La gestione del Data Breach negli studi che si occupano di lavoro, paghe e contributi

scritto da goal | 9 Luglio 2019

di Stefano Bacchiocchi*

Con la nuova normativa privacy (il regolamento europeo in materia di privacy, ovvero il GDPR, General Data Protection Regulation) abbiamo imparato un termine nuovo che deriva come al solito dall'inglese: "Data Breach". Questa terminologia indica un incidente di sicurezza durante il quale i dati personali di persone fisiche vengono trattati, consultati (o rubati) ecc. da soggetti non autorizzati.

In altre parole, è un evento non programmato che intacca l'integrità e correttezza dei dati personali trattati o il loro grado di riservatezza.

Come è facile intuire, si tratta di un evento che va prevenuto con ogni mezzo; pensiamo a cosa accadrebbe nei nostri studi se fossimo travolti da un evento di questo tipo: sarebbe il caos organizzativo e un problema reputazionale enorme, prima ancora che legale.

Se, nonostante le nostre precauzioni e procedure, tale evento dovesse verificarsi, la nuova normativa privacy ha previsto delle procedure ber precise da seguire che vanno conosciute ed applicate.

Siamo in un mondo sempre più informatizzato in cui la rapida diffusione di piattaforme web, anche istituzionali, ha portato senza dubbio vantaggi, ma anche alcune problematiche di sicurezza non trascurabili.

Quali dati dobbiamo proteggere nei nostri studi? È una domanda

non banale; infatti, prima di analizzare le problematiche e i rischi connessi alla violazione della privacy, è utile comprendere cosa si intende per dati personali. In linea generale, sono tutte quelle informazioni in grado di identificare una persona fisica, come i dati anagrafici, la residenza ecc. ma non solo: sono dati personali da proteggere anche le caratteristiche fisiche, i dati che rivelano la situazione economica, le opinioni politiche, l'orientamento religioso, le preferenze e gli orientamenti sessuali, ecc. In altri termini, i nostri studi trattano questi dati tutti i giorni e i nostri PC ed archivi ne sono pieni, ergo dobbiamo porci il problema di come proteggere tutto l'ufficio sia dal punto di vista informatico sia da quello cartaceo, non dimenticandoci dei comportamenti di dipendenti, colleghi e collaboratori. ricordiamoci, inoltre, dei dati personali che possiamo chiamare "inconsapevoli", ad esempio i dati della geolocalizzazione dello smartphone, i luoghi di interesse e luoghi frequentati (pensiamo a Facebook o Google), preferenze che vengono sfruttate per la pubblicità, come cookies informatici e dati di navigazione, dati inviati e ricevuti da applicazioni su smartphone PC e tablet ecc.

Risulta ovvio, quindi, che capire quali dati trattiamo è di fondamentale importanza per evitare che gli utenti possano subire dei danni.

Non a caso, la nuova normativa privacy impone la redazione del cd. Registro Dei trattamenti con lo scopo di elencare tutti i trattamenti di studio e i relativi dati personali utilizzati e/o trasferiti a terzi. Questo documento, se opportunamente redatto, permette di avere una panoramica completa di tutte le informazioni personali che trattiamo abitualmente nell'attività professionale; è quindi un ottimo punto di partenza per riuscire a studiare e coordinare i metodi di difesa.

Il GDPR prevede precisi obblighi cui il titolare

del trattamento dei dati deve assolvere in caso si verifichi il Data Breach. Chiariamo subito uno dei dubbi più frequenti: il Data Breach non è più (se mai lo è stato) un fenomeno da tenere nascosto; non è un "incidente" che riguarda la sola organizzazione aziendale, in questo caso i nostri studi professionali. La normativa non lo permette.

Questo poiché la divulgazione non autorizzata, la perdita, il furto, la modifica non autorizzata, ecc. dei dati personali di persone fisiche può causare gravi conseguenze. Addirittura potrebbe potenzialmente arrivare ad arrecare danni fisici, materiali, morali, immateriali ai soggetti coinvolti a cui i dati violati si riferiscono; inoltre si potrebbero verificare limitazioni di diritti garantiti, furti (anche di identità), discriminazioni, danni economici e patrimoniali, danni reputazionali, danni morali, modifiche dei comportamenti adottati e delle scelte dell'individuo, ecc. possiamo qui riassumere i requisiti minimi per essere aderenti (almeno per la parte documentale) alla normativa citata: è indispensabile avere adottato un registro dei trattamenti, avere effettuato la valutazione di impatto (DPIA) per quei trattamenti che la richiedono, avere adottato un protocollo per reagire al data Breach in modo tempestivo.

È utile non limitarsi a questi pochi adempimenti documentali: per uno studio professionale "standard" è consigliabile almeno coinvolgere i sistemisti informatici per effettuare dei test periodici per verificare la validità del protocollo nel tempo e per verificare che il Data Breach non si sia già verificato; talvolta, infatti, le violazioni citate non sono nemmeno visibili e solo un attento esame informatico può rivelare le violazioni subite nel tempo. Inoltre, bisognerebbe formare il personale di studio ed i collaboratori oltre che sulla normativa privacy in generale, anche sulla corretta rilevazione e gestione del Data Breach.

Il GDPR ha anche stabilito che il titolare del trattamento dei

dati, una volta riscontrata una violazione, debba necessariamente informare il Data Protection Officer (Responsabile della Protezione dei Dati, se nominato) e le autorità preposte (il Garante) del fatto entro 72 ore.

Eventuali ritardi possono essere fisiologici, ma devono essere attentamente e puntualmente giustificati.

La comunicazione al Garante deve avere dei contenuti minimi, (art. 33 GDPR): la natura della violazione dei dati personali, le categorie, il numero approssimativo di interessati in questione, le categorie e il numero approssimativo di registrazioni; il nome e i dati di contatto del responsabile della protezione dei dati (se nominato) o contatto presso cui ottenere più informazioni; le probabili conseguenze delle violazioni dei dati personali; le misure adottate per porre rimedio alla violazione dei dati personali.

Quando la violazione dei dati personali rappresenta un rischio elevato per i diritti e le libertà delle persone fisiche bisognerà, inoltre, comunicare la violazione all'interessato senza ritardo. Tale comunicazione descrive con un linguaggio semplice e chiaro la natura della violazione. Si può immaginare cosa voglia dire, anche solo in relazione alla reputazione, comunicare ai clienti che lo studio è stato violato ed i dati personali (clienti, dipendenti dei clienti, collaboratori, famigliari, ecc.) sono stati compromessi.

Fortunatamente tale comunicazione agli interessati non è richiesta:

- se il titolare del trattamento ha messo in atto le misure tecniche ed organizzative adeguate di protezione (es. cifratura dei dati) e tali misure erano state applicate correttamente da tutti gli incaricati e dai responsabili del trattamento;
- se il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di

un rischio elevato per i diritti e le libertà degli interessati;

- se detta comunicazione richiederebbe sforzi sproporzionati. In tale caso, si procede invece a una comunicazione pubblica o a una misura equivalente.

Per scongiurare i pericoli ed i danni che il Data Breach comporta, è consigliabile inoltre: nominare il Data Protection Officer, figura fondamentale per i nostri studi (abbiamo già avuto modo di parlare di questa figura in altri numeri di questa rivista) e di avere una copertura assicurativa per ottenere un indennizzo per fare fronte alle conseguenze negative derivanti dalla violazione dei dati, ad esempio per pagare le spese legali che si dovranno sostenere e/o per risarcire la clientela.

Infine è consigliabile predisporre un registro degli attacchi subiti, in modo da riuscire a identificare la tipologia di violazioni a cui si è più vulnerabili.

Anche i colleghi impegnati nei collegi sindacali e/o con ruoli di coordinamento e controllo non devono sottovalutare questi aspetti nell'ottica della valutazione della continuità aziendale (chiedendo magari agli uffici legali o agli amministratori dei report e/o facendo degli audit interni ad hoc); infatti, essere ottemperanti alla normativa privacy significa, di fatto, anche avere uno studio o una azienda più sicuri dal punto di vista della protezione dei dati ed una migliore possibilità di continuità aziendale.

* *Odcec Brescia*