A partire dal 25 maggio 2018 sarà direttamente applicabile il Regolamento UE 2016/679 (GDPR), in materia di protezione dei dati personali, che introduce significative novità che interessano imprese e professionisti.

Anche gli Studi legali ed il singolo Avvocato hanno l’obbligo di uniformarsi alla normativa, pena pesanti sanzioni, soprattutto pecuniarie.

In particolare, viene alla luce il principio di responsabilizzazione (*accountability*), che implica la libertà del titolare del trattamento nell’approntare misure adeguate alla protezione dei dati personali, senza basarsi solamente su modelli precompilati ovvero documentazione standard: dunque, oltre a prevedere delle misure di base (in applicazione del principio denominato “*privacy by default”*), ciascun titolare del trattamento dovrà adottare delle procedure modellate sulle necessità e caratteristiche del trattamento svolto all’interno della propria realtà (“*privacy by design*”).

Il professionista deve comprovare il rispetto dei principi applicabili al trattamento dei dati personali, tramite vari adempimenti:

* designazione del DPO, ove previsto dalla legge. La nomina non è obbligatoria per i singoli Avvocati, salvo che non si ricada nella lett. c) art. 37 GDPR (potrebbe essere il caso dei cosiddetti “*megastudi*”), ossia se lo Studio effettui trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala ovvero tratti, sempre su larga scala, categorie particolari di dati personali (previsti agli artt. 9 e 10 del Regolamento, si tratta dei c.d. “dati particolari”, ex “dati sensibili” nonchè dei dati c.d. “di carattere giudiziario”);
* istituzione del registro delle attività di trattamento, nei casi previsti dall’art. 30 GDPR: esso non compete “alle imprese o organizzazioni ***con meno di 250 dipendenti*,** a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell’interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all’articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all’articolo 10.”

L’istituzione e la tenuta del registro, in ogni caso, è fortemente consigliata dal Garante della privacy, perché consente una prima valutazione e diagnosi dei dati trattati all’interno della struttura;

* notifica di eventuali *data breach*, con specifiche procedure da attivare in caso di eventuali violazioni;
* aggiornamento dell’informativa sulla base degli artt. 13 e seguenti GDPR;
* verifica politiche interne in tema di trattamento dati, ai sensi dell’art. 24 GDPR, provvedendo a definire in maniera adeguata i ruoli e assicurandosi che tutto il personale riceva adeguata formazione;
* verifica dei sistemi informatici per assicurare il rispetto dei principi di protezione dei dati;
* formalizzare o rinnovare rapporti contrattuali con eventuali responsabili del trattamento dei dati, esterni o interni;

* prevedere nuove specifiche autorizzazioni per i soggetti che trattano i dati;
* verifica sull’adozione delle misure tecniche e organizzative adeguate per garantire un livello di sicurezza proporzionato al rischio;
* verifica sulla necessità di procedere ad una valutazione di impatto privacy (DPIA).

Ad oggi, il legislatore ha predisposto uno schema di decreto legislativo volto ad armonizzare la normativa interna con il Regolamento, tuttora in fase di approvazione.

Pertanto, le indicazioni nonchè la documentazione che verrà fornita in allegato alla presente potranno subire integrazioni e modifiche.