti di digitalizzazione di enti pubblici.

1.3 Consulenza e supporto normativo, giuridico, amministrativo e organizzativo in materia di protezione dei dati personali.

Lo scrivente si impegna a effettuare tutte le attività volte a implementare, mantenere e aggiornare il Sistema di Data Protection adottato dall'ASST, nonché tutte quelle necessarie a garantire il costante adeguamento e la conformità al GDPR. In particolare, provvederà ad effettuare le seguenti attività:

- verifica del livello di conformità attuale e misurazione del livello di esposizione dei rischi associati al trattamento dei dati;

- verifica e valutazione dei processi e delle procedure di gestione dei sistemi informativi, degli strumenti per la gestione della sicurezza informatica e dei sistemi di controllo esistenti all'interno dell'azienda;
- mappatura annuale dei trattamenti effettuati, comunicati dalle singole strutture, analisi della tipologia dei dati trattati, delle finalità del trattamento, del periodo di conservazione degli stessi, delle categorie di interessati, ecc. al fine di implementare il Registro dei trattamenti;
- aggiornamento e revisione della documentazione e della modulistica privacy rispetto alla normativa vigente (es. informative e consenso al trattamento dei dati);
- aggiornamento e revisione delle clausole contrattuali standard da inserire nei testi dei contratti, degli atti e dei disciplinari di gara;
- supporto nella predisposizione della documentazione privacy relativa a sperimentazioni cliniche e al trattamento di dati di tipo genetico;
- verifica e aggiornamento dei modelli di designazione dei Responsabili e degli Autorizzati al trattamento;
- individuazione di eventuali situazioni di contitolarità e conseguente predisposizione di modelli standard di accordi di contitolarità;
- individuazione dei responsabili esterni e conseguente predisposizione di modelli standard di nomine e contratti disciplinanti i rapporti con tali soggetti (es. fornitori);
- predisposizione di procedure aziendali contenenti istruzioni operative e organizzative per tutte le figure aziendali coinvolte in materia di privacy;

- predisposizione di procedure aziendali per identificare nuovi processi o modificare quelli esistenti (es. corretto utilizzo di internet, posta elettronica, social network e device aziendali da parte dei dipendenti e/o collaboratori dell'Azienda; riprese audio-video all'interno delle strutture sanitarie, newsletter, ecc.), in attuazione del principio della *"privacy by design"*;
- individuazione e valutazione dei rischi connessi al trattamento di dati personali e attuazione di misure tecniche e organizzative adeguate a garantire e dimostrare che i trattamenti sono effettuati conformemente al GDPR;
- individuazione e valutazione dell'impatto dei trattamenti sui diritti e sulle libertà degli Interessati (DPIA) e conseguente predisposizione degli strumenti ritenuti più idonei per contrastarli o comunque ridurli al minimo;
- predisposizione e implementazione delle procedure per la gestione delle richieste di accesso e di esercizio degli altri diritti da parte degli Interessati;
- individuazione di azioni correttive, tecniche e organizzative, volte a ridurre i gap di tipo normativo e informatico;
- supporto nell'individuazione degli Amministratori di Sistema interni o esterni, ai sensi del Provvedimento del Garante del 27 novembre 2008;
- analisi del sito web e predisposizione di adeguate Privacy policy e Cookie policy;
- analisi e aggiornamento del sistema di videosorveglianza;
- supporto nella predisposizione degli atti di gare necessari per effettuare una "Software selection" al fine di acquisire un gestionale privacy conforme al GDPR.

Le suddette attività verranno svolte sulla base del Cronoprogramma allegato (All. 1), tenendo in particolare considerazione le problematiche che richiedono pronta assistenza in virtù dei rischi connessi alle attività di trattamento eseguite dall'Azienda. Si resta a disposizione per modificare l'ordine di priorità oggetto della presente proposta sulla base di particolari esigenze e urgenze di volta in volta rappresentate dai Vostri Referenti privacy.

1.4 Attività di formazione

La presente proposta comprende l'attività di formazione obbligatoria a favore del Management aziendale, dei Dirigenti di struttura, del personale dipendente e/o dei collaboratori coinvolti nel sistema di Data protection, con la previsione di corsi di diverso livello per le figure interessate, conformemente alle diverse responsabilità in materia di sicurezza e protezione dei dati personali. Tale formazione avverrà preferibilmente mediante l'erogazione di lezioni in aula.

L'attività formativa avrà ad oggetto i seguenti argomenti:

- principi del Regolamento UE/679/2016, anche alla luce delle Linee Guida emanate dal Gruppo di lavoro Art. 29 e dal Garante della Privacy;
- misure di sicurezza, organizzative e tecniche adottate dall'Azienda e riferimenti specifici ai processi e procedure adottate;
- simulazione di casi concreti con impatto in materia privacy, i quali saranno analizzati dai partecipanti suddivisi in gruppi con il supporto del DPO. Durante l'esercitazione, il DPO illustrerà brevemente la fattispecie oggetto di analisi e fornirà a ciascun gruppo un documento da utilizzare come linea guida per la risoluzione del quesito posto. A conclusione, il DPO esaminerà

con i presenti le soluzioni da loro proposte e li supporterà nell'individuazione delle *best practices* da utilizzare.

- somministrazione di un questionario di verifica e apprendimento.

Nel corso del secondo ed eventuale terzo anno, lo Studio LCG si impegna a programmare tanti eventi formativi quanti saranno ritenuti necessari, in accordo con i Vostri Referenti interni, per raggiungere tutti i dipendenti dell'ASST coinvolti nel Sistema di *Data protection* (operatori di area sanitaria, socio-sanitaria e tecnico amministrativa), che saranno raggruppati per classi omogenee in relazione ai trattamenti di dati personali svolti dagli stessi.

2. *TEAM DI LAVORO*

Nello svolgimento delle attività sopra descritte, lo scrivente sarà supportato da un team di lavoro costituito, oltre dal coordinatore, da altri professionisti dello Studio LCG.

Ogni professionista impiegato ha altresì una specializzazione in altre branche del diritto che intersecano la materia della privacy, quali il diritto del lavoro, il *risk management*, la sicurezza sui luoghi di lavoro, il diritto sanitario e la *compliance* aziendale. Ciò a riprova della multi-disciplinarità dello Studio LCG.

3. *CORRISPETTIVO BIENNALE*

Il corrispettivo proposto dallo scrivente per l'affidamento dell'incarico di DPO e dei servizi di consulenza finalizzata all'adeguamento dell'ASST al GDPR, per l'intera durata dell'appalto, è pari a complessivi € 38.000,00 (euro trentottomila/00), oltre C.P.A. 4% e I.V.A. 22%.

Tale corrispettivo dovrà essere versato secondo le modalità ed alle scadenze da Voi comunicate.

4. *VARIAZIONI DEL CONTRATTO*

Le Parti possono concordare variazioni nella quantità delle prestazioni, con un limite in rialzo e in ribasso fino ad un massimo del 20% dell'importo contrattuale previsto. Oltre tale limite. Lo Studio LCG avrà diritto di risolvere il contratto.

5. *RISERVATEZZA E CONFIDENZIALITÀ*

Ai professionisti impegnati nel presente progetto inclusi soci, collaboratori, dipendenti è fatto divieto di divulgare informazioni riservate.

Le relazioni, lettere, informazioni e pareri che potranno essere forniti all'Azienda nel corso del presente incarico sono di carattere confidenziale, consegnati unicamente ai fini del presente lavoro.

Gli obblighi e i divieti di cui sopra non si applicano alle informazioni:

- che sono o diventano di dominio pubblico per motivi diversi da violazioni dei paragrafi precedenti;
- che vengono divulgate da altre fonti non assoggettate a vincoli di riservatezza;
- per le quali è richiesta la comunicazione da norme professionali o di legge, ovvero da Autorità alle quali non si possa opporre rifiuto.

6. *COPERTURA ASSICURATIVA*

Il professionista dichiara di aver stipulato adeguate polizze assicurative a copertura dei rischi derivanti da Responsabilità professionale:

- quale DPO (compagnia Lloyd's, polizza n. DCG00175549, massimale Euro 2.000.000,00);
- quale consulenza (compagnia Assicurazioni Generali, polizze nn. 370469032 e 370469051, massimale Euro 4.000.000,00).

7. *DURATA DELL'APPALTO*

L'appalto avrà la durata di **due anni (24 mesi)** a decorrere dal primo giorno del mese successivo all'intervenuta esecutività del provvedimento di aggiudicazione. Al termine del periodo sopracitato, l'ASST si riserva ai sensi dell'art. 35 comma 4 d.lgs. 50/2016 di proseguire il servizio per ulteriori 12 mesi. La volontà di avvalersi della facoltà di rinnovo dovrà essere comunicata almeno 30 giorni prima della scadenza del contratto a mezzo PEC.

Rimango a Vostra disposizione per qualsiasi ulteriore chiarimento o informazione riteniate utile.

In attesa di un cortese riscontro, porgo i più cordiali saluti.

Avv. Giuseppe Cannella

Si allega:

- Cronoprogramma delle attività di consulenza (All. 1);

All. 1

LCG

CRONOPROGRAMMA

	Attività	Tempistiche
Verifica dei livelli di conformità sussistenti	Intervista dei Referenti di funzione coinvolti nel trattamento dei dati Individuazione dei trattamenti eseguiti e delle categorie di dati, di Interessati coinvolti, delle finalità perseguite e del periodo di conservazione dei dati Individuazione dei rischi per gli Interessati connessi ai trattamenti eseguiti Valutazione dei processi e delle procedure di gestione dei sistemi informativi, sicurezza informatica e controllo Individuazione di misure tecniche e organizzative che permettano di ridurre i gap di tipo normativo e informatico	Entro il 30/11/2019
Verifica e aggiornamento della documentazione e della modulistica privacy.	Verifica delle informative rese agli Interessati e loro implementazione ai sensi del GDPR. Verifica dei moduli utilizzati per raccogliere il consenso degli Interessati, ove necessario, loro implementazione ai sensi del GDPR. Aggiornamento e revisione delle clausole contrattuali standard, degli atti e dei disciplinari di gara.	Entro il 28/02/2020

Elaborazione di un organigramma privacy.	Analisi del sito web e predisposizione di Privacy policy e Cookies policy Verifica degli atti di nomina interni (soggetti autorizzati e referenti interni) e loro implementazione ai sensi del GDPR. Verifica di eventuali situazioni di contitolarità ex art. 26 GDPR. Verifica di eventuali Responsabili esterni del trattamento e predisposizione degli atti di nomina. Individuazione e nomina degli Amministratori di Sistema interni e/o esterni	Entro il 31/03/2020
Predisposizione di procedure aziendali	Istruzioni operative e organizzative per i soggetti interni e per tutte le figure aziendali coinvolte nei trattamenti di dati personali Corretto utilizzo di internet, posta elettronica, social network e device aziendali da parte dei dipendenti e/o collaboratori dell'Azienda Riprese audio-video all'interno delle strutture sanitarie e/o invio di newsletter Gestione delle richieste di accesso e di esercizio degli altri diritti da parte degli Interessati Analisi e aggiornamento del sistema di videosorveglianza	Entro il 30/04/2020 Entro il 31/03/2020

	Supporto nella definizione del Registro dei trattamenti	
	Supporto nell'individuazione e valutazione dei rischi connessi al trattamento.	
Valutazione dei rischi e dell'impatto dei trattamenti di dati personali.	Valutazione della necessità di svolgere eventuali DPIA.	Attività avviata al momento di assegnazione dell'incarico e conclusa entro 12 mesi.
	Supporto nell'esecuzione della DPIA, per i trattamenti che presentano un rischio elevato per gli Interessati	
	Definizione di misure tecniche e organizzative che permettano di ridurre il rischio connesso al trattamento	
Mappatura annuale dei trattamenti effettuati, categorie di dati, finalità, periodo di conservazione e categorie di Interessati	Interviste periodiche dei Referenti di funzione coinvolti nel trattamento dei dati	Attività avviata entro il 31/12/2019 e svolta per tutta la durata dell'incarico.
	Istituzione di appositi flussi informativi da parte dei Referenti di funzione coinvolti nel trattamento dei dati	Trimestrali a decorrere dal 31/12/2019
	Revisione e aggiornamento del Registro dei trattamenti	Attività avviata al momento di assegnazione dell'incarico e svolta per tutta la sua durata.