Consiglio Nazionale
dei Dottori Commercialisti
e degli Esperti Contabili

DOCUMENTO

# La gestione della privacy negli studi professionali alla luce della normativa ISO/IEC 27701:2025

18 MARZO 2026

AREE DI DELEGA CNDCEC
Compliance e modelli organizzativi per le imprese

CONSIGLIERE DELEGATO
Eliana Quintili

COMMISSIONE DI STUDIO CNDCEC
Privacy studi professionali

PRESIDENTE
Simone Campigli

Consiglio Nazionale
dei Dottori Commercialisti
e degli Esperti Contabili

# Composizione del Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili

### Presidente
Elbano de Nuccio

### Vice Presidente
Antonio Repaci

### Consigliere Segretario
Giovanna Greco

### Consigliere Tesoriere
David Moro

### Consiglieri
Gianluca Ancarani
Marina Andreatta
Cristina Bertinelli
Aldo Campo
Rosa D'Angiolella
Michele de Tavonatti
Fabrizio Escheri
Gian Luca Galletti
Cristina Marrone
Maurizio Masini
Pasquale Mazza
Eliana Quintili
Maria Lucetta Russotto
Pierpaolo Sanna
Liliana Smargiassi
Giuseppe Venneri
Gabriella Viggiano

## Collegio dei revisori

### Presidente
Rosanna Marotta

### Componenti
Maura Rosano
Sergio Ceccotti

# Commissione di studio CNDCEC “Privacy studi professionali”

## Consigliera CNDCEC delegata

Eliana Quintili

## Presidente

Simone Campigli

## Segretario

Luciana Capo

## Componenti

Francesca Brega
Nathaniel Casadei
Angelo Lucio Cavallari
Rachelina Di Mauro
Alessandro Elisio
Giacomo Greci
Tiziana Guggino
Lapo Liguori
Nicola Nicoliello
Ottorino Pomilio
Claudio Sica
Edoardo Soglia
Guido Sorvillo
Michela Turri

# Sommario

Premessa 1

1. Introduzione 2
   - 1.1. Obiettivi del documento: dalla conformità legale alla resilienza organizzativa 2
   - 1.2. Il concetto di Privacy Information Management System (PIMS) 3
2. Quadro normativo di riferimento 3
   - 2.1. Rapporto tra norme cogenti (GDPR) e standard volontari (ISO) 3
   - 2.2. Novità: la ISO/IEC 27701:2025 (Protezione dei dati personali) 4
   - 2.3. Il valore della certificazione come strumento di *accountability* 5
3. Una nuova definizione di strategia basata sul rischio (*Risk-Based Approach*) 6
   - 3.1. Dal rischio per l'organizzazione ai rischi per i diritti e le libertà degli interessati (ISO/IEC 27701) 6
   - 3.2. Integrazione tra valutazione d'impatto (DPIA) e *Risk Assessment* 7
4. Impostazione del sistema di gestione privacy 8
   - 4.1. Leadership e pianificazione: definizione della politica e degli obiettivi di protezione 8
   - 4.2. Governance e ruoli: un esempio di rapido modulo di verifica per la leadership 10
   - 4.3. Responsabilità dei titolari, dei responsabili (e del DPO) 11
   - 4.4. Consapevolezza e risorse: i programmi di formazione continua 14
5. Gestione operativa e controlli 16
   - 5.1. Controlli specifici per il titolare (Annex A): trasparenza, consenso, gestione delle richieste degli interessati e Privacy by Design 16
   - 5.2. Controlli Specifici per il Responsabile (Annex B): sicurezza nel trattamento per conto terzi, sub-fornitori e catena del valore 17
   - 5.3. Controlli di cybersecurity 18
   - 5.4. Monitoraggio e miglioramento continuo 19

ALLEGATO 23

Check-list per l'analisi dei rischi "*Privacy-Centric*" 23

## Premessa

La crescente digitalizzazione dei processi professionali e l'evoluzione del quadro normativo europeo hanno reso la protezione dei dati personali una componente strutturale dell'organizzazione e dello svolgimento dell'attività professionale. Gli studi dei Commercialisti, infatti, trattano quotidianamente una quantità significativa di dati personali riferibili a clienti, collaboratori e soggetti terzi, spesso caratterizzati da particolare rilevanza sotto il profilo economico, patrimoniale e, in taluni casi, anche giudiziario. In tale scenario la corretta gestione dei dati personali, oltre che un obbligo giuridico derivante dal Regolamento (UE) 2016/679 (GDPR), rappresenta un parametro essenziale di qualità e affidabilità dell'attività professionale.

Con il presente documento si intende offrire agli studi professionali uno strumento operativo per gestire in modo consapevole e organizzato i principali adempimenti in materia di protezione dei dati personali, valorizzando al contempo le opportunità offerte dagli standard internazionali di riferimento. In particolare, il documento prende in esame l'evoluzione dello standard ISO/IEC 27701:2025, che introduce un modello avanzato di Privacy Information Management System (PIMS) e rafforza l'integrazione tra protezione dei dati personali, sicurezza delle informazioni e governance organizzativa.

Nell'illustrare tali strumenti, occorre sempre tenere presente che gli studi professionali si caratterizzano per una notevole eterogeneità organizzativa: accanto a strutture di dimensioni medio-grandi, dotate di articolazioni interne e processi più complessi, operano numerosi studi di dimensioni ridotte o individuali, nei quali l'attività professionale si svolge attraverso assetti organizzativi più snelli e semplificati. In tale prospettiva, gli strumenti e i modelli proposti devono essere letti come riferimenti metodologici flessibili, che possono essere adattati in modo proporzionato alla struttura, ai rischi e al volume dei trattamenti effettuati dallo studio.

L'obiettivo del documento, pertanto, non è 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, favorendo al contempo lo sviluppo di una cultura organizzativa orientata alla responsabilizzazione (*accountability*), alla prevenzione dei rischi e al miglioramento continuo.

Eliana Quintili

*Consigliera CNDCEC delegata Area "Compliance e modelli organizzativi delle imprese"*

# 1. Introduzione

## 1.1. Obiettivi del documento: dalla conformità legale alla resilienza organizzativa

L'esercizio della professione di Commercialista implica strutturalmente il trattamento di ingenti flussi di dati personali afferenti a clienti e soggetti terzi. Tale operatività impone il rigoroso rispetto del quadro normativo delineato dal Regolamento UE 2016/679 (GDPR).

Il sistema della protezione dei dati si fonda sul principio di responsabilità generale (*accountability*) del Titolare, il quale risponde di ogni operazione di trattamento effettuata direttamente o per il tramite di soggetti esterni qualificati come Responsabili del trattamento. Lo studio professionale, a seconda del contesto operativo e della natura della prestazione, può assumere la veste giuridica di Titolare o di Responsabile, con la conseguente e precisa ripartizione delle obbligazioni legali.

In virtù di tale ruolo, il Titolare è tenuto a implementare misure tecniche e organizzative adeguate ed efficaci, volte a garantire la sicurezza e a comprovare la conformità delle attività di trattamento (onere della prova). Parallelamente, il Responsabile del trattamento è vincolato all'assolvimento di compiti istruttori e operativi da cui derivano precise responsabilità contrattuali e di legge.

Entrambe le figure sono soggette ai poteri ispettivi e sanzionatori dell'Autorità garante per la protezione dei dati personali. La mancata conformità espone lo studio a sanzioni amministrative, provvedimenti inibitori e, non da ultimo, ad azioni risarcitorie per i danni cagionati agli interessati. In tale scenario, la corretta gestione dei diritti degli interessati – richieste di accesso, rettifica, cancellazione, limitazione, opposizione e portabilità – rappresenta un elemento critico della gestione del rischio professionale.

Oltre il perimetro della compliance legale, lo studio deve tendere alla resilienza organizzativa. Tale paradigma assicura che il trattamento avvenga in modo fluido e lecito attraverso protocolli strutturati, capaci di prevenire l'errore umano, mitigare le vulnerabilità tecniche e contrastare minacce cibernetiche. L'obiettivo è garantire la tutela dei diritti degli interessati mediante l'applicazione dei principi di *Privacy by Design* e *by Default*, assicurando la continuità operativa anche in presenza di criticità.

Un modello metodologico d'eccellenza per strutturare tale sistema è rappresentato dallo standard UNI CEI EN ISO/IEC 27701:2025 (di seguito, ISO 27701), il quale definisce i requisiti per un evoluto *Privacy Information Management System* (PIMS).

### 1.2. Il concetto di Privacy Information Management System (PIMS)

Il *Privacy Information Management System* (PIMS) rappresenta l'evoluzione dei sistemi di gestione della sicurezza delle informazioni, estendendo il focus dalla generica integrità delle informazioni alla specifica protezione dei dati personali, al fine ultimo di tutelare i diritti e le libertà delle persone fisiche.

Il PIMS si configura come un framework organico di governance, procedure e controlli volto a gestire le informazioni personali (PII) in modo sistematico; integra i controlli della sicurezza informatica con i requisiti specifici per la protezione della privacy, adottando la metodologia del miglioramento continuo (Ciclo PDCA - *Plan-Do-Check-Act).*

Il presente documento, ispirandosi agli allegati normativi dello standard ISO 27701, intende fornire strumenti operativi che possono contribuire a consolidare la conformità legale e la resilienza organizzativa di uno studio professionale.

## 2. Quadro normativo di riferimento

### 2.1. Rapporto tra norme cogenti (GDPR) e standard volontari (ISO)

Il quadro normativo in materia di protezione dei dati personali si caratterizza per la coesistenza di norme giuridicamente vincolanti e di standard volontari, che operano su piani distinti ma tra di loro integrabili.

In tale contesto si colloca il rapporto tra il GDPR e gli standard internazionali di riferimento.

Il GDPR costituisce la cornice normativa cogente che prescrive principi e responsabilità obbligatorie per chi tratta dati di persone fisiche, mentre gli standard ISO/IEC, quali le certificazioni 27001, 27002 e 27701, offrono linee guida volontarie e certificabili per tradurre quei principi in procedure concrete di gestione e controllo.

Integrare questi due livelli consente di costruire un sistema di gestione della privacy robusto, che unisce conformità legale e migliori pratiche organizzative.

Entrambi gli strumenti richiedono una gestione dei dati personali basata su un **approccio *risk-based*** e promuovono la consapevolezza della responsabilità dei Titolari e dei Responsabili del trattamento.

Tuttavia, mentre il GDPR detta le regole che tutte le organizzazioni e gli studi professionali devono rispettare, la ISO 27701 offre una guida per migliorare le misure di sicurezza e ridurre il rischio di incidenti e illeciti nel trattamento dei dati personali.

Sul piano attuativo, l'adozione di misure tecniche e organizzative appropriate per la protezione dei dati personali richiesta dal GDPR si traduce, nello standard, in un **sistema di gestione della sicurezza**

**e delle informazioni personali** (PII), che richiede azioni necessarie a garantirne la riservatezza *(confidentiality*), l'integrità e la disponibilità, attraverso un sistema strutturato e proporzionato alle caratteristiche strutturali e di esposizione al rischio di una determinata organizzazione o studio professionale.

## 2.2. Novità: la ISO/IEC 27701:2025 (Protezione dei dati personali)

La nuova versione della ISO 27701 introduce innovazioni strutturali rilevanti, tra cui l'autonomia dello standard, l'allineamento al modello Annex SL e la semplificazione del quadro dei riferimenti normativi.

Tale innovazione rappresenta un'evoluzione significativa nel panorama degli standard internazionali per la protezione dei dati personali, segnando il passaggio dello standard da semplice strumento aggiuntivo a vero e proprio **standard autonomo e certificabile in modo indipendente.**

Già a partire dal titolo, *Information security, cybersecurity and privacy protection – Privacy information management systems (PIMS) – Requirements and guidance*, la ISO 27701 riconosce il ruolo della protezione dei dati personali come disciplina gestionale a sé stante e completa, nonostante continui a mantenere una forte integrazione con i sistemi di sicurezza tecnica delle informazioni.

Mentre l'edizione del 2019 era concepita come estensione delle ISO 27001 e 27002, presupponendo l'esistenza di un sistema di gestione della sicurezza delle informazioni (ISMS), la nuova versione dello standard consente alle organizzazioni di adottare un sistema di *Privacy Information Management System* (PIMS) pur in assenza di altra certificazione.

Questa scelta riflette un **cambiamento sostanziale** di prospettiva: la protezione dei dati personali non è più considerata un sottoinsieme della sicurezza informatica, ma un sistema di gestione con propri obiettivi, processi, ruoli e responsabilità, orientati specificamente alla protezione dei diritti e alle libertà degli interessati.

Questo assetto amplia l'ambito applicativo dello standard, rendendolo adottabile anche da organizzazioni non interessate alla certificazione, ma orientate a strutturare una gestione dei dati personali conforme e sicura.

Lo standard, acquistando autonomia, è ora strutturato come tutti gli altri standard del sistema ISO, essendo stato allineato all'Annex SL.

Di conseguenza, dopo le clausole introduttive di prassi, il suo testo si articola in dieci clausole di gestione (dalla 4.1 alla 10.2), che coprono i seguenti temi:

- il **contesto dell'organizzazione** e le parti interessate;
- la **leadership** e il ruolo del top management nella governance della privacy;
- la **pianificazione**, inclusa la valutazione dei rischi per i dati personali;

- il **supporto** (risorse, competenze, consapevolezza e comunicazione);
- le **operazioni** di trattamento;
- la **valutazione delle prestazioni** e il monitoraggio del PIMS;
- il **miglioramento continuo**.

La sua configurazione come standard autonomo, non subordinato ad altri sistemi di certificazione, ne fa una guida completa, che, in linea con il GDPR, integra stabilmente la protezione dei dati nei livelli decisionali e strategici dell'organizzazione.

Infatti, la norma non contiene più i richiami diretti alle serie ISO 27000, 27001 e 27002 e mantiene come riferimento esterno principale la sola ISO/IEC 29100:2024 (*Privacy framework*).

Gli allegati della ISO 27701 (Annex), inoltre, sono stati riorganizzati e consolidati. In particolare, è stato introdotto un nuovo allegato contenente 29 controlli di sicurezza delle informazioni rilevanti per la privacy, che coprono ambiti quali:

- politiche e governance,
- classificazione delle informazioni,
- gestione delle identità e degli accessi,
- rapporti con fornitori e responsabili del trattamento,
- formazione e consapevolezza del personale.

Sotto l'aspetto dei controlli interni, invece, la nuova edizione ha mantenuto una **sostanziale uniformità** rispetto all'edizione 2019. Questo aspetto è particolarmente rilevante per le organizzazioni già certificate, poiché consente una transizione graduale e sostenibile fino all'**ottobre 2028**, mese entro il quale le organizzazioni dovranno aver adeguato il proprio sistema al nuovo standard.

Nel complesso, la nuova edizione della norma, al di là della certificazione, consente a un'organizzazione come uno studio professionale di strutturare in modo più consapevole e sistematico l'attuazione del principio di *accountability* nell'attuale contesto storico e tecnologico.

### 2.3. Il valore della certificazione come strumento di *accountability*

La certificazione ISO 27701 costituisce, nel quadro del GDPR, uno strumento concreto di attuazione dell'*accountability*, agevolando sia la conformità alla disciplina in materia di protezione dei dati sia la dimostrazione del suo effettivo rispetto.

Infatti, l'adozione di un PIMS certificato implica che l'organizzazione consideri la privacy come pratica integrata nella propria *governance*, coinvolgendo i vertici gerarchici e attribuendo le responsabilità operative in modo netto, chiarendo:

- l'ambito di applicazione del sistema;

- i ruoli e le responsabilità in materia di protezione dei dati;
- i processi decisionali e di controllo relativi ai trattamenti.

Il valore della certificazione si manifesta, quindi, nel superamento di un approccio esclusivamente documentale alla conformità legale.

La protezione dei dati personali passa da una conformità prevalentemente descrittiva, spesso affidata a singole valutazioni o report, a una gestione sostanziale e continuativa, integrata nei processi decisionali e di governo dell'organizzazione. La certificazione attesta, infatti, non solo l'esistenza di politiche e documenti formali, ma l'effettivo funzionamento del sistema di gestione privacy in quanto sottoposto a controlli interni strutturati, piuttosto che a valutazioni o report sporadici.

La certificazione ISO 27701, inoltre, contribuisce a rafforzare la fiducia di clienti, partner commerciali e autorità di controllo, rendendo verificabile e comunicabile l'impegno dell'organizzazione per la protezione dei dati personali. Tale aspetto, in contesti caratterizzati da elevata professionalità e competitività, può favorire la permanenza sul mercato di un'organizzazione o di uno studio professionale.

Sul piano interno, il PIMS certificato consente di gestire in modo ordinato l'intero ciclo di vita dei dati personali, dalla raccolta alla conservazione fino alla cancellazione, integrando *privacy* e sicurezza nei processi aziendali, comportando l'adozione di strumenti organizzativi, quali i registri dei trattamenti, la classificazione dei dati, le politiche di accesso e conservazione, le procedure per la gestione di incidenti e *data breach*.

## 3. Una nuova definizione di strategia basata sul rischio (*Risk-Based Approach*)

L'evoluzione dello standard rafforza e precisa l'approccio *risk-based* già previsto dal GDPR, introducendo una prospettiva più avanzata e sostanziale. Il rischio non è più valutato esclusivamente in funzione degli impatti negativi sull'organizzazione, ma viene analizzato principalmente in relazione alle **conseguenze in ordine ai diritti e alle libertà fondamentali delle persone fisiche**. Questo cambio di prospettiva incide positivamente sulle modalità di progettazione, gestione e controllo dei trattamenti di dati personali.

### 3.1. Dal rischio per l'organizzazione ai rischi per i diritti e le libertà degli interessati (ISO/IEC 27701)

L'approccio *risk-based* assume oggi una valenza strategica più ampia rispetto al passato, poiché la protezione dei dati personali non deve limitarsi all'adozione di misure standard, ma richiede una valutazione continua dei trattamenti, tenendo conto del contesto organizzativo, della natura dei dati

trattati e, soprattutto, dei rischi per i diritti e le libertà delle persone fisiche. La nuova edizione sancisce questa evoluzione, richiedendo che le misure tecniche e organizzative vengano periodicamente riesaminate e aggiornate in funzione della trasformazione dei trattamenti, delle tecnologie utilizzate e del contesto operativo.

Il focus si sposta dal rischio per l'organizzazione al rischio per gli interessati, in linea con l'impostazione del GDPR.

La valutazione d'impatto sulla protezione dei dati (DPIA) e gli altri strumenti di analisi del rischio, di conseguenza, entrano a far parte di un processo più ampio, volto a garantire che i trattamenti di dati personali tengano conto degli effetti sui diritti e sulle libertà delle persone fisiche e vengano costantemente monitorati ed esaminati.

Sotto tale aspetto le misure introdotte dalla ISO 27701 sono coerenti con l'evoluzione dei modelli di gestione e controllo, richiedendo valutazioni strutturate e processi di miglioramento continuo[1].

### 3.2. Integrazione tra valutazione d'impatto (DPIA) e *Risk Assessment*

Un elemento centrale della nuova impostazione è l'integrazione tra la valutazione d'impatto sulla protezione dei dati (DPIA) prevista dal GDPR e il processo di valutazione dei rischi richiesto dal PIMS.

La DPIA è obbligatoria se un trattamento comporta rischi elevati per i diritti e le libertà degli interessati e deve essere svolta prima dell'avvio del trattamento.

Anche la ISO 27701 richiede una valutazione strutturata e anticipata dei rischi per i diritti e le libertà delle persone. Tale valutazione si integra con la DPIA prevista dal GDPR, consentendo di evitare duplicazioni di analisi e di documentazione e di mantenere coerenza tra obblighi normativi e requisiti dello standard.

All'interno di un PIMS strutturato, ora la DPIA può essere gestita come parte di un processo unico, che ricomprende l'analisi dei trattamenti, la valutazione dei rischi per la privacy, l'individuazione di misure adeguate, la documentazione delle decisioni assunte e l'aggiornamento periodico delle valutazioni in caso di cambiamenti organizzativi, tecnologici o normativi.

Questo approccio integrato tra DPIA e *Risk Assessment* all'interno del PIMS consente un esame complessivo dei rischi legati ai trattamenti di dati personali, prendendo in esame una realtà complessa, interconnessa e dinamica, anziché una somma di parti isolate.

In tal modo viene costituito un presidio volto a prevenire i rischi per i diritti e le libertà delle persone, da un lato migliorando la qualità e l'affidabilità delle decisioni organizzative e la loro conformità

[1] Per un approfondimento sull'allineamento tra approcci basati sul rischio in ambito privacy e modelli di controllo interno, con riferimento agli standard SOC 1 (SSAE 18) e ISAE 3402, si veda: - GUGGINO T., *Analisi dei modelli organizzativi e dimensionali, della motivazione del personale negli studi professionali. System and Organization Controls Report – SOC 1, SOC 2 e SOC 3 – Differenze e analogie con i Sistemi di Gestione della Qualità e della Sicurezza delle Informazioni*, in *Vision Pro*, Euroconference Editoria, n. 29/2020.

normativa, dall'altro riducendo le ridondanze documentali e semplificando le attività di controllo interno.

In conclusione, l'approccio *risk-based*, nella prospettiva della ISO 27701, non rappresenta un semplice strumento di valutazione, ma il nucleo operativo dell'*accountability*, attraverso il quale la protezione dei dati personali costituisce un sistema evolutivo, proporzionato ai rischi e al contesto[2].

# 4. Impostazione del sistema di gestione privacy

## 4.1. Leadership e pianificazione: definizione della politica e degli obiettivi di protezione

La politica per la protezione delle informazioni (*Privacy Information*) costituisce un documento programmatico che funge da vera e propria guida per l'intera organizzazione dello studio professionale ed è fondamentale non confonderla con la semplice informativa fornita ai clienti e terzi, in quanto si tratta di un'assunzione di responsabilità scritta e approvata dal professionista o dagli associati, che stabilisce i seguenti impegni:

- rispettare in modo rigoroso il GDPR e tutte le leggi applicabili;
- considerare la protezione dei dati personali, per la tutela dei diritti e delle libertà di clienti, dipendenti e collaboratori, come una priorità strategica inscindibile dall'attività professionale (cultura della protezione);
- istituire un quadro di riferimento che consenta di revisionare i processi, adattandoli alle nuove minacce tecnologiche, comprese quelle derivanti dall'Intelligenza artificiale (miglioramento continuo);
- comunicare tale politica e renderla accessibile a ogni livello dello studio e a tutte le parti interessate (trasparenza).

Il vertice dello studio professionale ha il compito di stabilire gli **obiettivi di privacy in modo chiaro e quantificabile**, affinché siano specifici, misurabili, raggiungibili, rilevanti e definiti nel tempo. L'efficacia di questi obiettivi viene misurata attraverso **Indicatori chiave di prestazione (KPI)** specifici.

Ecco alcuni esempi pratici di obiettivi privacy di uno studio professionale:

- **tempestività operativa:** ridurre il tempo di risposta alle richieste degli interessati (DSAR) al di sotto dei **15 giorni lavorativi**, migliorando significativamente il limite legale di 30 giorni;

[2] Per un approfondimento sui modelli organizzativi e sulla gestione del rischio negli studi professionali, v. GUGGINO T., *Analisi dei modelli organizzativi e dimensionali, della motivazione del personale negli studi professionali. Lo studio professionale e la gestione del rischio*, in *Vision Pro*, Euroconference Editoria, n. 27/2020.

- **competenza:** assicurare che il **100% dei collaboratori** completi una formazione specifica su sicurezza dei dati e rischi di phishing entro il primo semestre di ogni anno;
- **resilienza tecnica:** puntare ad azzerare i *data breach* dovuti a errori umani o configurazioni errate, implementando l'**autenticazione multi-fattore (MFA)** su tutti gli accessi remoti;
- **analisi preventiva:** condurre una valutazione d'impatto (DPIA) per ogni nuova tecnologia o software che tratti dati sensibili o giudiziari dei clienti prima della sua adozione.

Un controllo adeguato trasforma la privacy da semplice costo gestionale a **valore distintivo** per lo studio. Questo approccio garantisce che l'organizzazione non si limiti a evitare sanzioni, ma costruisca un ecosistema di fiducia capace di proteggere la propria reputazione professionale nel tempo.

Il mancato rispetto del principio di ***accountability*** espone il vertice dello studio professionale – ovvero i soci o il titolare – a gravi sanzioni che spaziano dall'ambito amministrativo a quello civile e reputazionale. Il vertice dello studio (soci o titolare) deve assumere un ruolo proattivo che non può essere trasferito a collaboratori o consulenti esterni.

In conformità alla clausola 5 della ISO 27701, la gestione delle non-conformità richiede l'impegno diretto dello studio professionale (soci o titolare), che non può essere delegato.

**Per soddisfare il requisito di *accountability*,** il vertice deve dimostrare il proprio impegno attraverso l'allocazione delle risorse necessarie (economiche o umane) per risolvere il problema rilevato. Sotto l'aspetto della ***governance*,** i partner devono partecipare direttamente alle scelte necessarie per riportare il sistema in conformità.

Una volta identificata una non-conformità (ad esempio, il mancato raggiungimento di un KPI - indicatore chiave di prestazione), lo studio struttura la propria azione secondo le seguenti fasi:

- **identificazione della causa,** per riconoscere ed esaminare i motivi del mancato conseguimento di un obiettivo privacy; ad esempio, se la formazione dei collaboratori è stata inferiore al 100%, la causa potrebbe consistere in una mancanza di tempo allocato o di strumenti adeguati;
- **formulazione di un piano d'azione,** per definire misure concrete atte ad eliminare la criticità rilevata; ad esempio, se il problema è tecnico, potrebbe essere risolto aggiornando tutti i dispositivi utilizzati;
- **revisione dei processi,** per aggiornare la politica della privacy con le modifiche necessarie a prevenire il ripetersi dell'errore.

Se l'esame di una non-conformità mette in evidenza che un obiettivo era irraggiungibile o non più rilevante, la fase di pianificazione (clausola 6) permette di ricalibrarlo, sempre rispettando il requisito di **misurabilità, che garantisce la formulazione di Indicatori chiave di prestazione (KPI)** chiari e quantificabili.

**Esempio di riallineamento:** se il target di risposta alle richieste degli interessati inferiore ai **15 giorni** non è stato rispettato, lo studio può decidere di investire in un software di automazione per garantire la tempestività richiesta.

### 4.2. Governance e ruoli: un esempio di rapido modulo di verifica per la leadership

Si espone qui di seguito un modulo rapidamente utilizzabile dalla leadership per verificare i principali requisiti di un sistema di protezione dei dati personali.

| Area di Controllo | Requisito / Verifica | Stato (Sì/No/Parziale) | Evidenze / Note Correttive |
|---|---|---|---|
| **1. Leadership** | Politica Privacy approvata formalmente dal Titolare/Soci | ☐ | |
| | Coerenza della politica con la cultura dello studio | ☐ | |
| | Partecipazione attiva del vertice alle decisioni privacy | ☐ | |
| | Responsabilità assegnate chiaramente (non delegate) | ☐ | |
| | Allocazione risorse (economiche, umane, tech) | ☐ | |
| | Documento di ambito PIMS redatto e aggiornato | ☐ | |
| | Registro dei Trattamenti (ex Art. 30) conforme | ☐ | |
| | Politica Privacy comunicata a tutto il personale | ☐ | |
| **2. Obiettivi & KPI** | Obiettivi definiti secondo criteri SMART | ☐ | |
| | KPI identificati e misurabili per ogni obiettivo | ☐ | |
| | Obiettivi approvati e rivisti annualmente dal vertice | ☐ | |
| | **KPI:** Tempo medio risposta DSAR < 15 giorni | ☐ | |
| | **KPI:** Formazione completata dal 100% dei collaboratori | ☐ | |

| | | | |
|---|---|---|---|
| | **KPI:** MFA (Multifactor) attivo su tutti i login remoti | ☐ | |
| | **KPI:** Zero data breach derivanti da errore umano | ☐ | |
| | DPIA preventiva per nuovi software/tecnologie | ☐ | |
| **3. Rischio** | Analisi dei rischi aggiornata (minacce attuali) | ☐ | |
| | Piano di trattamento dei rischi documentato | ☐ | |
| | DPIA eseguite per dati sensibili o nuove tecnologie | ☐ | |
| | Registro delle DPIA centralizzato e aggiornato | ☐ | |
| **4. Operatività** | Procedura DSAR documentata e testata | ☐ | |
| | Procedura gestione incidenti e Data Breach | ☐ | |
| | Registro incidenti (inclusi i "Near Miss") compilato | ☐ | |
| | Contratti e nomine Responsabili Esterni (Fornitori) | ☐ | |
| | Piano formativo annuale definito e tracciato | ☐ | |
| | Test di phishing o simulazioni periodiche effettuate | ☐ | |

## 4.3. Responsabilità dei titolari, dei responsabili (e del DPO)

Per poter garantire la conformità normativa di uno studio professionale, uno dei passaggi essenziali è rappresentato dalla corretta individuazione dei soggetti che intervengono nel trattamento dei dati personali. In generale le figure principali previste (o ricavabili) dal GDPR sono quattro: il Titolare, il Responsabile, gli Autorizzati e, ove previsto, il *Data Protection Officer* (DPO o anche RPD). La distinzione delle quattro figure dipende principalmente dal grado di autonomia decisionale esercitato dalle stesse sulle finalità e sui mezzi del trattamento

Il Titolare del trattamento

Il Titolare del trattamento è la persona fisica o la persona giuridica che determina le finalità e le modalità del trattamento dei dati personali; semplificando e sintetizzando il concetto, potremmo sostenere che il Titolare è colui che decide "*perché*" e "*come*" i dati devono essere trattati. Nel

contesto dello studio professionale, risulta evidente che il ruolo di Titolare è assunto dal Commercialista quando opera con autonomia decisionale e non si limita a svolgere attività meramente esecutive per conto del cliente.

In particolare, nel caso di uno studio con un solo professionista, il Titolare del trattamento sarà quest'ultimo mentre nel caso di uno studio associato/società tra professionisti, il Titolare sarà l'organizzazione e quindi i singoli professionisti non saranno mai considerati Titolari.

Dovendo essere in grado di dimostrare la conformità al GDPR, il Titolare mantiene una responsabilità generale di *accountability*; in particolare le sue principali responsabilità possono essere riassunte schematicamente come segue:

- adozione di adeguate misure tecniche e organizzative;
- stesura e consegna dell'informativa privacy agli interessati;
- gestione delle basi giuridiche del trattamento (incluso il consenso quando necessario);
- tenuta del registro dei trattamenti;
- designazione di eventuali Responsabili e Autorizzati;
- formazione del personale;
- gestione e registrazione di eventuali Data Breach.

Il Responsabile del trattamento

Il Responsabile del trattamento è il soggetto che tratta dati personali per conto del Titolare sulla base di un contratto (o altro atto giuridico) che ne disciplina puntualmente compiti, limiti e istruzioni operative. Il Commercialista assume questo ruolo quando opera senza autonomia decisionale, limitandosi a eseguire le istruzioni dettagliate del cliente: è il caso, per esempio, dell'attività di elaborazione dati e cedolini paga.

L'atto di nomina, tra le altre cose, deve specificare:

- durata, natura e finalità del trattamento;
- tipologia di dati trattati e categorie di interessati;
- obblighi e diritti del Titolare;
- misure di sicurezza da adottare.

Sulla base di quanto stabilito sopra, il Responsabile è pertanto tenuto a:

- trattare i dati in base alle istruzioni documentate impartite dal Titolare;
- garantire la riservatezza da parte del personale autorizzato;
- adottare adeguate misure di sicurezza;
- assistere il Titolare nell'adempimento degli altri obblighi previsti dal GDPR;
- cancellare o restituire i dati al termine del proprio incarico.

La distinzione tra le due figure, Titolare e Responsabile, è pertanto dovuta al grado di autonomia decisionale del professionista o dello studio professionale: quando decide finalità e mezzi del trattamento, opera come Titolare; quando invece si limita a eseguire istruzioni dettagliate del cliente, agisce come Responsabile.

Il GDPR prevede infine la possibilità di nominare dei Sub-Responsabili, purché tale nomina sia autorizzata dal Titolare e formalizzata per iscritto.

Gli Autorizzati al trattamento

Gli Autorizzati al trattamento, che nel precedente quadro normativo venivano denominati "*Incaricati*", sono rappresentati dai dipendenti, collaboratori o praticanti dello studio, i quali operano sotto l'autorità del Titolare o del Responsabile. Gli Autorizzati, pertanto:

- agiscono entro i confini ricevuti dal Titolare e/o Responsabile;
- devono essere adeguatamente formati;
- sono anch'essi vincolati all'obbligo della riservatezza;
- contribuiscono all'attuazione delle misure di sicurezza.

Pur non avendo alcuna autonomia decisionale, il loro operato incide direttamente sul livello di compliance dell'organizzazione, motivo per cui è fondamentale una chiara definizione dei profili autorizzativi.

Il DPO/RPD (ove previsto)

Il Responsabile della protezione dei dati, ove previsto, svolge una funzione di supporto, consulenza e sorveglianza sull'osservanza della normativa privacy.

In particolare, il DPO:

- informa e consiglia il Titolare o il Responsabile;
- sorveglia l'osservanza del GDPR e delle policy interne;
- fornisce pareri sulla valutazione d'impatto (DPIA);
- coopera con l'Autorità di controllo;
- funge da punto di contatto per gli Interessati.

La sua nomina non è sempre obbligatoria: nel caso di uno studio individuale, in linea generale, non è richiesta, mentre per studi associati o società tra professionisti l'obbligo va valutato anche in base alla dimensione e alla natura dei trattamenti effettuati.

La responsabilità del DPO, oltre a quella legale, è anche di tipo contrattuale nei confronti del soggetto per cui opera. Il DPO non è comunque personalmente responsabile per una violazione dei dati, la quale resta comunque in capo al Titolare; eventualmente è responsabile degli adempimenti dei compiti di vigilanza e consulenza che gli sono stati assegnati.

### 4.4. Consapevolezza e risorse: i programmi di formazione continua

La preparazione del personale chiamato a dare applicazione pratica alle regole e alle procedure codificate a tutela dei dati personali rappresenta una componente essenziale della "architettura privacy" in grado di suggellare o, al contrario, vanificare gli interventi tecnici e organizzativi progettati.

La **formazione** svolge quindi un ruolo centrale e strategico per gli studi professionali, costituendo uno degli strumenti principali per garantire un trattamento dei dati personali lecito, corretto e sicuro.

È essenziale, infatti, che le persone coinvolte nel processo di trattamento dei dati personali comprendano pienamente il valore dei dati trattati, i rischi associati e le responsabilità individuali che derivano dalle loro attività quotidiane. In particolar modo, quando il trattamento ha ad oggetto dati particolari (ad es. dati relativi alla salute, dati giudiziari, etc.) la consapevolezza del personale non è solo una misura organizzativa raccomandata, ma un vero e proprio presidio di sicurezza.

La maggior parte delle violazioni di dati deriva, infatti, da errori umani, comportamenti negligenti o scarsa conoscenza delle regole applicabili.

A partire dal GDPR (v. artt. 24 e 32), la formazione rappresenta una componente strutturale delle misure organizzative richieste al Titolare del trattamento.

Un riferimento esplicito all'obbligo formativo sussistente in capo al Titolare del trattamento è contenuto nell'art. 29 GDPR che stabilisce: "*il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento*".

La formazione costituisce, pertanto, un **obbligo essenziale** che il Titolare del trattamento è tenuto a rispettare per una corretta gestione dei dati dello studio da parte di dipendenti e collaboratori (ivi compresi tirocinanti e stagisti), svolgendo una funzione preventiva fondamentale dei rischi connessi al trattamento dei dati.

L'attività formativa può assumere forme diverse. A titolo puramente esemplificativo potrà avvenire attraverso:

- la partecipazione a corsi formativi (in presenza o in modalità telematica sincrona o asincrona);
- l'implementazione di regolamenti interni, linee guida (contenenti indicazioni specifiche su come gestire situazioni particolari che si verificano durante l'attività di trattamento);
- la condivisione di contenuti, ad esempio FAQ (al fine di dare risposte concrete ed immediate su alcuni dubbi che potrebbero sorgere nell'esecuzione delle funzioni di competenza) o *case history* in grado di fornire un ottimo ausilio per l'operatività dello studio;
- l'attuazione di iniziative di sensibilizzazione costante quali newsletter, campagne interne e comunicazioni periodiche;
- la messa a disposizione di un archivio di pareri e opinioni delle Autorità di controllo su temi di interesse per lo studio.

Affinché la formazione risulti efficace (e conforme ai dettami del GDPR) è fondamentale che non sia improvvisata.

Al contrario, sarà opportuno sviluppare un piano formativo, progettato e articolato in modo da essere incisivo per ogni autorizzato al trattamento. Ciò significa che ciascuno dovrà ricevere la formazione necessaria all'esecuzione delle proprie mansioni in modo conforme rispetto alla normativa *data protection*.

Quanto affermato rende imprescindibile l'adozione di un approccio strutturato e continuo, differenziato e modulato in base ai ruoli, alle qualifiche e alle responsabilità del singolo autorizzato, individuando piani formativi "su misura".

Andrà pertanto garantita una formazione generica di base, rivolta a tutto il personale autorizzato al trattamento, con l'obiettivo di diffondere e implementare la cultura della privacy (impartendo le conoscenze essenziali e i concetti fondamentali della normativa *data protection*), e una formazione specifica e approfondita per coloro che svolgono funzioni che comportano trattamenti complessi.

Mentre la formazione generica persegue l'obiettivo di fornire un'alfabetizzazione privacy volta ad impartire le nozioni di base per applicare la normativa vigente, la formazione specifica, invece, sarà modulata in funzione dei ruoli e delle mansioni.

Così, a titolo esemplificativo, chi tiene i contatti con la clientela dovrà essere istruito sull'erogazione dell'informativa privacy e sulla raccolta e conservazione dei consensi ove necessari ai sensi di legge; chi si occupa di nuove assunzioni dovrà essere edotto sugli adempimenti da osservare in fase di preassunzione (conservazione dei *curricula vitae*, trattamento di dati sensibili e altri aspetti delicati).

Entrando più nello specifico, per la formazione dei referenti privacy di uno studio professionale occorre prevedere sessioni formative riguardanti l'adempimento dei principali obblighi legali, come quelli connessi, ad esempio, alla tenuta dei registri (registri dei trattamenti, delle richieste di esercizio dei diritti degli interessati, dei *data breach*) e alla formalizzazione dei ruoli privacy di fornitori e consulenti esterni.

Quanto all'individuazione del giusto percorso formativo (anche ai fini del c.d. principio di rendicontazione), incombe sul Titolare del trattamento e sul Responsabile del trattamento la scelta delle soluzioni formative più adatte alla propria organizzazione.

Per studi di piccole dimensioni, dove i compiti non sono ripartiti e non vi è, pertanto, una distinzione netta delle mansioni, il piano formativo può avere ad oggetto i medesimi contenuti per tutti i partecipanti, senza comprometterne l'efficacia. Tuttavia, proprio la mancanza di distinzione di ruoli rende la formazione ancor più necessaria e fondamentale per il corretto svolgimento dell'attività dell'organizzazione stessa, avendo un peso maggiore rispetto alla formazione generica prevista per studi che abbiano figure interne specializzate.

Per testare l'efficacia della formazione è consigliabile, poi, valutare il reale grado di competenze acquisite dal personale attraverso, ad esempio, la somministrazione di test a risposta multipla in

grado di fornire importanti indicazioni sia sulle conoscenze acquisite dai soggetti valutati e il buon esito della formazione sia sulla necessità di integrare l'attività formativa.

Al fine di raccogliere evidenze dell'attività formativa del personale dello studio, **in linea con il principio di *accountability***, occorre predisporre un registro dei corsi e percorsi di apprendimento pianificati ed erogati, archiviare gli attestati formativi rilasciati ai dipendenti e ai collaboratori, i test somministrati e gli eventuali report riepilogativi rilasciati da consulenti incaricati della formazione privacy.

Al fine di rispettare il requisito della formazione continua, è buona prassi prevedere e programmare aggiornamenti periodici per tenere conto delle evoluzioni normative, dei nuovi orientamenti giurisprudenziali, degli interventi delle autorità di controllo, etc.

Un simile approccio proattivo sulla formazione contribuisce significativamente a rispettare la legge e anche a creare una reputazione attraverso una cultura fatta di consapevolezza e responsabilità.

# 5. Gestione operativa e controlli

Nella struttura della ISO/IEC 27701, si evidenzia come gli Annex trasformino i principi del GDPR in protocolli operativi per Titolari e Responsabili del trattamento attraverso un framework di lavoro che prevede la mappatura dei controlli specifici ISO e la gestione operativa di sicurezza (tecnici, organizzativi, fisici), facilitando la dimostrazione della conformità e la gestione del rischio privacy.

## 5.1. Controlli specifici per il titolare (Annex A): trasparenza, consenso, gestione delle richieste degli interessati e Privacy by Design

L'Annex A1 configura un framework rigoroso per la governance dei dati personali, delineando le responsabilità operative del Titolare attraverso quattro pilastri fondamentali riguardanti:

1) le condizioni per la raccolta e il trattamento (A.1.2), per la necessità di definire preventivamente le basi giuridiche e gli scopi del trattamento; l'enfasi è posta sulla documentazione probatoria, che include la registrazione del consenso e l'adozione di valutazioni di impatto (DPIA) per i trattamenti ad alto rischio o modificati;
2) la tutela dell'interessato (A.1.3), per strutturare un modello di trasparenza proattiva; il Titolare non deve solo informare chiaramente l'interessato, ma deve garantirgli l'esercizio effettivo dei diritti (accesso, rettifica, opposizione ecc.) e una gestione lecita dei flussi verso terze parti;
3) la protezione dei dati personali (A.1.4), integrando i principi di *Privacy by Design* e *by Default*, per minimizzare i dati; il ciclo di vita dei dati è presidiato dall'accuratezza iniziale fino alla distruzione definitiva (smaltimento), passando per la gestione dei file temporanei e la sicurezza nelle trasmissioni;

4) la gestione dei trasferimenti dei dati (A.1.5), con riferimento alla circolazione dei dati extra-giurisdizionale, subordinandola all'identificazione di basi giuridiche certe e a un sistema di tracciabilità (*logging*) delle divulgazioni e dei trasferimenti, essenziale per la cooperazione internazionale e la compliance normativa.

In sintesi, l'apparato dei controlli trasforma i principi astratti di protezione dei dati in protocolli operativi verificabili, spostando il baricentro della privacy dalla semplice compliance formale alla gestione proattiva del rischio informativo.

### 5.2. Controlli Specifici per il Responsabile (Annex B): sicurezza nel trattamento per conto terzi, sub-fornitori e catena del valore

L'impianto normativo dell'Annex A2 definisce il perimetro di responsabilità del soggetto che tratta dati per conto del Titolare, declinando il principio di *accountability* attraverso le seguenti quattro direttrici operative:

1) condizioni per la raccolta e il trattamento specifiche (A.2.2), poiché il Responsabile opera entro i confini di un mandato formalizzato ed è tenuto a un ruolo proattivo, per garantire il rispetto delle finalità contrattuali, escludere usi secondari (ad esempio, marketing) senza consenso e, soprattutto, agire come "sentinella normativa", segnalando al Titolare eventuali istruzioni che violino la legge;
2) obblighi nei confronti degli interessati al trattamento nell'ambito del rapporto con il Titolare (A.2.3), poiché la funzione del Responsabile si estende alla fornitura di strumenti e mezzi necessari affinché il Titolare possa evadere le richieste degli interessati, garantendo una cooperazione tecnica essenziale per la tutela dei diritti;
3) protezione dei dati personali (A.2.4), applicando il principio di *Privacy by Design*, che impone protocolli rigorosi per la gestione dei file temporanei, la sicurezza nelle trasmissioni e la capacità certificata di restituire o smaltire i dati al termine del rapporto, per una piena trasparenza sulle procedure interne;
4) gestione dei trasferimenti dei dati (A.2.5), con riferimento ai Sub-responsabili (ad esempio, Sub-appaltatori), subordinandola all'autorizzazione del Titolare, anche per quel che riguarda i trasferimenti transfrontalieri e le richieste delle autorità, in modo tale che il Responsabile funga da filtro critico, proteggendo i dati da accessi non legalmente vincolanti.

In conclusione, l'Annex A2 trasforma il Responsabile da mero esecutore a custode tecnico e partner della conformità, strutturando un sistema di verifiche che garantisce la tracciabilità e la sicurezza del dato lungo l'intera catena di fornitura.

### 5.3. Controlli di cybersecurity

L'Annex A3 rappresenta il punto di collegamento tra i controlli indicati nell'Annex A della norma ISO/IEC 27001:2022 e la tutela dei diritti dell'interessato. Attraverso 29 controlli mirati, la sezione fornisce indicazioni su come utilizzare i controlli della cybersecurity per assicurare in modo coerente e coordinato la riservatezza, l'integrità e la disponibilità dei dati personali.

Questa sezione è destinata sia ai Titolari che ai Responsabili del trattamento, in quanto entrambe le figure devono gestire i rischi di sicurezza delle informazioni presenti nei trattamenti effettuati con strumenti informatici.

Il framework può essere analizzato a partire dalle seguenti quattro dimensioni strategiche:

1) governance organizzativa della cybersicurezza (A.3.3 - A.3.16), inquadrando la sicurezza non come evento isolato, ma come processo continuo, con il dovere di definire politiche, ruoli e classificazioni basate sul rischio, permettendo in tal modo di allineare la protezione dei dati agli obiettivi di business; inoltre un atteggiamento proattivo nella gestione degli incidenti (A.3.11-12) e la previsione di revisioni indipendenti garantiscono che l'*accountability* non sia solo dichiarata, ma verificabile;
2) coinvolgimento del fattore umano, riservatezza e comportamenti del personale (A.3.17 - A.3.19), riconoscendo che il personale designato al trattamento dei dati personali costituisce un anello critico della catena dei controlli, che richiede formazione specifica, accordi di riservatezza e policy operative quotidiane (ad esempio, *Clean Desk*), per trasformare la cultura aziendale in una barriera contro il *social engineering* e l'errore umano;
3) sicurezza tecnologica, inclusa la gestione degli accessi (A.3.8 - A.3.26), per controllare le identità e gli accessi, con sistemi di autenticazione sicura e crittografia; inoltre, la gestione del ciclo di vita dei log (A.3.25) e dei backup (A.3.24) assicura non solo la difesa dai *data breach*, ma anche la resilienza e la capacità di ripristino dei dati trattati;
4) ingegneria e sviluppo sicuro (A.3.27 - A.3.31), dall'acquisizione delle applicazioni alla gestione rigorosa dei dati di test e delle terze parti, per prevenire vulnerabilità strutturali che potrebbero esporre i dati a rischi sistemici (questo aspetto non è sempre applicabile nella sua interezza). Coerentemente con il principio di *Privacy by Design*, i controlli di sicurezza riguardano l'intero ciclo di vita dello sviluppo software.

In conclusione, l'Annex A3 formalizza l'inscindibilità tra *Sicurezza delle Informazioni e Protezione dei Dati Personali (Data Security and PII Protection)*: la prima fornisce le infrastrutture e i protocolli, la seconda definisce il valore umano e giuridico da proteggere, creando un ecosistema di difesa robusto e conforme ai moderni standard internazionali.

## 5.4. Monitoraggio e miglioramento continuo

Il paragrafo dedicato al monitoraggio e miglioramento continuo si configura come l'elemento più dinamico e vitale all'interno dello standard ISO 27701. Questa sezione è fondamentale perché garantisce che il sistema di gestione non si riduca mai a un mero insieme di procedure statiche o a una raccolta formale di documenti. Al contrario, il monitoraggio e il miglioramento continuo rappresentano la forza propulsiva che mantiene il sistema attivo, efficace e in grado di adattarsi alle esigenze mutevoli dell'organizzazione e del contesto normativo e tecnologico.

L'approccio sistematico e costante impedisce che il Sistema di gestione perda la sua capacità di evolvere, promuovendo un ciclo virtuoso di verifica, analisi e perfezionamento. In questo modo, la gestione della privacy dello studio non si limita al rispetto formale delle regole e diventa parte integrante della cultura organizzativa, rafforzando la resilienza e la sostenibilità dell'intero sistema.

Il contesto normativo e tecnologico è in costante evoluzione e la gestione dei dati personali all'interno dello studio deve essere misurata, analizzata e migliorata in modo sistematico, condizione essenziale di sostenibilità del sistema.

Il percorso da seguire - seguendo il ciclo PDCA - può essere suddiviso come segue:

- Plan - pianificazione degli obiettivi privacy e dei controlli
- Do - implementazione delle misure
- Check - monitoraggio e verifica delle prestazioni
- Act - azioni correttive e miglioramento.

La valutazione delle prestazioni si concentra sulle ultime due fasi, "Check" e "Act", misurando la maturità reale dell'organizzazione.

L'attività di monitoraggio non deve limitarsi all'archiviazione di report, ma deve definire indicatori chiari, responsabilità ben delineate e modalità di misurazione obiettive.

Lo studio professionale tipicamente tratta dati fiscali, dati reddituali, dati personali di clienti, fornitori, dipendenti e di altri interessati collegati; dati anagrafici e dati particolari (es. invalidità, situazioni familiari, dati giudiziari).

Il sistema di gestione deve saper gestire l'errore attraverso un processo strutturato per:

a) identificare la non conformità,
b) analizzarne le cause,
c) definire azioni correttive,
d) verificarne l'efficacia.

Lo studio professionale deve essere capace di intervenire sulle cause, oltreché sugli effetti, poiché non basta chiudere una violazione documentale ma occorre comprendere la fonte del problema che

può derivare da una carenza formativa, da procedure e istruzioni poco chiare o da carenze organizzative e di leadership.

Per un valido monitoraggio delle attività dello studio possono essere utilizzati indicatori pratici che nel loro insieme devono dimostrare che i dati personali sono protetti.

Un buon sistema di monitoraggio deve consentire di individuare le criticità prima che diventino violazioni e non è importante la quantità di indicatori, ma la loro capacità di fornire informazioni utili al processo decisionale.

Lo studio che si approccia agli audit interni deve eseguirli con cadenza programmata al fine di verificare che il sistema di gestione sia implementato ed efficacemente mantenuto nel tempo.

Attraverso gli audit, che devono essere condotti da personale competente e imparziale, lo studio deve poter essere in grado di dimostrare:

- la conformità ai requisiti dello standard di riferimento;
- l'effettiva applicazione delle procedure;
- gli scostamenti da quanto pianificato e le aree di miglioramento.

Un audit efficace non si limita alla verifica documentale: analizza processi, responsabilità, consapevolezza del personale e coerenza operativa e garantisce che i risultati vengano comunicati ai responsabili competenti.

L'audit interno è il momento in cui devono emergere le reali fragilità del sistema di gestione.

Il vertice dello studio non può essere un attore passivo, dovendo:

- esaminare i risultati del monitoraggio;
- valutare incidenti e non conformità;
- considerare cambiamenti normativi e organizzativi;
- approvare azioni di miglioramento.

Questo passaggio traduce in pratica il principio di *accountability*: la protezione dei dati non è un tema esclusivamente tecnico o legale, ma una responsabilità di governance.

Il titolare dello studio (professionista o il legale rappresentante o associati) deve riesaminare il sistema di gestione, a intervalli pianificati, per garantirne la continua idoneità, adeguatezza ed efficacia.

L'attività di riesame non consiste in un controllo tecnico, bensì in una valutazione strategica per comprendere se il sistema di gestione è ancora idoneo o se serve apportare dei miglioramenti.

La periodicità del riesame è stabilita dal vertice dello studio, ma è opportuno prevedere attività di riesame straordinaria in alcune occasioni casi quali:

- *Data Breach*;

- cambiamenti organizzativi importanti (introduzione di nuove mansioni, soppressione di vecchie mansioni);
- nuove normative.

Il riesame deve includere:

- lo stato delle azioni intraprese dai precedenti riesami;
- i cambiamenti nelle questioni esterne e interne rilevanti per il sistema di gestione delle informazioni sulla privacy;
- i cambiamenti nelle esigenze e nelle aspettative delle parti interessate rilevanti per il sistema di gestione delle informazioni sulla privacy;
- informazioni sulle prestazioni del sistema di gestione delle informazioni sulla privacy, inclusi gli andamenti relativi a non conformità e azioni correttive, risultati del monitoraggio e delle misurazioni; risultati dell'audit;
- opportunità di miglioramento continuo.

Il riesame da parte di uno studio professionale deve essere concreto soffermandosi su aspetti riguardanti ad esempio:

- l'aggiornamento del registro dei trattamenti;
- le nomine di Autorizzati al trattamento e di Responsabili;
- la completezza delle informative e la loro correlazione con le attività di trattamento;
- le procedure applicate e la necessità di istruzioni operative;
- la formazione del personale (numero di eventi in un periodo di riferimento e valutazione dell'efficacia);
- la verifica degli accessi ai gestionali contabili e i relativi profili di autorizzazione;
- il monitoraggio della scadenza degli antivirus e di altre licenze o abbonamenti inerenti alla sicurezza informatica;
- lo stato delle misure di sicurezza fisica.

I risultati del riesame della direzione devono includere decisioni relative alle opportunità di miglioramento continuo e qualsiasi necessità di modifica al sistema di gestione.

Lo studio professionale deve rendere disponibili informazioni documentate come prova dei risultati del riesame da parte del vertice per deliberare sullo stato di adeguatezza del sistema di gestione e sulle attività di miglioramento o di correzione necessarie.

Il miglioramento continuo deve essere interpretato come uno strumento strategico per rafforzare la fiducia di clienti e partner e ridurre il rischio sanzionatorio, nonché per migliorare l'efficienza dei processi interni, non come un adempimento formale finalizzato al mantenimento di una certificazione.

Il verbale di riesame deve includere alcuni elementi essenziali. È importante specificare la data in cui si è svolta la riunione e indicare tutti i partecipanti presenti; vanno dettagliate le informazioni che sono state esaminate durante l'incontro e annotate le decisioni prese; bisogna inoltre descrivere le azioni previste, assegnare responsabilità precise e definire le tempistiche per l'attuazione delle attività.

Un miglioramento dei risultati può essere raggiunto nel tempo attraverso l'elaborazione di un sistema di indicatori fondato sull'Annex A della ISO 27701.

# Allegato

## Check-list per l'analisi dei rischi "*Privacy-Centric*"

La seguente check-list è stata elaborata partendo dai controlli tecnici della norma ISO 27701, adattandoli alle esigenze operative di uno studio professionale di Commercialista.

I contenuti sono da considerare quali esempi e non prescrizioni.

Lo studio, in quanto Titolare del trattamento, gestisce dati ad alto rischio (dati fiscali, giudiziari, reddituali).

### SEZIONE A: Lo studio come TITOLARE del Trattamento (PIMS Controller)

*Esempio di lista da compilare per i trattamenti di cui lo studio decide finalità e mezzi (es. gestione clienti diretti, dipendenti dello studio).*

| Rif. ISO | Controllo / Verifica Operativa | Esito (S/N/P) | Evidenze / Azioni Correttive |
|---|---|---|---|
| **1.** | **Pianificazione e Basi Giuridiche** | | |
| A.1.2.2 | È presente un censimento/mappatura di tutti i dati (clienti, terzi, dipendenti)? | ☐ | |
| A.1.2.3 | È stata definita la base giuridica (contratto, legge, consenso) per ogni finalità? | ☐ | |
| A.1.2.4 | Esiste un registro/log per dimostrare come e quando è stato prestato il consenso? | ☐ | |
| A.1.2.6 | È stata eseguita una DPIA per nuovi software cloud o trattamenti ad alto rischio? | ☐ | |
| A.1.2.7 | Sono stati formalizzati gli atti di nomina per tutti i Responsabili Esterni (IT, Cloud)? | ☐ | |
| A.1.2.8 | In caso di database condivisi con altri colleghi, esiste un accordo di contitolarità? | ☐ | |
| **2.** | **Trasparenza e Diritti degli Interessati** | | |
| A.1.3.3 | Le informative sono redatte in linguaggio chiaro e rese facilmente accessibili? | ☐ | |

| | | | |
|---|---|---|---|
| A.1.3.5 | Esiste una procedura tecnica per bloccare i dati in caso di revoca del consenso? | ☐ | |
| A.1.3.7 | Lo studio risponde alle richieste di accesso/rettifica/cancellazione entro 30 giorni? | ☐ | |
| A.1.3.8 | Viene notificato ai fornitori esterni l'aggiornamento o la rettifica dei dati dei clienti? | ☐ | |
| A.1.3.9 | È possibile esportare i dati in formato leggibile (XML/CSV) per la portabilità? | ☐ | |
| **3.** | **Privacy by Design & Conservazione** | | |
| A.1.4.2 | Viene applicata la minimizzazione (raccolta dei soli dati necessari alla pratica)? | ☐ | |
| A.1.4.7 | I file temporanei (Excel/PDF) vengono eliminati post-invio telematico? | ☐ | |
| A.1.4.8 | È definita una policy con tempi certi di conservazione e distruzione dei dati? | ☐ | |
| A.1.4.9 | Lo smaltimento dei supporti (carta/hard disk) avviene con modalità sicure? | ☐ | |
| A.1.4.10 | L'invio di dati sensibili avviene esclusivamente via canali cifrati (PEC/Portal)? | ☐ | |
| **4.** | **Trasferimenti Internazionali** | | |
| A.1.5.2 | È stato mappato se i servizi Cloud risiedono fuori UE (es. USA) e su quali basi? | ☐ | |
| A.1.5.5 | Esiste un registro delle divulgazioni effettuate ad Autorità (GDF, Giustizia)? | ☐ | |

## SEZIONE B: Lo studio come RESPONSABILE del Trattamento (PIMS Processor)

*Esempio di lista da compilare per le attività svolte "per conto dei clienti" (es. elaborazione paghe, contabilità terzi).*

| Rif. ISO | Requisito Operativo per il Responsabile | Esito | Note sulla Compliance |
|---|---|---|---|
| **1.** | **Istruzioni e Finalità** | | |
| A.2.2.2 | Esiste un atto di nomina (*ex* art. 28) firmato dal Cliente-Titolare? | ☐ | |
| A.2.2.4 | È garantito il divieto di utilizzo dei dati dei clienti per marketing dello studio? | ☐ | |
| A.2.2.5 | Lo studio segnala al cliente se le sue istruzioni violano il GDPR? | ☐ | |
| **2.** | **Supporto al Cliente** | | |
| A.2.2.6 | Lo studio fornisce al cliente i log e i report per la sua "Accountability"? | ☐ | |
| A.2.3.2 | Lo studio è in grado di estrarre i dati se un dipendente del cliente esercita un diritto? | ☐ | |
| **3.** | **Fine Rapporto e Catena di Fornitura** | | |
| A.2.4.3 | Esiste una procedura per restituire o distruggere i dati al termine del mandato? | ☐ | |
| A.2.5.7 | L'elenco dei sub-responsabili (software house) è stato comunicato al cliente? | ☐ | |
| A.2.5.5 | Esiste una procedura per avvisare il cliente in caso di richieste dati dalle Autorità? | ☐ | |

## SEZIONE C: Cybersecurity & Asset Protection

*Esempio di lista di controlli tecnici trasversali applicabili a tutta l'infrastruttura dello studio.*

| Area | Controllo Tecnico / Organizzativo | Esito | Dettaglio Tecnico |
|---|---|---|---|
| **Gov.** | Esiste una politica di sicurezza scritta e approvata dal Titolare? | ☐ | |
| **Audit** | Viene effettuata una revisione indipendente della sicurezza (annuale)? | ☐ | |
| **Staff** | Ogni collaboratore ha firmato un impegno di riservatezza (NDA)? | ☐ | |
| **Staff** | È stata effettuata formazione specifica anti-phishing nell'ultimo anno? | ☐ | |
| **Fisica** | Chiavette USB e laptop sono protetti da cifratura (es. Bitlocker)? | ☐ | |
| **Accessi** | Ogni utente ha credenziali uniche? (Divieto di password condivise) | ☐ | |
| **Accessi** | L'autenticazione a due fattori (MFA) è attiva su mail e cloud? | ☐ | |
| **Dati** | I backup sono quotidiani e con test di ripristino periodico? | ☐ | |
| **Log** | Il sistema registra gli accessi ai dati sensibili in modo inalterabile? | ☐ | |
| **Incident** | Esiste un piano d'azione in caso di Ransomware (isolamento rete/contatti)? | ☐ | |

**Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili**
Piazza della Repubblica, 59 00185 Roma