

## Gestione della privacy negli studi professionali: il sostegno della bilateralità

La protezione dei dati personali costituisce oggi una componente strutturale dell'organizzazione degli studi professionali. L'intensificazione dei flussi informativi, la digitalizzazione dei processi e l'utilizzo diffuso di strumenti tecnologici (cloud, software gestionali, interoperabilità dei dati) hanno ampliato significativamente l'esposizione ai rischi connessi al trattamento delle informazioni.

In questo contesto, la formazione in materia di privacy assume un ruolo centrale: non più mero adempimento accessorio, ma leva organizzativa essenziale per garantire conformità normativa, gestione del rischio e tutela dei diritti degli interessati.

### Il quadro normativo

Il quadro normativo in materia di protezione dei dati personali è oggi caratterizzato dalla compresenza di norme giuridicamente vincolanti e di standard volontari, i quali sono tra loro integrabili benché operanti su piani distinti.

La cornice giuridica è rappresentata dal Regolamento (UE) 2016/679 (GDPR), applicabile in tutti gli Stati membri dal 25 maggio 2018. Il GDPR si inserisce in un percorso evolutivo già avviato con il d.lgs. 30 giugno 2003, n. 196 ("Codice Privacy"), che disciplinava le modalità di raccolta e trattamento dei dati personali da parte di soggetti pubblici e privati. Con il Regolamento europeo si è affermato un cambio di paradigma: dalla logica dell'adempimento formale si è passati alla responsabilizzazione del titolare del trattamento. Emblematico è il principio di accountability il quale, infatti, impone non solo il rispetto delle disposizioni normative, ma anche la capacità di provare l'adeguatezza delle misure adottate.

Dal canto loro, gli standard ISO/IEC quali le certificazioni 27001, 27002 e 27001, sono un sistema di linee guida volontarie e certificabili per tradurre i principi del legislatore comunitario in procedure concrete di gestione e controllo.

Entrambi gli strumenti richiedono una gestione di dati personali basata su un **approccio risk-based** e promuovono la consapevolezza della responsabilità di tutti coloro chiamati a tutelare la riservatezza delle informazioni personali.

### Gli sviluppi recenti: dalla compliance alla resilienza organizzativa

L'evoluzione più recente della materia evidenzia un progressivo spostamento dalla conformità documentale alla gestione integrata dei processi.

In questa direzione si colloca un recente documento del Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili, richiamato anche dalla stampa specializzata, che propone il

superamento del paradigma conformativo in favore di un modello orientato alla **resilienza organizzativa**, intesa come capacità dello studio di garantire trattamenti in modo fluido e lecito attraverso protocolli strutturati, capaci di prevenire l'errore umano, mitigare le vulnerabilità tecniche e contrastare minacce cibernetiche.

Tale approccio trova concreta attuazione nel **Privacy Information Management System (PIMS)** un "framework organico" di governance, procedure e controlli che consente di gestire le informazioni personali (PII) in modo strutturato e secondo logiche di miglioramento continuo (cosiddetto "Ciclo PDCA": Plan-Do-Check-Act).

Questo cambio di prospettiva impone una revisione continua dei trattamenti e delle misure adottate, rendendo centrale il ruolo della formazione nella prevenzione degli errori e nella gestione consapevole dei dati.

### La prassi degli Ordini professionali e delle associazioni di categoria

Il vademecum del Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili evidenzia come la gestione della privacy negli studi debba **[1]** evolvere verso modelli organizzativi strutturati, superando una logica meramente adempitiva.

In tale prospettiva:

- la privacy non è più un obbligo episodico, ma un processo continuo;
- il principio di accountability non è delegabile;
- il vertice dello studio è direttamente responsabile delle scelte organizzative;
- è necessario destinare risorse adeguate (economiche e umane) alla compliance.

Ulteriori contributi chiariscono inoltre come il ruolo del professionista nel trattamento dei dati (titolare o responsabile) dipenda dal grado di autonomia decisionale esercitato nelle singole attività. A titolo esemplificativo, si riportano alcune attività operative che rientrano nella responsabilità del titolare dello studio in materia di protezione dei dati personali.

#### Alcuni compiti nell'agenda dello studio-titolare\*

Censire/mappare tutti i dati (clienti, terzi, dipendenti)

Definire la base giuridica (contratto, legge, consenso) per ogni finalità

Eseguire, quando obbligatoria, una valutazione di impatto privacy (DPIA) per nuovi software cloud o trattamenti ad alto rischio

Formalizzare gli atti di nomina per tutti i responsabili esterni (IT, Cloud)

Stipulare accordo di contitolarità in caso di database condivisi con altri

### **Alcuni compiti nell'agenda dello studio-titolare\***

colleghi
Definire tempi certi di conservazione e distruzione dei dati
Osservare modalità sicure per lo smaltimento dei supporti (carta/hard disk)
Inviare dati sensibili esclusivamente via canali cifrati
Mappare i servizi Cloud collocati fuori UE
Effettuare una periodica revisione della sicurezza
Far firmare a ogni collaboratore un impegno di riservatezza
Formare specificamente i collaboratori sui cyberattacchi
Cifrare chiavette USB e laptop
Assegnare a ogni collaboratore credenziali uniche
Attivare l'autenticazione a due fattori su e-mail e cloud

\* Tabella tratta da "Professionisti a prova di privacy" de Antonio Ciccina Messina, Italia Oggi, 30 marzo 2026

### **La formazione: un obbligo essenziale**

Sebbene il GDPR non preveda un obbligo esplicito di formazione, quest'ultima costituisce una misura organizzativa imprescindibile ai fini dell'attuazione del principio di accountability e della sicurezza del trattamento, risultando de facto necessaria per la corretta applicazione della normativa.

La formazione rimane uno strumento essenziale per garantire la corretta applicazione delle procedure interne, ridurre il rischio di violazioni e assicurare la consapevolezza dei soggetti autorizzati al trattamento. A maggior ragione quando il trattamento ha ad oggetto dati sensibili (sanitari, giudiziari, fiscali), la consapevolezza del personale di studio forma un fondamentale presidio di sicurezza.

Così come per la salute e sicurezza sui luoghi di lavoro, anche la tematica privacy richiede una "alfabetizzazione" iniziale volta a impartire le nozioni di base, e una formazione specifica modulata in funzione di ruoli e mansioni.

Tale impostazione trova conferma anche nella prassi professionale più recente secondo la quale il vertice dello studio è tenuto a destinare risorse adeguate – economiche e organizzative – per assicurare la conformità alla normativa, soprattutto in presenza di criticità o non conformità riscontrate. In ambito applicativo, ciò si traduce nella definizione di obiettivi concreti e verificabili, come il completamento della formazione da parte della totalità dei collaboratori e l'aggiornamento periodico sui principali rischi informatici, inclusi phishing e minacce cyber.

## La formazione privacy nel sistema della bilateralità

Nel sistema delineato dal CCNL degli Studi e Attività professionali, la formazione rappresenta un ambito di intervento specifico della bilateralità.

E.BI.PRO., in coerenza con le proprie finalità istituzionali, prevede una **misura dedicata** al rimborso delle spese sostenute per la formazione in materia di privacy, rivolta ai datori di lavoro e ai lavoratori degli studi professionali. Come anche rilevato in guide informative pubblicate in passato dall'Ente, la copertura economica delle attività formative rimane uno strumento fondamentale per supportare gli operatori nell'adempimento degli obblighi normativi e nella gestione consapevole dei dati personali.

Il regolamento della misura di cui sopra, stabilisce che E.BI.PRO. rimborsa ai datori di lavoro parte delle spese sostenute per la formazione in materia di privacy, propria e dei dipendenti dello studio.

Per accedere al rimborso è necessario:

- applicare il CCNL degli Studi e Attività professionali;
- essere iscritti alla bilateralità da almeno due mesi alla data di avvio del corso;
- essere in regola con i contributi bilaterali[2].

Le attività formative ammesse al rimborso sono esclusivamente quelle presenti nei cataloghi accreditati presso Fondoprofessionij, il fondo paritetico interprofessionale del settore[3]. Il rimborso è pari al 60% del costo sostenuto (IVA esclusa), elevato al 100% per i soggetti aderenti anche a Fondoprofessionij, entro un massimale di 500 euro per richiesta.

## Una logica integrata di gestione del rischio

La crescente complessità del quadro normativo e tecnologico impone agli studi professionali di adottare un approccio sempre più strutturato alla gestione dei rischi connessi al trattamento dei dati personali.

In tale prospettiva, la **formazione in materia di privacy** – sostenuta attraverso il rimborso finora trattato della **Gestione Ordinaria** di E.BI.PRO. – rappresenta uno strumento di natura preventiva, volto a ridurre la probabilità di errori, violazioni e comportamenti non conformi.

Accanto a tali strumenti, il sistema bilaterale offre anche forme di tutela di carattere successivo. In particolare, nell'ambito della **Gestione Professionisti** dell'E.BI.PRO., è prevista la **Garanzia Cyber Risk**, che assicura la copertura delle perdite patrimoniali involontariamente cagionate a terzi in conseguenza di violazioni della privacy o del sistema informatico.

Le due misure, pur rispondendo a finalità differenti, risultano tra loro complementari: la formazione incide sulla probabilità del rischio, mentre la copertura assicurativa interviene sugli effetti economici del rischio.

## Bibliografia e fonti

- E.BI.PRO., La privacy per lo studio professionale
- E.BI.PRO., Il Regolamento UE 2016/679: adempimenti per gli studi professionali
- Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili, La gestione della privacy negli studi professionali alla luce della normativa ISO/IEC 27701:2025
- Giuseppe Vaciago, La gestione della privacy in studio a braccetto con la sicurezza informatica, Il Sole 24 Ore, 24 marzo 2026
- Antonio Ciccina Messina, Professionisti, privacy à la carte, Italia Oggi, 24 marzo 2026
- Antonio Ciccina Messina, Professionisti a prova di privacy, Italia Oggi, 30 marzo 2026
- E.BI.PRO., Regolamento rimborso spese formazione in materia di privacy
- Gestione Professionisti<sup>®</sup>, Garanzia Cyber Risk

## Note:

[1] Gli autori del vademecum precisano che l'obiettivo dello stesso non sia quello di «introdurre ulteriori livelli di complessità organizzativa, ma piuttosto di fornire ai professionisti un quadro di riferimento che consenta di gestire in modo efficace e sostenibile gli adempimenti privacy» (Eliana Quintili, "La gestione della privacy negli studi professionali alla luce della normativa ISO/IEC 27701:2025", pag. 1).

[2] Per maggiori dettagli si rinvia alla consultazione del **Regolamento amministrativo CA.DI.PROF.**, del **Regolamento amministrativo E.BI.PRO.** nonché alla visione dei contenuti informativi di supporto disponibili nella pagina "Le istruzioni" nella sezione del sito [www.ebipro.it](http://www.ebipro.it) "Come aderire".

[3] I fondi paritetici interprofessionali per la formazione continua operano nell'ambito della disciplina di cui all'art. 118 della L. 23 dicembre 2000, n. 388 e successive modificazioni. L'accesso alle risorse avviene attraverso procedure formalizzate (avvisi pubblici, cataloghi accreditati o piani formativi aziendali), che prevedono criteri di ammissibilità, requisiti di accreditamento degli enti formatori, verifica della coerenza dei contenuti con i fabbisogni del settore, valutazione tecnico-economica dei progetti e controlli documentali e amministrativi. I percorsi sono soggetti a monitoraggio in itinere ed ex post, con obblighi di rendicontazione, tracciabilità delle spese e verifica della corretta erogazione delle attività formative. Tali meccanismi assicurano standard di qualità, trasparenza e utilizzo vincolato delle risorse destinate alla formazione continua dei lavoratori.

24 aprile 2026