Tutela dei dati personali: risk management e analisi dei processi in capo al DPO

a colloquio con Matteo Colombo, Presidente Asso DPO
a cura della Redazione

ASSODPO è l'associazione che rappresenta i Data Protection Officer, una figura professionale al centro dell'attenzione del nuovo Regolamento Europeo. Quali sono gli scopi e la storia dell'associazione, la rappresentatività, le attività in campo istituzionale e della formazione/certificazione?

Il Data Protection Officer (DPO) è una figura introdotta dal Regolamento generale sulla protezione dei dati 2016/679 | GDPR, pubblicato sulla Gazzetta Ufficiale europea L. 119 il 4 maggio 2016.

Il DPO, figura storicamente già presente in alcune legislazioni europee, è un professionista che deve avere un ruolo aziendale (sia esso soggetto interno o esterno) con competenze giuridiche, informatiche, di risk management e di analisi dei processi. La sua responsabilità principale è quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'azienda (sia essa pubblica che privata), affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali.

Questo soggetto è già conosciuto nel mondo anglosassone con il termine di Chief Privacy Officer (CPO) oppure Privacy Officer, Data Protection Officer o Data Security Officer.

In questo contesto, l'Associazione Data Protection Officer (ASSO DPO) è nata nel 2013 per volontà di alcuni professionisti dei settori Privacy, Formazione e Consulenza Informatica per offrire ai propri Associati un

punto di riferimento con cui discutere e approfondire le tematiche relative all'applicazione della normativa europea e italiana in materia di Data Protection.

In particolare, l'Associazione è diretta a sostenere e sviluppare l'attività dei Data Protection Officer, dei Consulenti della Privacy, dei Responsabili della Protezione dei Dati e dei Chief Privacy Officers, mediante il confronto e lo scambio di informazioni tra gli Associati.

Per fare ciò, l'Associazione si è dotata di un Comitato Direttivo e di un Comitato Scientifico composto da professionisti in tema di Data Protection nei diversi ambiti di applicazione (sanità, P.A., web, IT, legal ecc.).

In occasione del recente rinnovo delle cariche sociali, il Comitato Scientifico ha visto l'ingresso di DPO europei.

In questi primi tre anni di attività ASSO DPO può già contare più di 200 associati.

Per raggiungere questo importante traguardo, ASSO DPO ha promosso diverse attività, workshop, congressi, convenzioni nell'ambito della Data Protection.

In particolare, l'Associazione ha organizzato due edizioni del **Congresso Annuale internazionale** di ASSO DPO che rappresenta un momento di confronto per tutti i DPO italiani ed europei sui temi più rilevanti in materia di Data Protection.

Grazie al taglio decisamente internazionale ed agli interventi di Autorità Garanti italiane ed europee, della Commissione Europea, di funzionari della Guardia di Finanza e di figure di spicco nel campo della Data Protection, il congresso consente di approfondire e condividere dubbi ed esperienze direttamente con i Key Opinion Leader.

E' già prevista una terza edizione in data 8 e 9 maggio 2017, il cui programma sarà definito dal Comitato Scientifico e sarà reso noto sul sito ufficiale del Congresso.

Nel 2015 ASSO DPO ha ottenuto l'iscrizione nell'elenco delle Associazioni Professionali presso il Ministero dello Sviluppo Economico e può, quindi, rilasciare, ai propri associati che ne facciano richiesta, l'Attestato di Qualità e di Qualificazione Professionale dei Servizi Prestati.

Come previsto dalla normativa vigente, detti Associati possono essere iscritti nel Registro Professionale ASSO DPO (Legge 4/2013 per le Professioni non Regolamentate).

I componenti del Comitato Direttivo e del Comitato Scientifico partecipano a congressi nazionali ed internazionali organizzati dall'IAPP e Privacy Law & Business, nonché alle Conferences dell'Information Commissioner's Office (ICO).

Uno dei prossimi obiettivi sarà sicuramente quello di continuare nella strada intrapresa e di portare l'Associazione sempre più vicina e a supporto dei DPO italiani ed europei.

Come avete affrontato fino a questo momento il tema della videosorveglianza-privacy dal punto di vista formativo degli operatori?

L'Associazione organizza workshop e corsi specifici anche per il settore della videosorveglianza con approfondimenti sui seguenti temi: responsabilità dell'installatore, misure idonee per l'installazione degli impianti e obblighi dettati da normative specifiche, quali lo Statuto dei Lavoratori ed i Provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali.

Quali sono le principali innovazioni introdotte dall'art. 32 del Regolamento sul piano del coinvolgimento del fornitore di sistemi di sicurezza, in relazione all'obbligo per il responsabile del trattamento dei dati di impiegare soluzioni "adeguate" per la loro tutela?

Grazie al GDPR, è stato finalmente superato il limite tecnologico previsto dalla normativa italiana dell'obbligo di implementazione di misure di minime di sicurezza, passando ad un criterio più attuale di obbligo di implementazione di misure idonee in modo che le stessi si adattino alla tecnologia corrente e futura.

In particolare, l'articolo 32 prevede, fra l'altro, le seguenti misure idonee che dobbiamo ritrovare anche nei sistemi di videosorveglianza:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Queste misure dovranno essere sicuramente affiancate da un Data Privacy Impact Assessment (DPIA) quando il sistema permetta un trattamento invasivo come, ad esempio, l'utilizzo di sistemi che permettano l'identificazione facciale o l'analisi del comportamento attraverso motion detention avanzata.

Come un direttore d'orchestra, il DPO è chiamato a governare tutte le tematiche privacy: infatti, il Regolamento sulla Data Protection, entrato in vigore il 24 maggio 2016 e che si applicherà a tutti gli Stati membri UE a decorrere dal 25 maggio 2018, disciplina l'istituzione della figura del Data Protection Officer (in italiano: Responsabile della Protezione dei Dati) nei seguenti casi:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

b) le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure

c) le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 (dati particolari | sensibili) o di dati relativi a condanne penali e a reati di cui all'articolo 10.

L'articolo 9 del Regolamento al comma 1 definisce quelli che sono le categorie particolari di dati personali (ex dati sensibili) ed in particolare i dati personali che: *"rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".*

Quali proposte formative si possono offrire agli operatori della sicurezza fisica (progettisti, integratori/installatori) per operare nel rispetto della normativa, tutelando i propri clienti e se stessi?

Oltre ad organizzare i workshop ed i corsi specifici per il settore della videosorveglianza, ASSO DPO è partner di Bureau Veritas Italia SpA per il rilascio della Certificazione delle competenze del Data Protection Officer in conformità alla norma ISO/IEC 17024.

Il rilascio della Certificazione è subordinata al superamento di un esame scritto ed orale su molteplici tematiche in materia di protezione dei dati personali.

Ai fini della preparazione all'esame, gli Associati possono frequentare, a condizioni vantaggiose, un corso di formazione della durata di 48 ore dal titolo "Corso di Alta Formazione per Data Protection Officer".

ASSO DPO
Associazione Data Protection Officer ®