

ADEMPIMENTI

Dal CNF le buone prassi per la sicurezza dei dati

di Lucia Recchioni

Nella giornata di ieri, 22 maggio, il **Consiglio Nazionale Forense** ha diffuso delle nuove [linee guida in materia di protezione dei dati personali](#), le quali, pure essendo specificatamente rivolte agli **avvocati**, possono fornire utilissimi spunti di riflessione a tutti i **professionisti**, soprattutto in considerazione del clima di incertezza che regna a pochi giorni dalla piena applicazione del [Regolamento UE 679/2016](#).

Tra l'altro, in allegato alle linee guida è fornito un **modello di informativa** ai sensi dell'**articolo 13 Regolamento UE 679/2016**, il quale potrà rappresentare un importante punto di riferimento in considerazione dei nuovi **obblighi di informativa ai clienti** che scatteranno dal prossimo **25 maggio**, che, come noto, imporranno non solo di **adottare i nuovi modelli** a fronte dei nuovi incarichi conferiti, ma anche di adeguare **l'informativa già fornita**.

Tutto ciò premesso concentriamoci soprattutto sulla **seconda parte del modello**, liberamente consultabile sul sito del Consiglio Nazionale Forense, la quale altro non è se non una **raccolta di schede pratiche**.

Innanzitutto viene chiarita la distinzione tra **titolare del trattamento** e **contitolari del trattamento**, fornendo un esempio: la differenza non è di poco conto in quanto, nel caso in cui vi sia **contitolarietà del trattamento** si renderà necessario un **esplicito accordo interno** con il quale dovranno essere definiti le **responsabilità** e gli **obblighi** dei **singoli contitolari**.

Sul punto viene quindi chiarito che, nel caso in cui, ad esempio, **due avvocati** abbiano ricevuto **distinti mandati** dallo **stesso cliente** per **prestazioni diverse**, seppur connesse, **non** si realizza un'ipotesi di **contitolarietà**: è il classico caso del cliente che affida la **difesa in sede civile** ad un avvocato e la **difesa penale** ad un altro avvocato.

Se, invece, lo **stesso mandato** è conferito a **più colleghi** si ritiene che in questo caso scatti l'obbligo di formulazione di uno **specifico accordo interno**, ravvisandosi **contitolarietà** del trattamento.

Tutto quanto premesso, nel documento si sofferma poi l'attenzione su uno dei **nuovi adempimenti** introdotti dalla disciplina, ovvero l'obbligo di **tenuta del registro dei trattamenti**.

Sul punto si reputa utile ricordare che il suddetto registro si rende obbligatorio non solo in tutto i casi in cui l'**organizzazione presenti più di 250 dipendenti**, ma anche quando il **trattamento** "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".

Le linee guida ritengono pertanto che il **registro dei trattamenti** sia **obbligatorio** anche per gli **avvocati**, sebbene presentino un numero di dipendenti decisamente inferiore alla prevista soglia, se il trattamento si riferisce a **particolari fatti relativi a condanne o sanzioni**: sarà quindi **obbligatorio il registro del trattamento** per gli avvocati che si occupano di **diritto penale** o di **diritto di famiglia e minori**, ma sarà parimenti necessaria l'istituzione del registro se l'avvocato si occupa di **diritto della previdenza sociale** o di vertenze in materia di **risarcimento danni da lesioni personali**.

In considerazione dell'ampio numero delle fattispecie richiamate pare quindi evidente che, come anche sottolineato nelle linee guida, la **possibilità che un avvocato tratti solo dati comuni e non sia quindi obbligato alla tenuta del registro è un'ipotesi quasi di scuola**.

Questa interpretazione si scontra, in parte, con quella fornita dal **CNDCEC** e dalla **Fondazione Nazionale dei Commercialisti** con il documento dello scorso **27 aprile** (si rinvia, a tal proposito, all'articolo "[Consulenza in materia di privacy anche per gli iscritti all'Albo](#)").

In quest'ultimo documento, infatti, la tenuta del registro **non è stata ritenuta obbligatoria**, sebbene **fortemente consigliata** ("*nonostante il registro dei trattamenti previsto dal GDPR non sia obbligatorio per gli studi professionali, se ne consiglia l'adozione*").

Dubbi potrebbero quindi sorgere se si considera che anche i professionisti dell'**area fiscale** trattano spesso **dati relativi alla salute** dei propri clienti al fine di consentirne la detrazione delle spese, sicché l'adozione del registro del trattamento potrebbe ritenersi non solo **fortemente consigliata**, ma addirittura **obbligatoria**.

Tornando però a concentrare l'attenzione sul documento, non può sfuggire un'interessante sezione, dedicata a "**L'adozione di buone prassi per la sicurezza dei dati**".

Le **linee guida** distinguono quindi **due fattispecie**:

- la **conservazione cartacea dei documenti**,
- la **conservazione informatica**.

Nel primo caso dovremo "mettere in atto **misure di sicurezza fisica nello studio**", come, ad esempio:

- **limitare l'accesso agli uffici**,
- **non archiviare i documenti in locali accessibili a tutti**,
- **installare allarmi**.

Nel secondo caso, invece, le misure da porre in essere sono ovviamente diverse, e il

documento suggerisce le seguenti:

1. **autenticare gli utenti** e impostare una **password personale** che presenti almeno 8 caratteri con lettere minuscole, maiuscole, numeri e caratteri speciali. La **password non potrà essere scritta** su un foglio accessibile a tutti, **non potrà essere condivisa** e dovrà essere **modificata** regolarmente;
2. **individuare le persone** che possono accedere ai dati personali e rimuovere le autorizzazioni di accesso obsolete,
3. scrivere un **regolamento sull'utilizzo del computer** da inserire nel regolamento interno dello studio (se adottato),
4. fornire **mezzi di crittografia** per i **computer portatili** e per i **dispositivi di archiviazione removibili**, come ad esempio le **chiavette USB**,
5. **evitare di memorizzare i dati sensibili dei clienti**,
6. eseguire il **backup regolarmente** e **conservare i supporti di backup in un luogo sicuro**.

Da ultimo merita una riflessione anche la sezione del documento dedicata all'individuazione del **responsabile del trattamento**.

Troviamo infatti scritto che “*i soggetti a cui lo studio comunica i dati personali trattati sono considerati responsabili del trattamento (es. commercialista, consulente del lavoro, consulente, fornitori di servizi digitali, conservatori di documenti informatici, ecc.)*”.

Ricordiamo quindi, a tal proposito, che l'[articolo 28 Regolamento UE 679/2016](#):

- impone al titolare del trattamento di **ricorrere unicamente a responsabili del trattamento** (e quindi anche a consulenti fiscali e del lavoro) **che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate** in modo tale che il trattamento soddisfi i requisiti della disciplina *privacy*;
- sancisce l'obbligo di **stipulare un contratto tra titolare e responsabile del trattamento**, dettagliandone il contenuto.



Direzione Scientifica: Sergio Pellegrino, Giovanni Valcarenghi e Paolo Meneghetti