Protezione dei dati personali

Adempimenti per il singolo professionista

Codice per la protezione dei dati personali – T.U. - D.Lgs 30 giugno 2003, n. 196

Regolamento generale sulla protezione dei dati - Regolamento UE 2016/679

Sull'applicazione della normativa vigila l'Autorità Garante per la protezione dei dati personali

https://www.garanteprivacy.it/

I singolo professionista è tenuto a alcuni adempimenti:

- sicurezza informatica
- documentare l’analisi dei rischi
- autodenunciare una violazione di sicurezza
- aggiornare le informative e i consensi

Corso di circa 4 ore gratuito organizzato dal CSI su https://www.teachmood.it

La situazione delle associazioni e delle società tra professionisti è più complessa. Adempimenti quali la la nomina di un responsabile della protezione dei dati o la stesura della valutazione di impatto non sono stati espressamente esclusi per chi svolge la professione non in forma individuale.

Sicurezza informatica

- crittografia server
- dispositivi mobili con password
- salvataggio dati ridondante
- gestione password

Dedicare un po' di tempo a fare un'analisi dei rischi ed al suo aggiornamento ed adeguare gli strumenti, che siano o meno elettronici, migliora anche la gestione documentale, quella del tempo nonché la qualità del lavoro e del servizio offerto.

Documentare l’analisi dei rischi

- Analisi dei rischi: con qualche minimo adeguamento sui contenuti (ad esempio riportando in allegato le valutazioni di impatto del trattamento, DPIA, ed il registro degli incidenti), il DPS potrebbe diventare la descrizione del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI)
- DPIA: Provvedimento del Garante (11 ottobre 2018): Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto
- Registro dei trattamenti (erede del Documento programmatico sulla sicurezza, obbligatorio fino al 2012) non si applica alle imprese o organizzazioni con meno di 250 dipendenti

Attenzione alla norma di esonero dall’obbligo di tenere i registri dei trattamenti: se si trattano dati sensibili o altri dati particolari il registro va istituito (comma 5 art. 30 GDPR – Regolamento Generale sulla Protezione dei Dati – UE/2016/679). Le analisi dei rischi dipendono invece dal tipo di attività professionale svolta.

Obbligo di autodenuncia

- L'art. 4 del regolamento europeo definisce la violazione dei dati personali come "*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*"
- Evento doloso (attacco informatico) o accidentale (accesso abusivo, incidente, smarrimento di chiavetta USB, sottrazione di documenti con dati personali , furto di un notebook)
- L'art. 33 del GDPR prevede l'obbligo di notificare alle autorità di controllo la violazione dei dati, tranne che nel caso in cui "*sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche*" (perdita di una chiavetta usb con dati cifrati). La notifica deve avvenire "*senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza*" il titolare. Qualora la notifica non avvenga nelle 72 ore, il titolare dovrà indicare i motivi del ritardo.

Informative e consensi

- Nei rapporti con i committenti non è esplicitamente previsto se i professionisti debbano farsi nominare responsabili del trattamento dai propri committenti che trasferiscono dati di persone fisiche. L'aspetto è particolarmente rilevante a fronte della necessità di sottoscrivere un contratto e della responsabilità civile solidale (tra titolare e responsabile esterno del trattamento). In materia i garanti europei (riuniti nell'organismo chiamato WP29) hanno affermato che la questione dipende dal grado di autonomia nell'esecuzione dell'incarico. Nella prassi, probabilmente, la gestione dei dati per conto di un cliente sposta al professionista la qualifica di responsabile esterno.
- Informazioni normate dal GDPR al Capo III Diritti dell'interessato, artt. 12, 13, 14
- Acquisizione del consenso normata da GDPR al Capo II Principi, artt. 7 e 8

Consenso punti 1 e 2 art.7 GDPR

1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante

Privacy_Presentazione.pdf
Informativa ai sensi dell’art. 13.docx
Informativa ai sensi dell’art. 13.pdf
Regolamento UE 2016 679. Regolamento sulla Protezione dei Dati.pdf
Tabella adempimenti GDPR.pdf
Decalogo GDPR.pdf

https://we.tl/t-JLs6fiaRgw