Studio dott. Fulvio Divina

Evoluzione normativa

Legge n. 675 del 31 dicembre 1996

DPR 28 luglio 1999 n. 318

D.Lgs 28 dicembre 2001 n. 467

D.Lgs 30 giugno 2003 n. 196

Regolamento Ue/2016/679

Non c'è un disciplinare tecnico delle misure di sicurezza

Responsabilità del titolare di definire le misure di sicurezza idonee

Accountability

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

[doc. web n. 1147314]

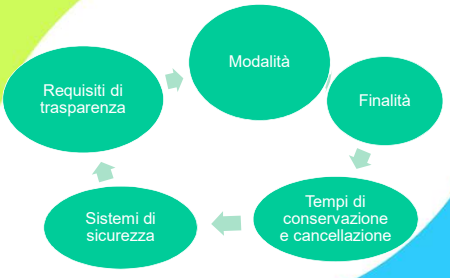
Autorizzazione n. 4 del 1998 - Trattamento dei dati sensibili da parte dei liberi professionisti - 30 settembre 1998
(G. U. n. 229 del 1 ottobre 1998)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

AUTORIZZA

i liberi professionisti iscritti in albi o elenchi professionali a trattare i dati sensibili di cui all'articolo 22, comma 1, della legge n. 675/1996, secondo le prescrizioni di seguito indicate.

Trattamento dei dati



Il regolamento europeo richiede misure

sufficienti

Non fornisce indicazioni specifiche

La valutazione viene rimessa alla responsabilità del titolare

Tutela dei soli dati personali (persone fisiche)

Sono escluse dalla tutela i dati delle persone giuridiche

Quali dati vengono tutelati?

«*qualsiasi informazione riguardante una persona fisica identificata o identificabile*»

Principi cardine del regolamento

- Responsabilizzazione
- …ed essere in grado di dimostrare ….
- Consenso dell'interessato (art. 4) *qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile ….*

Consenso mediante
dichiarazione scritta
anche attraverso mezzi elettronici
orale (principio di libertà delle forme)

Non configura consenso il silenzio, l'inattività o la preselezione di caselle

Il titolare del trattamento deve sempre dimostrare che l'interessato ha prestato inequivocabilmente il proprio consenso

Se il consenso non viene dato per iscritto come si fa a dimostrare ?

Quando il consenso viene dato all'interno di un contratto deve essere esposto in modo chiaramente distinguibile e in forma comprensibile.

Diritto di revoca del consenso

Deve essere sempre indicato nell'informativa comunicata all'interessato

Il consenso è revocato con la stessa facoltà con cui è accordato.

Limitazione della conservazione dei dati (art. 5)

Per un arco temporale non superiore a quello strettamente necessario per il raggiungimento delle finalità per cui i dati sono trattati

Indicare nel contratto concluso con il cliente il periodo di conservazione

D.P.O.

Data Protection Officer – responsabile della protezione dei dati

La sua nomina è obbligatoria solo se i trattamenti e monitoraggi dei dati vengono fatti in modo regolare e sistematico degli interessati su larga scala……

Non obbligatorio per gli studi professionali e le aziende

La nomina è obbligatorio per gli Enti Pubblici.

E' consigliabile la nomina di un referente GPDR

Ogni misura adottata dovrà essere documentabile

Registro dei trattamenti non è obbligatorio (<250 dipendenti) ma se ne consiglia l'adozione

Informative ai clienti

Strumenti in cluod es. google drive, office 365

Il gestore dello spazio virtuale esterno dovrà essere nominato responsabile del trattamento per conservazione dei dati dei nostri clienti per i quali conserviamo la titolarità.

Dobbiamo autorizzare i nostri collaboratori ad effettuare il trattamento dei dati personali degli interessati

Titolare del trattamento: persona che determina le finalità e i mezzi del trattamento dei dati personali

prende decisioni in relazione alle finalità del trattamento;

impartisce istruzioni e direttive;

svolge funzioni di controllo.

Responsabile del trattamento: la persona che tratta dati personali per conto del titolare

In caso di furto o perdita di dati va comunicato entro 72 ore al Garante

Assicurare il cyber risk

MASSIMALE ANNUO	PREMIO ANNUO (massimo 7 addetti)	PREMIO AGGIUNTIVO (per ogni addetto)	FRANCHIGI
€ 50.000	€ 245,00	€ 37,00	€ 2.500
€ 100.000	€ 367,00	€ 52,00	€ 2.500
€ 150.000	€ 489,00	€ 73,00	€ 2.500
€ 250.000	€ 612,00	€ 91,00	€ 2.500

PERDITA E RIPRISTINO DI DATI compresi decontaminazione e recupero

PERDITA DI PROFITTO per interruzione delle attività aziendali a seguito di attacco informatico, falle nella sicurezza della rete, errore umano, errore di programmazione

BUSINESS INTERRUPTION

SPESE LEGALI ivi comprese quelle per far valere le penali contrattuali

SPESE DI ESTORSIONE O RISCATTO derivante da una minaccia credibile, con l'intento di pubblicare, diffondere, distruggere o utilizzare informazioni riservate o tutelate, archiviate nel sistema informatico dello studio

SPESE PER L'INCARICO DI ESPERTI IN SICUREZZA INFORMATICA per il contenimento del danno (gestione crisi, pubbliche relazioni, negoziazione, ecc)

RESPONSABILITA' CIVILE per danni derivanti dalla violazione dei dati (GDPR)

INCIDENT RESPONSE e costi investigativi con il supporto di una linea diretta e multilingue, attiva 24/7, per il supporto in situazioni di crisi

Casi pratici

Non avete mai fatto nulla?

Avete già adempiuto al precedente dettato normativo?