cgn

FISCO [7]

Autrice: Giulia Zecca

CENTRO STUDI CGN

Privacy in Studio: guida operativa per Commercialisti e Consulenti del Lavoro

Dalla teoria alla pratica, come organizzare la privacy nello studio professionale con metodo e consapevolezza



Ultimo aggiornamento: 2/2/2026

EBOOK GRATUITO

Indice

Prefazione **5**

Introduzione **7**

Soggetti obbligati 8

Definizioni fondamentali 8

1. Ruoli e adempimenti **10**

1. Ruoli 10

2. Adempimenti 10

2.1 I Registri 11

2.1.1 Il Registro del trattamento 11

2.1.2 Il Registro dell'amministratore di sistema o Registro degli accessi 13

2.1.3 Il Registro delle violazioni – data breach 13

2.1.4 Il Registro della formazione 15

2.1.5 Il Registro dei penetration test 16

2.1.6 Il Registro delle disaster recovery 16

2.1.7 Il Registro dell'esercizio dei diritti da parte degli interessati 16

2.1.8 Il Registro dei visitatori 17

2.2 L'informativa 17

2.3 La valutazione d'impatto 20

2.4 La comunicazione della violazione 21

2. Sanzioni e casi di controllo **23**

1. Sanzioni 23

2. Casi di controllo 24

Introduzione

Il testo normativo di riferimento in tema di protezione dei dati è il General Data Protection Regulation (GDPR) cioè il Regolamento generale sulla protezione dei dati 2016/679 del Parlamento Europeo e del Consiglio approvato il 27 aprile 2016 ed entrato in vigore dal 25 maggio 2018.

L'art. 1 definisce le finalità del Regolamento: proteggere i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali e la libera circolazione di tali dati.

È proprio nel GDPR che vengono stabiliti i diritti dell'interessato negli artt. 7, 15, 16, 17, 18, 19, 20, 21, 22 e 77 e i principi applicabili al trattamento dei dati personali trovano riferimento dall'art. 5 all'art. 11.

Il Comitato europeo per la Protezione dei Dati (sigla inglese: EDPB) è un organismo indipendente dell'Unione europea con sede a Bruxelles, il cui scopo è garantire un'applicazione coerente del Regolamento generale sulla Protezione dei Dati e promuovere la cooperazione tra le autorità di protezione dei dati dell'UE.

Il Garante per la Protezione dei Dati Personali (GPDP, anche detto Garante della privacy) è un'autorità amministrativa indipendente istituita dalla cosiddetta legge sulla privacy (legge n. 675 del 31 dicembre 1996) e successivamente disciplinata dal Codice in materia di protezione dei dati personali (decreto legislativo n. 196 del 30 giugno 2003) come modificato dal decreto legislativo n. 101 del 10 agosto 2018, che ha anche istituito il Garante per la protezione dei dati personali come autorità di controllo incaricata di vigilare sull'applicazione del Regolamento generale sulla protezione dei dati (ai sensi dell'articolo 51 del Regolamento n. 2016/679).

Soggetti obbligati

La norma non ha previsto un elenco tassativo dei soggetti obbligati ma tramite la FAQ del 8/10/2018 il Garante afferma l'obbligo della tenuta del registro dei trattamenti per "qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti delle categorie particolari di dati di cui all'articolo 9, paragrafo 1 del GDPR, o di dati personali relativi a condanne penali e a reati di cui all'articolo 10 del GDPR". Tra gli esempi riportati nella FAQ sono indicati i liberi professionisti con almeno un dipendente e/o che trattino dati sanitari e/o dati relativi a condanne penali o reati (es. commercialisti, notai, avvocati, fisioterapisti, farmacisti, medici).

È ragionevole dedurne che i commercialisti che redigono la dichiarazione dei redditi ed entrano in contatto con dati sanitari sono soggetti obbligati.

Definizioni fondamentali

L'articolo 4 del GDPR fornisce le definizioni, tra quelle presenti ne estrapoliamo alcune:

- **dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- **trattamento:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- **titolare del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- **responsabile del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare;
- **archivio:** qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- **consenso dell'interessato:** qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile, con la quale manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i suoi dati personali siano oggetto di trattamento;
- **violazione dei dati personali:** 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.