ORZINUOVI 30.09.2026

# AI nella professione: regole e informative

**Avv. Riccardo Berti**
Avvocato – Data Protection Officer
*riccardo.berti@rblex.it*

# Possiamo usare l'IA restando nel perimetro normativo?

- **Risposta breve: sì,** a condizione di non immettere nel sistema dati personali o altre informazioni riservate. Se quei dati servono (e spesso servono) la risposta diventa: **dipende**.
- **Riservatezza e segreto professionale.** Ricorrere a un sistema di IA non costituisce, in sé, violazione del dovere di riservatezza né del segreto professionale, se lo strumento è scelto fra prodotti affidabili e usato con le cautele già adottate per posta elettronica, gestionali e archivio documentale.
- **Selezione del fornitore:** il prodotto va scelto, non semplicemente installato (così come tutti i nostri strumenti informatici).
- **Cautele d'uso:** accessi nominativi, autenticazione forte, riservatezza delle credenziali.
- **Proporzione al dato:** il livello di garanzia richiesto cresce con la sensibilità delle informazioni immesse.
- **Da consumatore posso essere leggero, da professionista no.** Quando uso l'IA su pratiche, dati o documenti dei clienti la scelta dello strumento diventa una decisione organizzativa, motivata e documentata, con responsabilità civile e deontologica.

# Le IA non sono tutte uguali: quattro livelli di garanzia

| Livello | Metafora | Caratteristiche |
|---|---|---|
| **Generaliste (ChatGPT, Claude e analoghi)** | «Fast food» | Rapide, flessibili, adeguate a usi generici. |
| **DeepSeek** | «All you can eat» | Prestazioni elevate a costi contenuti, ma garanzie e flussi di dati da esaminare con attenzione. |
| **IA professionali** | «Ristorante» | Più strutturate: controlli, contratti e presidi generalmente compatibili con l'uso di Studio. |
| **Soluzioni premium** | «Stellato» | Governance, sicurezza, tracciabilità e supporto enterprise: il livello più alto di garanzia. |

- Al crescere del livello crescono governance, garanzie contrattuali e tracciabilità: è su questi elementi, non sulla sola qualità delle risposte, che si misura l'idoneità professionale dello strumento.
- Non serve un audit integrale del fornitore, ma tre passaggi proporzionati: scegliere fornitori affidabili con condizioni d'uso leggibili; chiedere garanzie (documentazione privacy, DPA, misure di sicurezza); ridurre il rischio con regole d'uso interne.

# Quattro domande prima di aprire il prompt

## 1 Intendo immettere dati personali?

Se no, gli adempimenti si riducono a: alfabetizzazione (art. 4 AI Act), informativa al cliente (art. 13 L. 132/2025), trasparenza (art. 50 AI Act, solo per alcuni contenuti diffusi). Più una verifica del contratto di licenza: niente licenze «as is»; estrazione dei dati possibile alla cessazione e in formati interoperabili.

## 2 Di chi sono i dati?

Se sono titolare (es. parere su una cartella ricevuta dal cliente) decido io e nomino il fornitore di IA mio responsabile. Se sono responsabile (ipotesi più frequente: dati di dipendenti, clienti, fornitori del cliente) il contratto con il cliente può vietare l'IA in cloud o imporre la comunicazione dei sub-responsabili → guardo alla Nomina

## 3 Sto acquistando un prodotto professionale?

Il fornitore deve riconoscere di trattare i dati per mio conto, con un Data Processing Agreement. I prodotti generalisti hanno condizioni standard pensate -di default- per l'utenza non professionale.

## 4 Dove vanno i dati?

Scala di affidabilità:

- dati in UE/SEE
- dati in paesi terzi con decisione di adeguatezza (es. Svizzera) USA con Data Privacy Framework
- dati in paesi terzi con sole clausole contrattuali standard

# Le quattro normative: si applicano in modo cumulativo, non alternativo

| Normativa | Cosa regola | Quando si applica in Studio |
|---|---|---|
| 1. Legge 132/2025<br>Legge italiana sull'IA | IA nelle professioni intellettuali solo per attività strumentali e di supporto, con prevalenza del lavoro intellettuale; informativa al cliente (art. 13). | Sempre, per il professionista che usa sistemi di IA. |
| 2. AI Act<br>Reg. (UE) 2024/1689 | Alfabetizzazione del personale (art. 4); trasparenza per chatbot e contenuti generati con IA (art. 50, dal 2.8.2026). | Sempre per l'alfabetizzazione; la trasparenza se l'IA interagisce con terzi o genera contenuti diffusi all'esterno. |
| 3. GDPR<br>Reg. (UE) 2016/679 | Ruoli privacy, nomina del fornitore, minimizzazione, addestramento, conservazione, trasferimenti extra-UE. | Se immetto dati personali di clienti, dipendenti o terzi. |
| 4. NIS2<br>Dir. (UE) 2022/2555 – D.Lgs. 138/2024 | Cybersicurezza dei soggetti essenziali e importanti e della catena di approvvigionamento. | Raramente in via diretta; più spesso di riflesso, se lo Studio è fornitore di un soggetto NIS2. |

**Lo stesso strumento di IA può dover rispettare tutte e quattro le discipline contemporaneamente.**

LEGGE 132/2025

# Art. 13: limite di contenuto e obbligo di informativa

> *«L'utilizzo di sistemi di intelligenza artificiale nelle professioni intellettuali è finalizzato al solo esercizio delle attività strumentali e di supporto all'attività professionale e con prevalenza del lavoro intellettuale oggetto della prestazione d'opera. Per assicurare il rapporto fiduciario tra professionista e cliente, le informazioni relative ai sistemi di intelligenza artificiale utilizzati dal professionista sono comunicate al soggetto destinatario della prestazione intellettuale con linguaggio chiaro, semplice ed esaustivo.»*

- **In vigore dal 10 ottobre 2025.** Attenzione: evitare l'IA è oggi quasi impossibile (correttori di Word, dettatura, smart compose, antispam evoluti).
- **Conseguenze dell'omessa informativa.** Nessuna sanzione espressa nella L. 132/2025; possibili contestazioni sulla debenza del compenso (violazione del comma 1, prevalenza del lavoro intellettuale «umano») e sanzioni disciplinari.

*Fonte: art. 13, commi 1 e 2, L. 23 settembre 2025, n. 132.*

LEGGE 132/2025

# Codice deontologico CNDCEC (agg. 21.11.2025)

- **Art. 21, c. 8 – Perimetro.** IA solo per attività strumentali e di supporto; l'esito della prestazione deve essere il risultato prevalente dell'attività intellettuale del professionista. Divieto di usare l'IA in sostituzione della valutazione o interpretazione di fatti e norme.
- **Art. 21, c. 9 – Responsabilità.** Il professionista assume piena responsabilità e controllo e deve: a) verificare fonti e veridicità di dati e informazioni; b) accertarsi che i sistemi abbiano adeguate misure di sicurezza e riservatezza e siano conformi alla normativa privacy.
- **Art. 21, c. 10 – Informativa.** Comunicare al cliente i sistemi di IA utilizzati, con linguaggio chiaro, semplice ed esaustivo, facendone menzione anche nella documentazione prodotta.

*Fonte: Codice deontologico CNDCEC, artt. 6 e 21, commi 8, 9 e 10 (agg. 21.11.2025).*

LEGGE 132/2025

# La clausola informativa: contenuti e raccomandazioni

## Contenuto del modello di clausola

- IA, inclusi LLM, esclusivamente per finalità di supporto e natura ausiliaria.
- Categorie di sistemi: ricerca normativa e di prassi; redazione e revisione di documenti; analisi e controllo di dati contabili e fiscali; consulenza e pianificazione (simulazione di scenari); strumenti con IA integrata (posta, browser, gestionali, videoscrittura, produttività, comunicazione).
- Chiusura: valutazioni, interpretazione, firma di atti e decisioni restano al Professionista, che ne assume la piena responsabilità.

## Cinque raccomandazioni

- **Allineare** la clausola agli strumenti effettivamente in uso.
- **Rivederla periodicamente** al mutare di strumenti e modalità operative.
- **Calibrare il linguaggio** sul destinatario: semplice o più tecnico a seconda del tipo di cliente cui è rivolta.
- **Valutare se valorizzare la formazione** svolta sull'uso consapevole dell'IA.
- **Coordinare i documenti:** informativa privacy ex art. 13 GDPR (es. trasferimenti extra-UE), clausole su riservatezza e proprietà intellettuale, policy interne.

*Fonte: art. 13 L. 132/2025; Codice deontologico CNDCEC, artt. 6 e 21.*

AI ACT, REG. (UE) 2024/1689

# Lo Studio come deployer e l'obbligo di alfabetizzazione

- **Deployer (art. 3):** chi utilizza un sistema di IA sotto la propria autorità, salvo attività personale non professionale. Lo Studio che usa l'IA è deployer.
- **Art. 4, testo originario (dal 2.2.2025):** fornitori e deployer adottano misure per garantire nella misura del possibile un livello sufficiente di alfabetizzazione in materia di IA del personale e di chi usa i sistemi per loro conto, tenendo conto di conoscenze, esperienza, formazione e contesto d'uso.
- **Omnibus IA – Reg. (UE) 2026/1744 (in vigore dal 27.7.2026):** l'art. 4 è riformulato: fornitori e deployer «adottano misure per sostenere lo sviluppo dell'alfabetizzazione in materia di IA» (traduzione non ufficiale). L'obbligo resta, in forma attenuata.
- **Calendario:** trasparenza (art. 50) applicabile dal 2.8.2026; obblighi per i sistemi ad alto rischio posticipati dall'Omnibus IA al 2.12.2027 / 2.8.2028.

*Fonti: artt. 3, 4, 50, 113 Reg. (UE) 2024/1689; Reg. (UE) 2026/1744.*

AI ACT, REG. (UE) 2024/1689

# Trasparenza (art. 50, dal 2.8.2026): quando scatta e cosa fare

| Caso | Esempi in Studio | Cosa fare |
|---|---|---|
| **Chatbot e assistenti (par. 1)** | Chatbot sul sito, assistente WhatsApp, centralino con voce sintetica, risposte automatiche alle e-mail. | Messaggio iniziale «Sono un assistente virtuale basato su IA» e indicatore persistente; annuncio vocale e modo per parlare con un professionista. |
| **Deepfake (par. 4, primo periodo)** | Foto realistiche del team generate con IA, avatar o voce clonata del socio, testimonial mai esistiti. | Etichetta o didascalia «Immagine generata con IA»; avviso all'inizio di video/audio e nella descrizione del post. |
| **Testi su temi di interesse pubblico (par. 4, secondo periodo)** | News fiscali sul blog, newsletter, post LinkedIn su novità normative, guide e FAQ. | Esenti con revisione umana sostanziale e responsabile editoriale (firma del professionista); altrimenti «Testo redatto con il supporto di sistemi di IA». |
| **Di regola fuori dall'art. 50** | Post promozionali; pareri, bilanci, e-mail al singolo cliente (non «pubblicati»). | Nel dubbio indicare l'uso dell'IA; per i clienti resta l'informativa ex art. 13 L. 132/2025 (+ estensione sui documenti ex 21 co. 10 Cod. Deont.) |

- La marcatura leggibile da macchina del fornitore (par. 2) non va rimossa né aggirata, ma NON assolve gli obblighi dello Studio; neppure le etichette automatiche dei social.
- Sanzioni fino a 15 mln € o 3% del fatturato mondiale annuo (per le PMI l'importo minore) – art. 99.

*Fonti: art. 50 Reg. (UE) 2024/1689; Linee guida della Commissione sugli obblighi di trasparenza (luglio 2026).*

GDPR, REG. (UE) 2016/679

# Di chi sono i dati? Titolare o responsabile

## Titolare (art. 4, n. 7)

- Determina finalità e mezzi del trattamento.
- Il commercialista è titolare per i dati dei dipendenti dello Studio, i dati di contatto e fiscali dei clienti, i dati usati nelle difese giudiziali.
- Può nominare il provider di IA come proprio responsabile.

## Responsabile (art. 28)

- Tratta i dati per conto del titolare, secondo istruzioni.
- Il commercialista è responsabile per i dati di terzi che gli sono trasmessi dai clienti (dipendenti, fornitori): contabilità, paghe, dichiarazioni.
- Nomina scritta (o «auto-nomina»); nessun uso per finalità proprie né di strumenti di IA non autorizzati; rendicontazione e ispezioni (art. 28, par. 3, lett. h).

---

## Se immetto dati di clienti o terzi: quattro conseguenze

- I sistemi LLM trattano dati per nostro conto: la titolarità della finalità resta nostra.
- Il fornitore va nominato responsabile e munito di istruzioni scritte.
- L'addestramento con quei dati richiede l'autorizzazione del cliente o del terzo: va disattivato.
- Se sono responsabile, rispetto la nomina ricevuta: sub-responsabili sempre ammessi, ammessi con comunicazione, o solo previa autorizzazione.

*Fonti: artt. 4, n. 7, 5, 28 GDPR.*

GDPR, REG. (UE) 2016/679

# Uso legittimo dell'IA: adempimenti, minimizzazione e conservazione

### 1 Nomina aggiornata

Il contratto o la nomina ex art. 28 con il cliente deve includere espressamente l'uso di strumenti di IA e le regole sui sub-responsabili.

### 2 Provider come responsabile / sub-responsabile (art. 28, par. 4)

Verificare il DPA con il provider; comunicazione o autorizzazione del titolare-cliente.

### 3 Addestramento disattivato

Sempre, quando si immettono dati di terzi.

### 4 Registro dei trattamenti (art. 30)

Aggiornato con i trattamenti via IA; valutare la DPIA per i trattamenti a rischio elevato.

### 5 Istruzioni e formazione (art. 29)

Ai collaboratori: quali strumenti, con quali dati, con quali limiti.

- **Minimizzazione e anonimizzazione.** L'anonimizzazione preventiva è utile (strumenti offline: Presidio, A5PII, CamoText, Privacy Scrubber, Anondocs, Anonimator), ma anonimizzazione ≠ anonimato: il dato pseudonimo resta dato personale.
- **Conservazione e cancellazione.** I sistemi di IA entrano nel perimetro informativo dello Studio: la cancellazione dei dati personali va programmata nei termini dichiarati nelle informative → no "shadow AI"

⊗ Senza questi adempimenti l'uso dell'IA su dati di cui non si è titolari è illecito ed espone lo Studio a sanzioni.

GDPR: CASI PRATICI

# Pochi sistemi gratuiti accettano la nomina a responsabile: due eccezioni

Molti sistemi di IA, specie gratuiti, non accettano la nomina a responsabile: anche con informativa e alfabetizzazione, su quei sistemi non si immettono dati personali e i file vanno anonimizzati prima.

## Mistral

- **Player UE,** dati residenti in Unione europea.
- **DPA** disponibile per tutte le funzionalità, non solo enterprise.
- **Addestramento:** opt-in sui piani a pagamento, opt-out sul piano gratuito (Impostazioni → Privacy).
- **Attenzione:** se non si è titolari dei dati, notificare il fornitore al titolare o farlo autorizzare.

## Lumo

- **Player svizzero** orientato alla massima riservatezza delle conversazioni.
- **Nessun addestramento:** i dati degli utenti non alimentano i modelli.
- **Crittografia zero-knowledge:** il fornitore non può leggere le conversazioni.
- **Giurisdizione:** dati in Svizzera, Paese con decisione di adeguatezza.

GDPR: CASI PRATICI

# ChatGPT & co.: le verifiche per immettere dati personali

## Verifica 1 – Piano con DPA

Per immettere dati personali in ChatGPT servono i piani Business o Enterprise (Professional ≠ Enterprise).

## Verifica 2 – Trasferimento extra-UE

OpenAI non aderisce al Data Privacy Framework: il trasferimento verso gli USA poggia sulle fragili clausole contrattuali standard. Solo il piano Enterprise consente la localizzazione in UE, che comunque non esclude il Cloud Act.

> **La differenza tra piano consumer e business non è commerciale: è la differenza tra essere titolare o responsabile dei dati che immettiamo.**

*Fonti: artt. 44 ss. GDPR; decisione di adeguatezza UE-USA (Data Privacy Framework); openai.com/it-IT/policies/data-processing-addendum/*

GDPR: CASI PRATICI

# ChatGPT & co.: cosa cambia con la DPA

## Impegni contrattuali chiari

Con la DPA siamo noi i titolari del dato e il fornitore deve rispettare le nostre istruzioni.

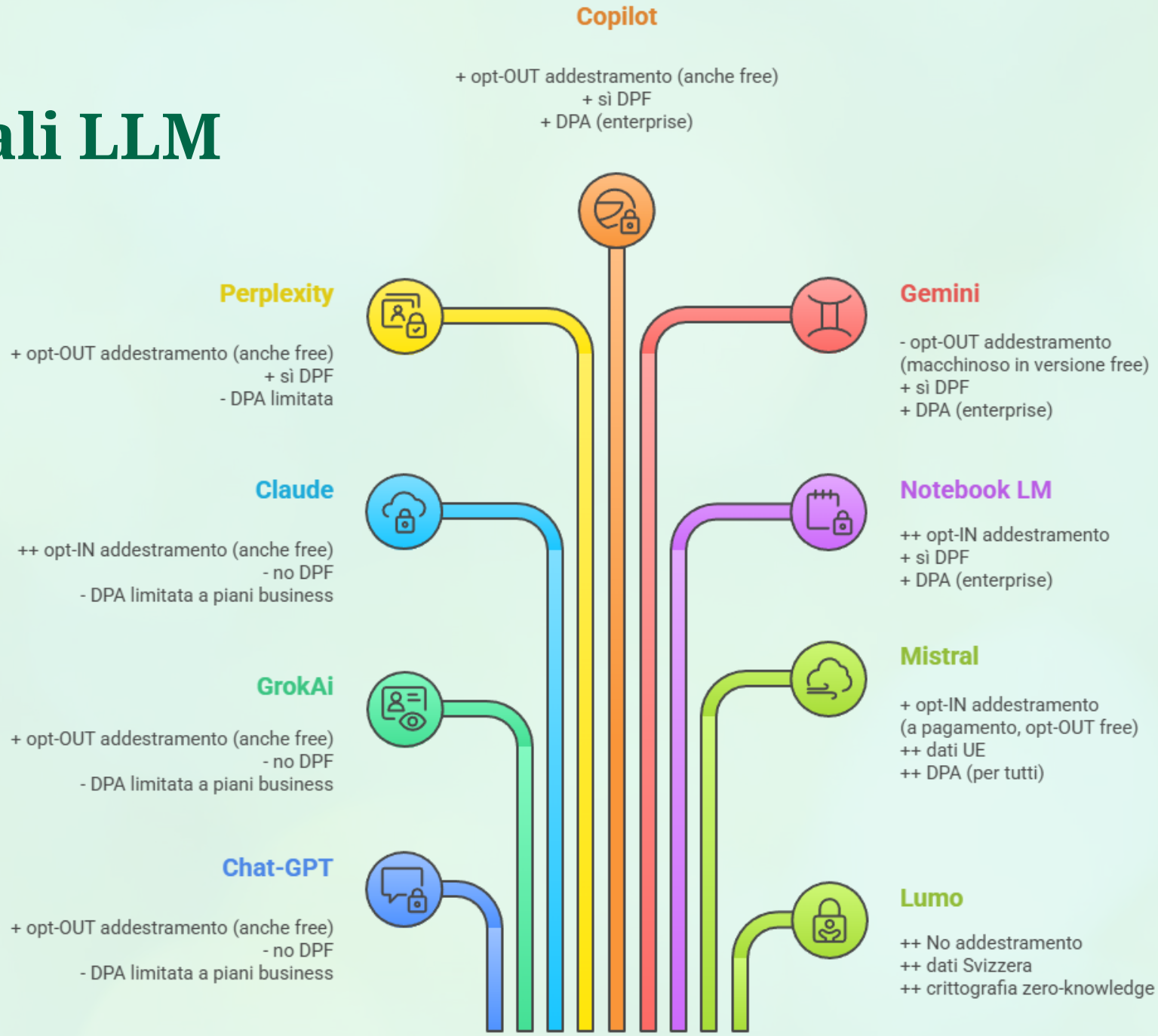
Per sei mesi nel 2025 tutte le nostre chat (anche temporanee o cancellate) sono state conservate per ordine di un Giudice USA nell'ambito di una causa con il New York Times.

Tutte **tranne** le chat dei piani Business e Enterprise (OpenAI ha infatti fatto presente al Giudice di non essere titolare di quei dati e di dover seguire le istruzioni di cui alla DPA, senza poter intervenire con conservazioni ultra-termine).

## Presunzione di uso professionale

Con sentenza del 24 gennaio 2025, la Corte d'appello di Parigi ha confermato la correttezza del comportamento di Google che ha chiuso l'account consumer di un legale che aveva immesso nel suo Google Drive un fascicolo processuale relativo ad un procedimento per pedopornografia che includeva alcune immagini esplicite raccolte dalla Procura.
Il legale, col sostegno dell'Ordine degli Avvocati di Parigi, contestava la decisione affermando che l'inserimento era legato all'attività professionale del legale. La Corte afferma che solo con un account di tipo professionale questa presunzione può operare.

# Confronto principali LLM



NIS2, DIR. (UE) 2022/2555 – D.LGS. 138/2024

# NIS2 e Studio professionale: l'impatto arriva «di riflesso»

## Il quadro

- Soggetti essenziali e importanti dei settori degli Allegati I e II, di regola di media o grande dimensione. Autorità: ACN.
- Obblighi: organi di amministrazione (art. 23), misure di sicurezza inclusa la catena di approvvigionamento (art. 24), notifica incidenti (art. 25: 24 h / 72 h / 1 mese).
- Notifica incidenti operativa dal 15.1.2026; misure di base entro il 31.10.2026 per i soggetti in elenco 2025.
- Sanzioni (art. 38): fino a 10 mln € o 2% (essenziali), 7 mln € o 1,4% (importanti).
- Lo Studio difficilmente è soggetto NIS2 (settore e dimensione), salvo verifica caso per caso (es. servizi TIC gestiti). Ma il cliente NIS2 trasferisce requisiti di sicurezza nei contratti: il fornitore è vincolato dal contratto, non dalla legge.

## Impatti sull'uso dell'IA in Studio

- **Strumenti autorizzati:** elenco di strumenti e fornitori usati sui dati del cliente, anche soggetti ad autorizzazione.
- **Stop alla «shadow AI»:** niente account personali o versioni gratuite non approvate.
- **Accessi e tracciabilità:** utenze nominative, MFA, log, riesame periodico.
- **Incidenti:** comunicazione immediata al cliente (lui ha 24 ore per la pre-notifica).
- **Dati e continuità:** localizzazione, conservazione, cancellazione; alternative in caso di indisponibilità.
- **Evidenze:** certificazioni del fornitore (es. ISO/IEC 27001), questionari, verifiche.

*Fonti: artt. 23, 24, 25 e 38 D.Lgs. 138/2024; determinazioni e FAQ ACN.*

ROADMAP DI COMPLIANCE

# Roadmap di compliance per normativa

| Normativa | Obblighi |
|---|---|
| L. 132/2025 (sempre) | Informativa ex art. 13 sui sistemi di IA utilizzati, con linguaggio chiaro, semplice ed esaustivo (+ nei documenti sulla base del Cod. Deont.). |
| AI Act (alfabetizzazione sempre; trasparenza nei casi dell'art. 50) | Misure per sostenere l'alfabetizzazione del personale (art. 4 riformulato). Avviso nei chatbot; etichetta su deepfake e testi pubblicati di interesse pubblico, salvo revisione umana e responsabilità editoriale. |
| GDPR (se immetto dati personali) | Verifica di titolarità; minimizzazione; nomina del fornitore a responsabile; legittimità del trasferimento extra-UE; addestramento disattivato. |
| NIS2 (se fornitore di un soggetto NIS2) | Verificare i requisiti contrattuali del cliente; comunicare o far autorizzare il fornitore; utenze nominative e MFA; notifica tempestiva degli incidenti. |

CASO PRATICO

# Registrazione e trascrizione delle riunioni con l'IA

- **1. Base giuridica.** Spesso il consenso di tutta la platea; può bastare il legittimo interesse per riunioni da verbalizzare o convegni, se registra l'organizzatore.
- **2. Trasparenza.** Informare prima dell'avvio su trattamento e conservazione (GDPR e, se applicabile, art. 50 AI Act).
- **3. Fornitore.** Plaud; read.ai; menutes.com (UE) → quali prodotti/piani hanno DPA?
- **4. Minimizzazione.** Limitare durata, diffusione e riuso delle trascrizioni.
- **AI Act.** Assistente che interviene in riunione: chiarire che è un'IA (art. 50, par. 1). Analisi del «sentiment» su voce o volto: può essere riconoscimento delle emozioni, vietato sul luogo di lavoro (art. 5, par. 1, lett. f). Verbali pubblicati: revisione umana o etichetta (art. 50, par. 4). Alfabetizzazione su limiti ed errori (art. 4).
- **NIS2.** Con clienti NIS2: contratto che consenta lo strumento, fornitore autorizzato, MFA, localizzazione e cancellazione coerenti, notifica immediata degli incidenti.
- **L. 132/2025.** Lo strumento va ricompreso nell'informativa al cliente (art. 13).

PROFILI OPERATIVI

# IA in locale e aspetti contrattuali

## IA in locale: più controllo, più responsabilità

- Non sostituisce: una strategia (perché usiamo l'IA?), policy e procedure, verifiche periodiche su sicurezza, qualità e impatti sui diritti.
- Rischi: assenza di competenze interne di sicurezza e MLOps; configurazioni errate (modello esposto in rete, log non protetti); difficoltà di aggiornamento e conformità; costi di infrastruttura, manutenzione e formazione.

## Contratti con lo sviluppatore

- **Lato sviluppatore:** garanzie di conformità all'AI Act; descrizione di funzionalità, casi d'uso e limiti; allocazione delle responsabilità; aggiornamenti e supporto.
- **Lato cliente:** documentazione e trasparenza; clausole su dati, audit e sicurezza; assistenza in caso di incidenti e data breach; recesso o sospensione se il sistema non è conforme.

**Il contratto è uno strumento di chiarezza reciproca, non solo di tutela legale.**

SINTESI OPERATIVA

# Checklist e governance dell'IA nello Studio

## Checklist di conformità

- Sottoporre l'informativa ex art. 13 L. 132/2025.
- Aggiornare l'informativa privacy (anche trasferimenti USA).
- Condurre la formazione normativa e operativa (art. 4 AI Act).
- Mappare gli strumenti di IA dello Studio.
- Verificare gli strumenti professionali: garanzie e DPA.
- Gestire la trasparenza AI Act (art. 50).
- Verificare il perimetro NIS2 dei clienti.
- Adottare un regolamento interno sull'uso dell'IA.

## Regole di governance

- Solo account dello Studio, salvo espressa autorizzazione.
- Divieto di immettere categorie particolari di dati, dati giudiziari, dati di minori e credenziali.
- Output sempre verificato e validato da un professionista.
- Avvisi ed etichette sui contenuti IA: la marcatura del fornitore non basta.
- Canali per segnalare anomalie e incidenti.
- Formazione su rischi, regole e trasparenza.
- Requisiti NIS2 dei clienti: strumenti autorizzati, MFA, notifica incidenti.
- Monitoraggio periodico e aggiornamento delle regole (Omnibus IA, Linee guida, ACN).