Conformità al GDPR, si parte dalla mappatura delle informazioni

La legge sulla protezione dei dati personali si applica a tutti: grandi e piccole aziende, settore privato e ambito pubblico, associazioni e studi professionali. Il motivo è chiaro: nella società delle informazioni, il governo della loro corretta circolazione è compito di chiunque. Dunque, studi e associazioni professionali sono anch'essi catturati dalla rete a strascico del data protection. Quelli di grandi dimensioni o di profilo internazionale appaiono analoghi a imprese complesse.

Più spesso, però, lo studio è composto da un titolare, coadiuvato da collaboratori e da un supporto amministrativo-segretariale: tutto ciò che non fa parte del processo professionale tipico viene esternalizzato per quanto necessario.

Questa caratura organizzativa elementare rischia di andare in fibrillazione allorché affronta la conformità "alla privacy"; di converso, un corretto sistema di gestione delle informazioni non solo consolida la reputazione professionale, ma fa anche risparmiare tempo e denaro, grazie alla possibilità di avvalersi di dati corretti, pertinenti e sicuri.

Il codice privacy e il regolamento Ue prevedono percorsi agevolati per le piccole imprese e per talune finalità perseguite dagli studi legali, come per le investigazioni difensive e l'esercizio del diritto di difesa. Nell'affrontare lo "scoglio privacy", tocca al professionista, in primo luogo, riuscire a distinguere quando le informazioni sono gestite per esigenze proprie, con autonomia decisionale (cioè come "titolare del trattamento"), rispetto a situazioni in cui tale attività viene svolta per conto di un cliente (cioè come "responsabile"): l'operazione non è sempre agevole.

Di certo, i dati personali dei propri dipendenti e collaboratori, come quelli dei clienti sono gestiti dal professionista in qualità di titolare del trattamento: riguardo a essi, infatti, il professionista decide le finalità d'uso, gli strumenti e le misure di sicurezza da adottare.

«Responsabile» e «titolare»

Al contrario, non sempre può risultare facile la determinazione del ruolo del professionista in merito alla gestione dei dati personali necessari per l'esecuzione dell'incarico ricevuto: **il professionista agirà come "responsabile del trattamento", per conto del cliente, quando quest'ultimo si troverà a impartire istruzioni sulla gestione dei dati mantenendo un proprio potere decisionale**. In questo caso il professionista sarà vincolato a precisi obblighi contrattuali data protection, da formalizzare in un apposito atto giuridico. **Se, invece, anche nella conduzione del mandato il professionista mantiene un'ampia autonomia nella gestione dei pertinenti dati personali, allora rivestirà il ruolo di titolare del trattamento e dovrà rispondere direttamente delle prescrizioni di legge.**

In proposito occorre sgombrare il campo da un equivoco alquanto diffuso: l'utilizzo dei dati personali da parte del singolo professionista, per esigenze dello studio professionale, non può essere considerato un uso per finalità personali, al quale non si applica la normativa sulla privacy (come nel caso di agende o rubriche). Sia nell'ambito della propria gestione organizzativa sia in quello della prestazione professionale, il professionista titolare del trattamento dovrà fornire l'informativa ai soggetti cui si riferiscono i dati personali che raccoglie e gestisce (dipendenti, collaboratori, visitatori, clienti). Analogamente, dovrà mettere in atto alcune procedure interne, ancorché semplici, per assicurare l'agevole risposta in caso di richiesta di accesso ai dati o di altre forme di esercizio dei diritti da parte degli interessati.

Altro snodo fondamentale, è la discriminazione dei dati personali a più alto rischio (cosiddetti "sensibili" e "giudiziari") dagli altri più "comuni", in fase sia di archiviazione sia di loro circolazione, in modo da poter indirizzare adeguate risorse e protezioni laddove maggiormente necessario. Propedeutica, al riguardo, è l'attività di mappatura delle attività svolte in relazione ai dati personali gestiti e, in presenza di dati sensibili, l'evidenza documentale di tale rendicontazione (cioè il registro dei trattamenti, richiesto dal Gdpr).

Con la piena applicazione di quest'ultimo eventuali data breach subiti dallo studio richiedono al titolare una serie di tempestivi e puntuali interventi per valutarne gli impatti, contenere gli effetti e, se del caso, notificare al Garante e persino comunicare la violazione ai diretti interessati.

Ma non sembri il tutto un apparato insostenibile per l'agile struttura dello studio professionale tipo. Il Gdpr tiene conto delle particolarità di organizzazioni "sotto-soglia": ad esempio, il registro dei trattamenti non è dovuto per le organizzazioni con meno di 250 dipendenti e se non ci sono rischi; la notifica dei data breach non scatta se è improbabile il rischio per i soggetti interessati.

Lo stesso legislatore promuove l'elaborazione di codici di condotta da parte di organizzazioni rappresentative di microimprese o Albi professionali, che tengano conto delle specificità dei trattamenti nei propri settori e delle esigenze di tali entità, in particolare calibrando gli obblighi in rapporto al potenziale rischio del trattamento per diritti e libertà degli individui.

Fonte: Il Sole 24 Ore - Articolo a cura di Rosario e Riccardo Imperiali