

POSSIBILI ACCORGIMENTI PER LO STUDIO D'AVVOCATO PER CONFORMARSI ALLE NUOVE DIRETTIVE IN MATERIA DI PROTEZIONI DEI DATI PERSONALI.¹

Nell'ambito del presente documento sono elencati dieci accorgimenti implementabili negli Studi legali al fine di assicurare la compatibilità dei processi di trattamento dei dati personali con il nuovo quadro svizzero e dell'Unione europea sulla protezione dei dati.

1) Acquisire le metodiche interne concernenti la “governance” e definire un modus operandi relativo al trattamento dei dati personali.

Nominare in seno allo studio una persona (o un gruppo di persone), incaricata della protezione dei dati personali. La persona in questione (o il gruppo) dovrà avere una buona conoscenza del sistema informatico utilizzato presso studio, rispettivamente lavorare in stretta collaborazione con gli eventuali specialisti in informatica interni (oppure esterni) dello studio.

La persona (o un membro del gruppo) potrà, inoltre, contemporaneamente, assumere il ruolo di Data Protection Officer (DPO), la cui nomina è obbligatoria, in alcuni casi, sotto l'egida del GDPR (art. 37).

2) Allestire un registro delle attività di trattamento dei dati personali.

Lo scopo di tale registro è quello di esaminare i diversi processi di trattamento dei dati personali, le categorie dei dati personali trattati, le finalità del trattamento, gli operatori (interni o esterni) che trattano tali dati e li trasferiscono a dei terzi, in Svizzera e/o all'estero. Il contenuto minimo del registro è stabilito all'art. 30 del GDPR e all'art. 11 p-LPD. Tenuto conto del fatto che tali due normative prevedano delle eccezioni/delle facilitazioni per le piccole e medie imprese (<250 collaboratori secondo il GDPR, / <50 collaboratori (in linea di principio), secondo il p-LPD), nell'ambito di un approccio pratico, la preparazione di un cosiddetto “registro semplificato” potrebbe, di per sé, già costituire un primo passo nell'ottica di identificare i processi di trattamento dei dati personali che sono stati implementati in seno allo studio.

3) Esaminare le misure di sicurezza adottate al fine di proteggere i dati personali.

Il relativo compito dovrà essere realizzato in collaborazione con un informatico specializzato nel campo della sicurezza delle informazioni ed essere formalizzato sotto forma di un rapporto scritto (in specie allo scopo di assicurare che siano messe in pratica dei correttivi). Gli accorgimenti di sicurezza adottabili sono, in particolare: la scelta di un server interno o esterno allo studio, la scelta di un sistema di copie di sicurezza dei dati e dei relativi parametri, la cifratura o la pseudonimizzazione dei dati e l'implementazione di un sistema strutturato di mantenimento delle attrezzature informatiche.

¹Testo originario: “Mesures envisageables pour les études d'avocats afin de se conformer aux nouvelles règles en matière de protection des données personnelles”, di Mes Corinne Corminboeuf Harari, Sophie Montalcini, Philipp Fischer, Adrien Alberini et Alice Parmentier. Traduzione in italiano dell'avv. Roberto Valsangiacomo

4) Garantire che lo studio, nella sua qualità di responsabile del trattamento, rispetti il suo dovere di informazione nei confronti delle persone i cui dati personali sono trattati.

Le informazioni che devono essere comunicate sono elencate agli art. 13 e 14 del GDPR e 17 del p-LPD; le eccezioni e restrizioni agli art. 13, comma 4, e 14, comma 5, del GDPR e 18 p-LPD.

Sono elencati qui di seguito alcuni accorgimenti concreti implementabili:

- sulla base del registro (cfr. cifra 2), allestire un documento ("privacy notice") relativo al trattamento dei dati personali dei clienti e degli impiegati e collaboratori dello studio, fermo restando che il dovere di informare riguarda anche i motivi giustificativi che sono alla base del trattamento;
- decidere in merito al miglior modo possibile di comunicare tali informazioni alle persone interessate, in particolare ai clienti e ai collaboratori (attuali e futuri) dello studio.

5) Sottoporre a revisione il modello di contratto di mandato d'avvocato / la lettera di incarico o il modello di procura da far sottoscrivere al cliente in uso presso lo studio.

Il contratto di mandato d'avvocato, rispettivamente la lettera d'incarico, oppure, perlomeno, il modello di procura in uso presso lo studio, da far firmare al cliente, possono essere dei buoni mezzi atti a: (i) adempiere al dovere di informazione nei confronti delle persone interessate (cfr. cifra 4) e (ii) ottenere, se necessario, il loro accordo quanto ai processi di trattamento dei dati personali che non sono coperti da un diverso motivo giustificativo.

6) Definire i processi adottati al fine di trattare le richieste provenienti dalle persone interessate.

Revisionare le metodiche di archiviazione degli incartamenti e gli strumenti informatici in uso presso lo studio, al fine di permettere allo studio di dare un riscontro, entro un periodo di tempo e a un costo ragionevoli, ad un'eventuale domanda di accesso ai dati personali proveniente da una persona interessata.

7) Definire come operare nel caso di un "data leak".

Definire cosa intraprendere all'interno dello studio nel caso di un "data leak" (perdita di dati personali): quali persone-chiave in seno allo studio devono essere informate? Chi adotta la decisione di prendere contatto, se necessario, con le autorità?

Come informare le persone interessate? A chi spetta occuparsi delle particolarità concernenti le relazioni pubbliche?

8) Revisionare i contratti di appalto sottoscritti, implicanti il trattamento dei dati personali.

Revisionare i contratti di appalto sottoscritti (in particolare nel caso dell'esternalizzazione dello stoccaggio dei dati), alla luce delle nuove normative, in particolare l'art. 28 GDPR. Assicurarsi, in particolare, della fattiva collaborazione degli interessati nel caso di domande provenienti da una persona interessata.

9) Esaminare se occorra designare un rappresentante in seno all'Unione europea.

Qualora lo studio sia assoggettato al GDPR, deve, in linea di principio, nominare un "rappresentante" nell'Unione europea. Avrà, in particolare, l'obbligo di essere il punto di contatto per le autorità dell'Unione europea in materia di protezione dei dati personali. Delle eccezioni all'obbligo di nominare un rappresentante figurano, ad ogni buon conto, all'art. 27, comma 2, GDPR.

10) Prestare attenzione ai rischi connessi con un'eventuale violazione delle nuove normative.

Il GDPR e il p-LPD prevedono numerose sanzioni di carattere penale e/o amministrativo. Oltre a tali sanzioni, qualora un'autorità dovesse comunicare pubblicamente che uno studio di avvocati non rispetti le normative in materia di protezione dei dati personali, per lo studio potrebbe concretizzarsi un grave rischio reputazionale.

Lugano, 13 dicembre 2018