PRESENTAZIONE

Dati Anagrafici:

Avv. Luca De Toffani
Vicolo Abate Della Piazza n. 8/c
36015 Schio (VI)
www.studiolexin.it
l.detoffani@studiolexin.it
0445 532551
Data di Nascita : 22/03/1966
C.F.: DTFLCU66C22L157L

Competenze specialistiche:

- Avvocato dal 1999 e Cassazionista dal 2012, occupandomi in particolare di tutela dei dati personali e Cybersicurezza, sia a livello consulenziale, sia in ambito giudiziale, per Enti pubblici ed aziende.
- "Privacy Officer" e "Consulente della Privacy" CERTIFICATO con TÜV in conformità alla norma ISO/SEC 17024:2012.
- "Responsabile Protezione dei Dati Personali – R.P.D. (D.P.O. – Data Protection Officer) CERTIFICATO con INTERTEK in conformità alla norma UNI 11697:2017.
- "Lead Auditor di sistemi di gestione per la sicurezza delle informazioni UNI CEI ISO/IEC 27001:2014" ATTESTATO da CSQA (AICQ – SICEV).
- MASTER universitario di secondo livello in Cybersecurity presso l'Università degli Studi di Milano (anno accademico 2020-2021), mutuato dai Dipartimenti di Informatica, di Economia e Management e Scienze Giuridiche, con qualifica di CISO (Chief Information Security Officer) e DPO (Data Protection Officer).
- Le mie conoscenze specifiche, quindi, non riguardano solo la normativa europea e nazionale in materia di privacy (compresi i provvedimenti dell'Autorità Garante italiana e dell'EDPB europeo) e la giurisprudenza di settore, ma anche le prassi e le metodologie in materia di protezione delle informazioni (COBIT, ENISA, misure di sicurezza AgID, Nist e ISO 27000), come anche l'aspetto informatico del trattamento dei dati e di processo.
  In relazione a quest'ultimo aspetto preciso di aver frequentato numerosissimi corsi, anche di alta formazione, sulla protezione dei dati personali per responsabile della protezione dei dati e, da ultimo, un corso per giuristi esperti nella trasformazione digitale della P.A.

Esperienze professionali:

- Dal 2018 ricopro/ho ricoperto il ruolo di Responsabile della Protezione dei Dati di alcuni Comuni del Vicentino:
  Comune di Schio, Comune di Santorso, Comune di Torrebelvicino, Comune di Dueville, Comune di San Pietro Mussolino, Comune di Fara Vicentino, Comune di Monte di Malo, Comune di Monticello Conte Otto, Comune di Montecchio Precalcino, Comune di Bressanvido, Comune di Montegaldella, Comune di Piacenza D'Adige, Comune di Zovencedo, Comune di Valli del Pasubio, Unione Montana Pasubio – Alto Vicentino;
- Dal 2018 ricopro l'incarico di Responsabile della Protezione dei Dati dei seguenti Consorzi: Consorzio di Polizia Locale Nord-Est Vicentino, Consorzio di Polizia Locale Valle Agno;
- Dal 2018 ricopro l'incarico di Responsabile della Protezione dei Dati dell'Istituto I.P.A.B. La C.A.S.A di Schio;
- Dal 2022 sono Responsabile della Protezione dei Dati di VIACQUA S.p.A.
- Consulente Privacy e Responsabile della Protezione dei Dati di numerose Aziende private e associazionistiche in ambito sanitario ed informatico.

- La mia esperienza maturata presso gli Enti Pubblici in cui sono D.P.O. unita alla mia competenza come CISO (Chief Information Security Officer), in particolare con i sistemi di gestione che si occupano di sicurezza delle informazioni (COBIT, NIST, ENISA, ISO 27000 e Misure di sicurezza AgID) mi porta ad applicare questi framework per la gestione dei dati personali nel rispetto della normativa specifica e nella massima sicurezza, come richiesta dai predetti sistemi di gestione internazionali.

Progetto operativo:

- Le azioni che intendo promuovere come RPD sono relative ai compiti previsti per questa funzione, riportati qui di seguito.
- Informazione e consulenza per Titolare e incaricati del trattamento, resa sia tramite newsletter periodica sugli obblighi in materia di trattamento, sulle principali novità normative e tendenze applicative europee e domestiche, sia tramite contatto mail - o in presenza presso il Comune - per consulenza puntuale e tempestiva su specifiche questioni per tutto il periodo di erogazione del servizio**, senza limiti quantitativi e/o di orario.**
  Le consulenze saranno scritte e consisteranno in pareri "*pro veritate*" su questioni giuridiche afferenti al trattamento dei dati personali.
- Formazione e sensibilizzazione periodica mirata, per Titolare e tutti gli incaricati di trattamento, diversificata per livello e per tipo di trattamento, al fine di raggiungere il grado di competenza richiesto dalla specifica funzione svolta in materia di trattamento dati.
  Durante gli incontri di formazione, che verranno fatti con le scadenze concordate con l'Ente e comunque in presenza presso il Comune, verrà sottoposto un test di apprendimento che farà parte del "Registro della Formazione" tenuto dal RPD.
  La formazione sarà continua per tutto il periodo di erogazione del servizio.
- Assistenza in caso di "Data Breach" entro il giorno lavorativo successivo alla comunicazione dell'incidente, con indicazione delle modalità operative da seguire da parte del comune ed assistenza per la notifica al Garante (se necessario) e assistenza alla compilazione del "Registro dei Data Breach".
- Sorveglianza dell'applicazione del GDPR e di tutta la normativa in materia di "Protezione dei Dati Personali". Tale attività viene svolta attraverso un "Piano di Audit", concordato con il Comune, che viene svolto in ottemperanza alle previsioni di cui alla UNI ISO 19011 (Linee Giuda per la conduzione di Audit).
  Con tale piano vengono periodicamente auditati a campione tutti i processi di trattamento di dati per verificare sia la conformità delle policy e delle procedure interne alla normativa, sia la concreta applicazione di tali policy e procedure, ciò per tutta la durata dell'incarico.
  L'esito degli Audit determinerà il piano dei miglioramenti dei singoli trattamenti.
- Pareri in merito alla "Valutazione di impatto sulla protezione dei dati" (DPIA) ai sensi dell'art 35 GDPR e sulla scorta delle indicazioni dell'EDPB.
  Tale valutazione è necessaria ogniqualvolta il Comune pone in essere trattamenti nuovi che prevedono un trattamento automatizzato, o su larga scala o di sorveglianza sistematica su larga scala di una zona accessibile al pubblico, ad esempio nell'ipotesi di videosorveglianza in materia di sicurezza integrata o di varchi per il controllo del traffico.
  La DPIA, indipendentemente dalla metedologia adottata (Enisa, EDPB, Nist o 27K) avrà sempre come base il Risk Assessment relativo alla protezione delle persone fisiche e dei diritti fondamentali. Tale attività viene svolta ogni qualvolta si renda necessaria una "Valutazione di impatto sui diritti fondamentali e sulle libertà degli interessati".
- Punto di contatto con il Garante per la protezione dei dati personali: in qualità di RPD sono il referente dell'ente per tutti i contatti relativamente all'applicazione della normativa a tutela della privacy: dalla consultazione preventiva ad ogni richiesta a fronte di reclami di interessati ed in senso ampio per qualsiasi questione che riguardi il Comune e l'Autorità Garante o i suoi

delegati (Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza – NSTPFT). Tale attività viene svolta qualora si renda opportuna.

- Supporto nella tenuta del Registro dei Trattamenti. In qualità di RPD concorro ed assisto alla compilazione del Registro dei Trattamenti collaborando affinché siano mappate le finalità del trattamento, le categorie di interessati ed il loro numero, la fonte del dato, il tipo di dati personali, la base giuridica del trattamento, le modalità di esercizio dei diritti, i principi e le policy di trattamento e le modalità di trattamento. All'interno del trattamento sarà necessario determinare il rischio tramite la matrice di rischio (impatto e probabilità), così da determinare la valutazione di rischio per quello specifico trattamento e le conseguenti misure di sicurezza da adottare, nell'ottica della minimizzazione del rischio (rischio accettabile dal punto di vista GDPR).
  Tale attività dura per tutta la durata dell'incarico, andando progressivamente a considerare tutti i trattamenti di dati personali effettuati dal Comune.
- Modalità di reporting: oltre alle singole e-mail inviate per le consulenze di volta in volta richieste, alla fine di ogni anno verrà inviato via e-mail anche un resoconto delle questioni affrontate in merito all'attività di DPO.
- L'importo proposto per l'affidamento dell'incarico di DPO per il biennio certo è pari ad **€ 12.000,00 iva esclusa**;

Elementi di rilievo:

- Progetto "Altovicentino Comuni-ty": in qualità di RPD del Comune di Santorso – ente capofila – attività di coordinamento della Protezione dei dati personali di tale progetto biennale (2020-2021), approvato con deliberazione n. 26/2020 della Giunta Comunale del Comune di Santorso, volto in particolare alla: Creazione di un Family Hub informativo sui servizi erogati dal territorio alle famiglie; Realizzazione di un portale con i servizi alle famiglie mappati dagli enti partner; Costituzione di un Albo delle professioni e dei servizi di sollievo; Erogazione di voucher per inserimenti lavorativi e frequentazione di centri e strutture.
  Sono partners del progetto i seguenti Enti: Comune di Santorso (capofila), Comune di Schio, Comune di Thiene, Comune di Marano, Comune di Arsiero, Comune di Breganze, Comune di Caltrano, Comune di Carrè, Comune di Chiuppano, Comune di Zugliano, Comune di Valdagno, Comune di Posina, Unione Montana Pasubio (Comune di Monte di Malo, Piovene Rocchette, Posina, Santorso, San Vito di Leguzzano, Schio, Torrebelvicino, Valli del Pasubio), Unione Montana Alto Astico (Comuni di Arsiero, Cogollo del Cengio, Laghi, Lastebasse, Pedemonte, Tonezza del Cimone, Valdastico, Velo d'Astico), Unione Montana Astico (Comuni di Breganze, Caltrano, Calvene, Fara Vicentino, Lugo di Vicenza, Salcedo), Aulss7.

- Progetto "Cittadino al centro della PA digitale (AVATAR)":
  progetto della Regione Veneto – POR FERS 2014-2020, approvato con deliberazione n. 91/2019 della Giunta Regionale Veneta, per l'Azione 2.3.1 "Soluzioni tecnologiche per l'alfabetizzazione e l'inclusione digitale, per l'acquisizione di competenze avanzate da parte delle imprese e lo sviluppo di nuove competenze ICT; costituzione di Innovation Lab diretti al consolidamento/sviluppo del network "Centri P3@ - Palestre Digitali ed alla cultura degli Open Data.
  Sono partners del progetto i seguenti Enti: Comune di Schio (capofila), Comune di Santorso, Comune di Thiene, Comune di Marano Vicentino, Comune di Zugliano, Comune di Valdagno, Comune di Isola vicentina, Comune di Malo, Comune di Monte di Malo, Comune di San Vito di Leguzzano, Comune di Valdagno, Comune Torrebelvicino, Comune di Villaverla, Comune di Zugliano.

In qualità di RPD del Comune di Schio – ente capofila – ho svolto attività di coordinamento e di sorveglianza sulla protezione dei dati personali, in modo tale che i singoli processi di trattamento si svolgessero nel pieno rispetto dei principi posti dal GDPR.
Nello specifico è stato analizzato l'intero processo di conformità dei trattamenti dei dati personali alla normativa vigente, implementando un sistema di Privacy Risk Management così da indirizzare i contitolari verso le procedure ritenute più idonee in relazione ai singoli adempimenti che via via si rendevano necessari vista la tipologia di dati coinvolti, e ciò al fine di garantire la riservatezza degli interessati e, al contempo, creare prodotti "compliance".
Attesa la delicatezza di tutti i dati (non solo "personali") che formavano oggetto di trattamento, e tenuto conto che la privacy è strettamente collegata alla security (in quanto i dati che attraversano un sistema informatico diventano un'"informazione"), sono state poste in essere e verificate le opportune misure di protezione delle proprietà fondamentali dell'informazione stessa, le c.d. proprietà "RID", ovvero riservatezza, integrità e disponibilità; per tale motivo il DPO ha svolto al contempo anche la funzione di CISO (chief information security officer).
Oltre alle singole consulenze svolte sulle attività o iniziative poste in essere nell'ambito del progetto AVATAR, ho predisposto e redatto il "Manuale del Sistema di Gestione per la Sicurezza dei Dati personali ed Analisi del Rischio", tenuto conto delle misure minime di sicurezza ICT emanate da AgID per valutare e migliorare il livello di sicurezza informatica della P.A.

- Sicurezza Urbana Integrata (D. L. n. 14/2017, convertito nella L. 48/2017 (Decreto Minniti): in qualità di DPO del Consorzio di Polizia Locale Nordest Vicentino e del Consorzio di Polizia Locale Valle Agno, nonché di alcuni Comuni consorziati e convenzionati con gli stessi, agisco come soggetto facilitatore per addivenire, d'intesa con la Prefettura di Vicenza e con le Forze di Polizia interessate, alla realizzazione di un progetto strategico condiviso in materia di videosorveglianza urbana, nell'ottica di poter poi procedere con la stipula del Patto per l'attuazione della sicurezza urbana e successiva formalizzazione dell'accordo di contitolarità dei dati diretto a regolamentare prerogative e responsabilità di Prefettura e Comuni coinvolti.

- Associazione UNIDPO: sono socio fondatore dell'Associazione "Unione Nazionale Data Protection Officer", costituita nel 2018 con sede a Milano, che unisce i DPO – RPD con alte competenze nella materia di protezione dei dati.

- Socio ordinario del CLUSIT (associazione italiana per la sicurezza informatica).

- Pareri legali in merito alla protezione dei dati personali: in qualità di Avvocato, i pareri che rilascio nell'esercizio della mia attività di RPD (compresi nel servizio) relativi alla protezione dei dati personali (in materia di "Amministrazione trasparente", accesso agli atti, ecc.) sono confezionati come "Pareri giuridici *pro veritate*" e possono essere utilizzati dall'Ente, anche nei rapporti con i terzi, siano essi interessati oppure altri enti pubblici o privati.

- Studio Legale Lexin: è lo studio di cui sono titolare, ubicato a Schio, con uno staff di oltre dieci professionisti per una assistenza puntuale e competente nell'ambito della protezione della privacy, della sicurezza dei dati, delle nuove tecnologie e della "Transizione al digitale per la PA". Il sito dello studio è visitabile al seguente link: www.studiolexin.it

Avv. Luca De Toffani