Risk Management in Studio in ottica Privacy, Data Protection e DLgs. 231/01

Avv. Giovanna Boschetti

7/07/2021

Il ruolo dell'avvocato:

la tutela di diritti di rango costituzionale e la fornitura di servizi

Art. 24 Costituzione

«Tutti possono agire in giudizio per la tutela dei propri diritti e interessi legittimi. La difesa è diritto inviolabile in ogni stato e grado del procedimento. Sono assicurati ai non abbienti, con appositi istituti, i mezzi per agire e difendersi davanti ad ogni giurisdizione […]».

Art. 1 Codice Deontologico vigente – «L'avvocato»

1. L'avvocato tutela, in ogni sede, il diritto alla libertà, l'inviolabilità e l'effettività della difesa […].

2. L'avvocato, nell'esercizio del suo ministero, vigila sulla conformità delle leggi ai principi […], a tutela e nell'interesse della parte assistita.

3. Le norme deontologiche sono essenziali per la realizzazione e la tutela dell'affidamento della collettività e della clientela, della correttezza dei comportamenti, della qualità ed efficacia della prestazione professionale.

Rapporto OCSE 2007

«*In Italy, several aspects of the provision of* ***legal services*** *are subject to some form of regulation. Such regulation, however, does not affect the ability* ***of potential service providers to access the market, since no quantitative restrictions on entry exist for the acquisition of the relevant professional qualifications (with the exception of notaries), nor a numerus clausus policy is applied for registration in Law Departments at universities****. In fact, Italy is the European country with the highest number of registered lawyers*».

«(25) Taluni *servizi legali sono forniti da prestatori di servizi designati da un organo giurisdizionale di uno Stato membro*, comportano la rappresentanza dei clienti in procedimenti giudiziari da parte di avvocati, devono essere prestati da notai o sono connessi all'esercizio di pubblici poteri. Tali *servizi legali* sono di solito prestati da organismi o persone selezionate o designate secondo modalità che non possono essere disciplinate da norme di aggiudicazione degli appalti, come può succedere ad esempio per la designazione dei pubblici ministeri in taluni Stati membri.».

L'avvocato come responsabile del trattamento

L'Avvocato può «*essere responsabile del trattamento dei dati personali nel momento in cui - ad esempio - gli venga richiesta una consulenza da un soggetto che è titolare del trattamento*. […]».

(Consiglio Nazionale Forense, Il GDPR e l'avvocato, disponibile all'indirizzo web https://www.consiglionazionaleforense.it/utilita-per-la-professione/-/asset_publisher/asZkPXtZCb2T/content/gdpr-linee-guida-avvocati?normalfont)

Art. 28 GDPR – «Responsabile del trattamento»

«1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato. […]

3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento […]. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento: a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento […] b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza […]»

Panorama normativo di riferimento

- Regolamento (UE) 2016/679 (“Regolamento Generale sulla protezione dei dati - GDPR”) e D.Lgs. 196/03 («Codice Privacy»)
- Regolamento (UE) 2019/881 dell’UE, in vigore dal 27 giugno 2019, sulla cybersicurezza
- D.Lgs. 30/05 «Codice della proprietà industriale»
- L. 633/41 «Legge sulla protezione del diritto d’autore»
- D.Lgs. 231/2001 «Responsabilità amministrativa delle società e degli enti»

Raccomandazione del Garante privacy

«La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì **parte integrante di un sistema di corretta gestione dei dati personali**. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta. I contenuti del registro sono fissati, come detto, nell'art. 30; tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva **valutazione di impatto** dei trattamenti svolti».

(Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali, a cura del Garante privacy e disponibile al link https://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili)

Il legal design dello Studio

L’adozione del modello organizzativo e del modello di gestione del sistema privacy e data protection in Studio

Per gli avvocati, che gestiscono dati particolari (ex dati «sensibili») talvolta anche su larga scala ai fini della normativa previgente e che hanno espressi doveri professionali e deontologici di riservatezza è fondamentale adottare, e poter così dimostrare di avere adottato, un corretto modello organizzativo su cui si modella anche la gestione del sistema privacy e data protection.

Mappare i rischi, i ruoli ed i processi interni diventa attività fondamentale

Il perimetro degli assett

- Sistema di corporate governance e modello organizzativo
- Codice etico - *mission* aziendale
- Segni distintivi
- Titoli di proprietà intellettuale ed industriale
- Know how
- Sito internet
- Tecnologia
- Database/mailing list
- Attività di comunicazione
- Attività su Social Media

Gli assett aziendali sono a rischio?

Nel Report ENISA (European Union Agency for Cybersecurity) sulle minacce del 2020 dedicato al phishing (disponibile all'indirizzo www.enisa.europa.eu/publications/phishing), è evidenziato che gli attacchi di phishing collegati al COVID-19, rilevati inizialmente alla fine del 2019, **sono aumentati del 667% nel periodo di un mese (tra la fine di febbraio 2020 e la fine di marzo 2020).**

Il mio Studio legale ha adottato un efficace modello di organizzazione ai fini della tutela dal rischio di attacchi esterni e da fattispecie di reati informatici/illecito trattamento di dati personali?

Le sanzioni ai sensi del GDPR

- sanzioni amministrative (art. 83 GDPR e art. 166 del Codice Privacy)
- sanzioni penali (considerando 148 GDPR e artt. 167-170 Codice Privacy)
- inutilizzabilità dei dati (art. 2-*decies* Codice privacy)
- danni d'immagine

- ogni Ente può essere ritenuto responsabile per determinati reati commessi nel suo interesse o a suo vantaggio da soggetti in posizione apicale e/o in posizione subordinata
- a tale responsabilità segue l'applicazione, a carico dell'ente, di rilevanti sanzioni di natura interdittiva e pecuniaria (che si aggiungono ai danni d'immagine);
- la normativa è applicabile anche agli studi legali (sono destinatari della normativa, tra gli altri, enti forniti di personalità giuridica, società ed associazioni anche prive di personalità giuridica)

I reati presupposto ai sensi del D.Lgs. 231/01

Art. 24. **Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture**

Art. 24-bis. Delitti informatici e trattamento illecito di dati

Art. 24-ter. Delitti di criminalità organizzata

Art. 25. Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio

Art. 25-bis. Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento

Art. 25-bis.1. Delitti contro l'industria e il commercio

Art. 25-ter. Reati societari

Art. 25-quater. Delitti con finalità di terrorismo o di eversione dell'ordine democratico

Art. 25-quater.1. Pratiche di mutilazione degli organi genitali femminili

Art. 25-quinquies. Delitti contro la personalità individuale

Art. 25-sexies. Abusi di mercato

Art. 25-septies. Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro

Art. 25-octies. Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio

Art. 25-novies. Delitti in materia di violazione del diritto d'autore

Art. 25-decies. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

Art. 25-undecies. Reati ambientali

Art. 25-duodecies. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare

Art. 25-terdecies. Razzismo e xenofobia

Art. 25-quaterdecies. Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati

Art. 25-quinquiesdecies. Reati tributari

Art. 25-sexiesdecies. Contrabbando

Art. 26. Delitti tentati

Requisiti del Modello *ex* D.Lgs. 231/01

Il Modello deve :

- individuare le attività nel cui ambito possono essere commessi reati;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- prevedere obblighi di informazione nei confronti dell'Organismo deputato a vigilare su funzionamento ed osservanza del Modello (O.d.V.);
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

(N.B.: fase preliminare determinante Risk Assesment)

La progettazione del sistema *data protection* in azienda

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (art. 25 GDPR)

1.«Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, **sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso** il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

2.Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, **per impostazione predefinita**, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.»

GDPR

Privacy by design

Protezione dei dati fin dalla progettazione

Privacy by default

Protezione dei dati per impostazione predefinita

Approccio fondato sulla valutazione del rischio (*risk based approach*) inerente l'attività svolta

Obiettivi:

- responsabilizzare il titolare (principio di ***accountability***)
- fornire evidenza di tutti gli adempimenti compiuti

«Privacy by design» e «Privacy by default»

Privacy by design

Obbligo di protezione dei dati personali sin dalla **progettazione di**:

- processi aziendali;
- sistemi informatici (hardware e software);
- pratiche commerciali;
- strategie;
- sistemi di presidio.

Privacy by default

Obbligo di trattamento **per impostazione predefinita** di quei soli dati personali necessari per ogni specifica finalità del trattamento.

Misure di sicurezza a 360°

Analizzando il GDPR, si possono distinguere:

- misure dettate dai **principi generali del GDPR** (*id est* minimizzazione del trattamento in termini qualitativi e quantitativi);
- misure di sicurezza **tecniche** (*id est* anonimizzazione, pseudonimizzazione dei dati);
- misure di sicurezza **organizzative** (*id est* capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento);
- misure di sicurezza **informatiche** o logiche (*id est* procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento);
- misure di sicurezza **fisiche** (*id est* capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico).

La gestione del rischio in Studio. Perché adottare un MOGP?

- per mantenere apertura verso il mercato internazionale, trattandosi di regole vigenti in tutta Europa e con un ampio respiro internazionale;
- per mettere in sicurezza tutta l'attività (compreso il *know how*, espressamente tutelato ai sensi del D.Lgs. 63/2018);
- per avere un unico modello di compliance che consenta di rispondere alle norme di prevenzione del rischio di reato ex D.Lgs. 231/01, di *privacy* e di *cybersecurity*;
- perché le diverse normative perseguono obiettivi che finiscono per coincidere.

Avv. Giovanna Boschetti

giovanna.boschetti@cbalex.com

www.cbalex.com

20122 **MILANO**
C.so Europa, 15
Tel. +39 (0)2 778061
Fax +39 (0)2 76021816
E-Mail: milano@cbalex.com

00198 **ROMA**
Via Donizetti, 10
Tel. +39 (0)6 89262900
Fax +39 (0)6 89262921
E-Mail: roma@cbalex.com

35137 **PADOVA**
Galleria dei Borromeo, 3
Tel. +39 (0)49 0979500
Fax +39 (0)49 0979521
E-Mail: padova@cbalex.com

30135 **VENEZIA**
Santa Croce, 251
Tel. +39 (0)41 2440266
Fax +39 (0)41 2448469
E-Mail: venezia@cbalex.com

D-80539 **MÜNCHEN**
Ludwigstrasse, 10
Tel. +49 (0)89 99016090
Fax +49 (0)89 990160999
E-Mail: muenchen@cbalex.com