La privacy e lo studio professionale: l’approccio basato sul rischio

scritto da goal | 7 Agosto 2020

***di Stefano Bacchiocchi** **

Con l’introduzione del GDPR (regolamento UE 679/2016) si pone con forza l’accento sulla “responsabilizzazione” (c.d. accountability) del titolare del trattamento, cioè sull’adozione di comportamenti ed adempimenti tali da dimostrare, anche a posteriori, la concreta adozione di misure finalizzate ad assicurare l’applicazione della normativa.

In altre parole, i titolari del trattamento hanno il compito (non facile) di decidere autonomamente le modalità con le quali rispettare tale normativa.

Questo approccio legislativo, basato sul rischio, non è nuovo: basti pensare alle altre normative di derivazione europea come, ad esempio, l’antiriciclaggio.

Di fatto non esiste più un elenco di cose da fare, così come non esistono più adempimenti standard.

A questi principi di ordine generale spesso si accompagnano sanzioni elevatissime che non tengono conto concretamente delle dimensioni dell’organizzazione che le deve applicare: in altre parole, la stessa normativa si applica sia alla grande multinazionale sia al piccolo studio di provincia.

Tuttavia vi è la possibilità di costruirsi una serie di procedure ed adempimenti pensati in modo “sartoriale”, ossia modellati sulle specifiche caratteristiche di ogni organizzazione.

In questo articolo si proverà a dare qualche indicazione

pratica per riuscire a calare questi principi di ordine generale nei nostri studi professionali.

Tra i criteri che il titolare del trattamento deve seguire per raggiungere l'obiettivo di attuare l'approccio basato sul rischio è la c.d. «protezione dei dati by default and by design»: la necessità di costruire la propria organizzazione prevedendo immediatamente le garanzie indispensabili per tutelare i diritti degli interessati.

Da ciò si evince la prima indicazione di ordine pratico: bisogna studiare attentamente i flussi di dati personali sia in entrata sia in uscita fin da subito, prima di porre in essere il trattamento stesso. Questa attività è bene che sia fatta con personale competente e/o dopo un attento studio della normativa ed una ricognizione di tutti gli aspetti coinvolti: le tipologie e le quantità di dati trattati, i soggetti coinvolti, le infrastrutture (fisiche e informatiche), la contrattualistica e così via.

Già da queste poche righe dovrebbe essere evidente che si richiede uno sforzo notevole. Purtroppo, o per fortuna, la normativa privacy è fatta di principi, non di adempimenti; da un lato, infatti, ci permette una configurazione ad hoc, dall'altro lato richiede tempo e competenze specifiche.

Un ulteriore aspetto che deve essere chiarito fin da subito è che, non essendoci una lista predefinita di adempimenti, è virtualmente impossibile essere certi di essere "a norma". Come fare quindi a dimostrare (magari ex post) di aver fatto tutto il possibile per rispettare la normativa e quindi di aver utilizzato un approccio "basato sul rischio"? Il mio consiglio è di fare quello a cui siamo già abituati in quanto professionisti: tenere traccia di tutte le attività, anche prodromiche e meramente introduttive; sistematicamente e per iscritto.

Ad esempio: se facciamo formazione periodica ai nostri

dipendenti, è opportuno predisporre fogli di firma, programmi predefiniti e calendarizzati, attestati e così via.

Di nuovo, appare subito evidente come i piccoli studi siano più in difficoltà con questi adempimenti che spesso esulano dalle normali attività professionali; tuttavia, è possibile accedere a competenze di alto livello in maniera piuttosto semplice, ancorché a pagamento, affidandosi ad un Responsabile della protezione dei Dati (cd. DPO *data protecion officer*) di cui abbiamo parlato su queste stesse pagine (numero luglio-agosto 2018).

Ma cosa si intende esattamente per "approccio basato sul rischio"? Trattasi del rischio di impatti negativi sulle libertà e i diritti degli interessati.

In altre parole, maggiore è la possibilità di impatti negativi per gli interessati, più gli adempimenti, le garanzie, i presidi di sicurezza, ecc. dovranno essere adeguati al rischio.

Da questa definizione discende il secondo consiglio pratico: c'è bisogno di un'analisi preventiva anche per individuare e mitigare i rischi connessi allo specifico trattamento di dati.

Ossia, dovrà essere messo in atto uno specifico processo di valutazione che faccia emergere non solo i rischi evidenti ma anche quelli solo potenziali.

Conseguentemente bisognerà predisporre (possibilmente nero su bianco) le misure di sicurezza che si intendono adottare per eliminare o mitigare il rischio rilevato.

Di nuovo, non esistono indicazioni standard: a volte basterà un antivirus, in altre occasioni bisognerà eseguire un aggiornamento totale della rete informatica, altre volte ancora si dovranno rivedere le contrattualistiche ecc. Questa fase è estremamente delicata: i titolari del trattamento sono infatti tenuti non soltanto a garantire l'osservanza della

normativa, ma anche a dimostrare in concreto in che modo essa venga rispettata. Al di là degli obblighi di legge, questa analisi puntuale è sicuramente una buona prassi che permette di ricavare indicazioni importanti (e soprattutto utili) a prevenire incidenti futuri.

La valutazione del rischio poi è integrata e completata dall'analisi degli impatti sui dati personali degli interessati al verificarsi dei rischi rilevati.

Questa operazione è individuata come "Valutazione di impatto sulla protezione dei dati" (c.d. DPIA).

Infatti, all'esito di questa valutazione, potrebbe addirittura emergere la necessità di non porre in essere, o interrompere immediatamente, il trattamento dei dati personali: questo ovviamente quando non sia possibile ridurre in maniera soddisfacente il rischio.

In questi casi vi è l'opportunità di consultare l'autorità di controllo per ottenere delucidazioni su come gestire il rischio; si badi bene però che l'autorità non ha il compito di autorizzare il trattamento, ma solamente quello di indicare le misure eventualmente ancora da implementare.

Anche per questo adempimento è consigliabile ricorrere all'intervento di un Responsabile della Protezione dei Dati (DPO), che abbia esperienza e competenza in materia, al fine di evitare lungaggini, costi inutili e responsabilità che possono essere anche di natura penale.

In merito, il Garante (e più in generale le omologhe istituzioni europee) ha messo a disposizione un protocollo di valutazione che permette, passo per passo, di effettuare la valutazione d'impatto mediante un software gratuito disponibile su https://www.cnil.fr/fr/outil-pia-telechargez-et- installez-le-logiciel-de-la-cnil.

Vi sono ulteriori adempimenti che, sebbene non strettamente obbligatori per alcune realtà, permettono di analizzare gli aspetti citati in modo formale e di mitigare le possibili sanzioni.

Un esempio è il c.d. registro dei trattamenti, che può essere tenuto in modalità cartacea o informatica; trattasi di uno strumento fondamentale non soltanto ai fini dell'eventuale controllo ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere.

È assolutamente consigliato cogliere l'occasione della redazione del registro dei trattamenti per effettuare un'analisi più approfondita del proprio ufficio a prescindere dalle dimensioni dello stesso.

Per le organizzazioni più strutturate, è inoltre consigliabile utilizzare specifici codici di condotta e certificazione per attestare l'adeguatezza delle misure di sicurezza adottate.

Detto questo è però bene essere consapevoli che il GDPR prende atto che gli eventi rischiosi e gli atti (volontari o meno) che provocano violazioni dei dati personali, sono per loro natura incerti.

Di conseguenza, eliminare del tutto qualsiasi rischio è impossibile.

In conclusione, è opportuno ribadire che per poter garantire, per quanto possibile, la conformità dello studio alla normativa in esame, il professionista non deve solo limitarsi alla mera valutazione del rischio, deve anche dotarsi di un sistema di procedure, documenti e prassi che siano dimostrabili e coerenti con il grado di rischio rilevato.

Il professionista non può più limitarsi solo a "far funzionare" lo studio ma deve essere in grado di proteggere tutti i portatori di interessi (soprattutto clienti ed interessati) anche in materie, come la privacy, che non sono

sempre oggetto dell’attività professionale.

Da questo si evince che è fondamentale la formazione e l’accesso a professionalità qualificate che aiutino i titolari del trattamento ad ottemperare ai dettati normativi sempre più multidisciplinari.

**Odcec Brescia*