

PERCORSO FORMATIVO — AI GENERATIVA APPLICATA

Dispensa 12

GDPR e Protezione dei Dati nell'Uso dell'AI

Come applicare i principi della protezione dei dati personali quando si utilizzano strumenti di AI generativa.

A cura di Marco Consiglio

Formatore e Course Director — Contenuti aggiornati al 2026

Indice

1. Introduzione e obiettivi didattici	3
2. Che cos'è un dato personale, in termini comprensibili	4
3. I principi fondamentali del GDPR applicati a questi strumenti.....	6
4. Il ruolo del fornitore dello strumento come responsabile del trattamento	9
5. Un principio pratico di minimizzazione dei dati condivisi.....	11
6. Le basi giuridiche per l'utilizzo di questi strumenti	undefined
7. I diritti degli interessati e le implicazioni pratiche	15
8. Un principio di sintesi: la privacy come pratica quotidiana	17
9. Caso pratico guidato.....	18
10. Glossario dei termini chiave.....	20
11. Checklist finale e autoverifica.....	21
12. Riferimenti e risorse aggiornate al 2026	22

1. Introduzione e obiettivi didattici

Questa dispensa prosegue il percorso AI Generativa Applicata, affrontando il primo dei due temi normativi presentati in questo percorso: il Regolamento generale sulla protezione dei dati, comunemente noto con l'acronimo GDPR, e le sue implicazioni pratiche per un utilizzo responsabile di questi strumenti.

Applicando quanto già presentato nella Dispensa 6 di questo percorso a proposito del principio di riservatezza nei dati condivisi, questa dispensa sistematizza e approfondisce quel principio già introdotto, fornendo un quadro più strutturato dei principi normativi rilevanti, senza pretesa di sostituire una consulenza legale specialistica per situazioni di particolare complessità.

A chi si rivolge questa dispensa

Si rivolge a chi ha seguito le prime undici dispense di questo percorso e desidera comprendere, in termini accessibili e senza tecnicismi giuridici eccessivi, come applicare i principi della protezione dei dati personali nell'uso quotidiano di questi strumenti.

Un chiarimento preliminare importante

Applicando lo stesso principio di onestà metodologica già più volte richiamato in questo percorso, questa dispensa non sostituisce una consulenza legale specialistica: per situazioni di particolare complessità o rilevanza, un professionista dovrebbe sempre rivolgersi a un consulente legale qualificato. L'obiettivo di questa dispensa è fornire una comprensione di base sufficiente per riconoscere le situazioni che richiedono attenzione e, quando necessario, un approfondimento specialistico.

Obiettivi di apprendimento

1. Comprendere che cos'è un dato personale, in termini comprensibili;
2. Conoscere i principi fondamentali del GDPR applicati a questi strumenti;
3. Comprendere il ruolo del fornitore dello strumento come responsabile del trattamento;
4. Saper applicare un principio pratico di minimizzazione dei dati condivisi;
5. Conoscere le basi giuridiche per l'utilizzo di questi strumenti;
6. Comprendere i diritti degli interessati e le loro implicazioni pratiche.

2. Che cos'è un dato personale, in termini comprensibili

Applicando quanto già presentato nella Dispensa 6 di questo percorso a proposito della riservatezza, iniziamo con una definizione chiara e accessibile di dato personale, il concetto centrale attorno a cui ruota l'intera normativa che sarà presentata in questa dispensa.

Una definizione operativa

Un dato personale è qualunque informazione che, direttamente o indirettamente, permette di identificare una persona fisica specifica: non solo nome e cognome, ma anche un indirizzo email, un numero di telefono, un codice fiscale, e persino combinazioni di informazioni che, pur non identificando direttamente una persona, potrebbero farlo se combinate tra loro (una data di nascita specifica insieme a una città di residenza poco popolosa).

Un errore comune da evitare

Un errore comune, spesso fonte di sottovalutazione del rischio: pensare che solo dati esplicitamente identificativi come nome e cognome costituiscano dati personali rilevanti. In realtà, applicando quanto già presentato nella Dispensa 6 di questo percorso a proposito dell'anonimizzazione, anche informazioni apparentemente generiche, se combinate tra loro o con altre informazioni già disponibili, possono permettere l'identificazione di una persona specifica, un rischio che un professionista dovrebbe considerare con maggiore ampiezza rispetto alla sola presenza esplicita di un nome proprio.

Una distinzione importante: dati personali comuni e categorie particolari

Il GDPR distingue tra dati personali comuni e categorie particolari di dati, che includono informazioni relative alla salute, alle opinioni politiche, alle convinzioni religiose, o all'orientamento sessuale, per le quali sono richieste tutele ancora più rigorose: un professionista dovrebbe prestare un'attenzione particolare quando un compito coinvolge, anche indirettamente, questo tipo di informazioni particolarmente sensibili.

Un elemento pratico: i dati relativi a persone giuridiche

Un ultimo chiarimento pratico, distinto dalla distinzione già presentata in questo capitolo: il GDPR si applica specificamente ai dati personali di persone fisiche, non alle informazioni relative a società o altre persone giuridiche in quanto tali. Tuttavia, informazioni apparentemente aziendali possono comunque contenere dati personali indiretti, ad esempio l'indirizzo email diretto di un dipendente specifico o un numero di telefono personale associato a un ruolo aziendale, un elemento che un professionista dovrebbe considerare anche quando lavora con documenti apparentemente di natura puramente commerciale o organizzativa.

3. I principi fondamentali del GDPR applicati a questi strumenti

Applicando quanto già presentato nel capitolo 2 di questa dispensa a proposito della definizione di dato personale, presentiamo ora i principi fondamentali del GDPR, tradotti in implicazioni pratiche per l'utilizzo di strumenti di AI generativa.

Il principio di liceità, correttezza e trasparenza

Il trattamento di dati personali deve avvenire secondo una base giuridica legittima, un principio che sarà approfondito con maggiore dettaglio nel capitolo 6 di questa dispensa, e in modo trasparente verso le persone i cui dati vengono trattati, un principio che si collega a quanto già presentato nella Dispensa 11 di questo percorso a proposito della trasparenza proporzionata.

Il principio di limitazione della finalità

Applicando quanto già presentato nella Dispensa 6 di questo percorso a proposito della riservatezza, i dati personali dovrebbero essere trattati solo per finalità specifiche e legittime, determinate esplicitamente prima della raccolta: un professionista che condivide dati personali con uno strumento di AI generativa dovrebbe considerare esplicitamente se questo utilizzo sia coerente con la finalità per cui quei dati erano stati originariamente raccolti (un dato raccolto per gestire un ordine commerciale non dovrebbe essere utilizzato, senza un'ulteriore base giuridica, per finalità completamente diverse e non collegate).

Il principio di minimizzazione dei dati

Applicando quanto già presentato nella Dispensa 6 di questo percorso a proposito dell'anonimizzazione, questo principio, che sarà approfondito con maggiore dettaglio pratico nel capitolo 5 di questa dispensa, richiede che vengano trattati solo i dati personali effettivamente necessari per una finalità specifica, non un volume di informazioni superiore a quanto strettamente richiesto dal compito da svolgere.

Il principio di limitazione della conservazione

I dati personali non dovrebbero essere conservati più a lungo di quanto necessario per la finalità del trattamento, un principio rilevante anche per le conversazioni intrattenute con strumenti di AI generativa, che possono conservare, secondo le proprie specifiche politiche, la cronologia delle interazioni per periodi di tempo variabili.

Il principio di integrità e riservatezza

Un ultimo principio fondamentale, distinto dai precedenti già presentati in questo capitolo, richiede che i dati personali vengano trattati con misure tecniche e organizzative adeguate a garantirne la sicurezza, proteggendoli da trattamenti non autorizzati o illeciti e da perdita, distruzione, o danno accidentale. Applicando quanto già presentato nel capitolo 4 di questa

dispensa a proposito del ruolo del fornitore come responsabile del trattamento, questo principio si traduce, per un utilizzatore di strumenti di AI generativa, nella necessità di verificare che il fornitore prescelto adotti misure di sicurezza adeguate, un elemento che dovrebbe far parte della verifica già presentata in quel capitolo prima di autorizzare l'uso di un determinato strumento per compiti che coinvolgono dati personali.

4. Il ruolo del fornitore dello strumento come responsabile del trattamento

Presentiamo ora un concetto tecnico giuridico di particolare rilevanza pratica: il ruolo che il fornitore di uno strumento di AI generativa assume, dal punto di vista normativo, quando un utilizzatore condivide dati personali con quello strumento.

Una distinzione tecnica importante

Nel linguaggio del GDPR, un'organizzazione che decide le finalità e le modalità del trattamento di dati personali è definita titolare del trattamento, mentre un soggetto che tratta dati per conto del titolare, secondo le sue istruzioni, è definito responsabile del trattamento. Quando un professionista, per conto della propria organizzazione, condivide dati personali con uno strumento di AI generativa, il fornitore di quello strumento assume tipicamente il ruolo di responsabile del trattamento, un rapporto che dovrebbe essere regolato da un accordo contrattuale specifico tra l'organizzazione e il fornitore dello strumento.

Un'implicazione pratica di questo ruolo

Applicando quanto già presentato nella Dispensa 10 di questo percorso a proposito delle linee guida condivise, un'organizzazione dovrebbe verificare, prima di autorizzare l'uso di uno specifico strumento di AI generativa per compiti che coinvolgono dati personali, che esista un accordo contrattuale adeguato con il fornitore, spesso indicato come accordo sul trattamento dei dati, che regoli le modalità con cui quel fornitore tratta i dati personali condivisi attraverso lo strumento stesso.

Un principio pratico: verificare, non presumere

Applicando quanto già presentato nella Dispensa 1 di questo percorso a proposito della verifica sistematica, un professionista non dovrebbe presumere automaticamente che uno strumento sia adeguato dal punto di vista della protezione dei dati per il proprio specifico contesto professionale, ma dovrebbe verificare, o richiedere che la propria organizzazione verifichi, le specifiche garanzie contrattuali e tecniche offerte da quello strumento prima di un utilizzo che coinvolga dati personali di rilievo.

Un elemento pratico: il trasferimento di dati verso paesi terzi

Un ultimo elemento tecnico rilevante, distinto dalla verifica già presentata in questo capitolo: molti strumenti di AI generativa sono forniti da organizzazioni con sede al di fuori dello Spazio Economico Europeo, un elemento che può comportare un trasferimento di dati personali verso paesi terzi, soggetto a garanzie specifiche aggiuntive richieste dal GDPR. Un'organizzazione dovrebbe verificare, come parte della valutazione già presentata in questo capitolo, che il fornitore prescelto offra garanzie adeguate per questo tipo di trasferimento, un aspetto tecnico

che richiede tipicamente il supporto di un consulente legale qualificato, specialmente per organizzazioni che trattano volumi significativi di dati personali attraverso questi strumenti.

5. Un principio pratico di minimizzazione dei dati condivisi

Applicando quanto già presentato nella Dispensa 6 di questo percorso a proposito dell'anonimizzazione, approfondiamo ora sistematicamente il principio pratico più immediatamente applicabile da un singolo professionista: la minimizzazione dei dati personali condivisi con questi strumenti.

Un principio pratico fondamentale

Applicando quanto già presentato nella Dispensa 6 di questo percorso, prima di condividere qualunque contenuto con uno strumento di AI generativa, un professionista dovrebbe chiedersi esplicitamente se tutti i dati personali presenti in quel contenuto siano effettivamente necessari per il compito specifico da svolgere, rimuovendo o anonimizzando quelli non strettamente necessari, secondo lo stesso principio già presentato in quella dispensa applicato ora con una consapevolezza normativa più esplicita.

Un esempio pratico di applicazione di questo principio

Compito	Dati effettivamente necessari
Riassumere l'andamento generale delle vendite	Solo i totali aggregati, non i nomi dei singoli clienti
Redigere una lettera personalizzata a un cliente	Nome e dettagli specifici di quel singolo cliente

Un principio pratico complementare: preferire dati aggregati quando possibile

Applicando quanto già presentato nella Dispensa 6 di questo percorso a proposito dell'analisi di fogli di calcolo, quando un compito richiede l'analisi di un insieme di dati che include informazioni personali, un professionista dovrebbe considerare se sia possibile ottenere il risultato desiderato utilizzando dati già aggregati o anonimizzati, piuttosto che condividere l'intero insieme di dati personali dettagliati, un principio che riduce significativamente il rischio associato senza necessariamente sacrificare l'utilità del compito richiesto.

Un ultimo elemento: la minimizzazione non è un ostacolo alla qualità del lavoro

Un'ultima riflessione utile per questo capitolo: applicare sistematicamente il principio di minimizzazione già presentato in questo capitolo non dovrebbe essere percepito come un vincolo che riduce la qualità del lavoro professionale, ma come una disciplina che, con la pratica, diventa naturale quanto le altre buone pratiche già presentate in questo percorso. Un professionista che sviluppa l'abitudine di chiedersi sistematicamente quali dati siano realmente necessari per un compito specifico, prima ancora di considerare l'uso di questi strumenti, applica in realtà una disciplina di pensiero chiaro e strutturato che porta benefici anche al di là della sola

conformità normativa, un parallelo con il principio già presentato nella Dispensa 3 di questo percorso a proposito della chiarezza nella formulazione delle richieste.

6. Le basi giuridiche per l'utilizzo di questi strumenti

Applicando quanto già presentato nel capitolo 3 di questa dispensa a proposito del principio di liceità, approfondiamo ora le principali basi giuridiche che possono legittimare il trattamento di dati personali attraverso strumenti di AI generativa in un contesto professionale.

Le basi giuridiche più rilevanti in un contesto professionale

- L'interesse legittimo, quando l'organizzazione ha un interesse ragionevole e proporzionato nel trattamento, bilanciato con i diritti e le libertà delle persone interessate;
- L'esecuzione di un contratto, quando il trattamento è necessario per adempiere a obblighi contrattuali verso un cliente o un fornitore;
- Il consenso esplicito della persona interessata, quando applicabile e richiesto dalla natura specifica del trattamento.

Un principio pratico: la base giuridica dovrebbe essere già definita a livello organizzativo

Applicando quanto già presentato nella Dispensa 10 di questo percorso a proposito delle linee guida condivise, l'identificazione della base giuridica appropriata per l'uso di questi strumenti non dovrebbe essere una decisione lasciata al giudizio individuale di ciascun professionista caso per caso, ma dovrebbe essere definita a livello organizzativo, con il supporto di un consulente legale qualificato quando necessario, e comunicata chiaramente attraverso le linee guida condivise già presentate in quella dispensa.

Un principio di cautela per il singolo professionista

Applicando lo stesso principio di prudenza già più volte richiamato in questo percorso, quando un professionista non è certo che esista una base giuridica adeguata per un utilizzo specifico che coinvolge dati personali, dovrebbe astenersi da quell'utilizzo e consultare il proprio referente interno già presentato nella Dispensa 10 di questo percorso, o la funzione aziendale competente in materia di protezione dei dati, prima di procedere.

Un elemento pratico: il consenso non è sempre la soluzione più semplice

Un ultimo chiarimento pratico, spesso motivo di equivoco: sebbene il consenso esplicito già presentato in questo capitolo possa apparire come la base giuridica più intuitiva e semplice da applicare, nella pratica organizzativa risulta spesso meno agevole di quanto sembri, poiché richiede requisiti specifici di validità (informato, libero, specifico, revocabile in ogni momento) e una gestione accurata delle revoche nel tempo. Per questo motivo, molte organizzazioni preferiscono, quando applicabile secondo la natura specifica del trattamento, basarsi su altre basi giuridiche già presentate in questo capitolo, come l'esecuzione di un contratto o l'interesse legittimo, riservando il consenso esplicito alle situazioni in cui è effettivamente richiesto dalla natura del trattamento o non sono disponibili alternative giuridicamente adeguate.

7. I diritti degli interessati e le implicazioni pratiche

Presentiamo ora un ultimo tema di rilevanza pratica: i diritti che il GDPR riconosce alle persone i cui dati vengono trattati, indicate come interessati, e le implicazioni pratiche di questi diritti per un utilizzo consapevole di strumenti di AI generativa.

I principali diritti degli interessati

- Il diritto di accesso, che permette a una persona di sapere quali dati personali la riguardano vengono trattati e con quali finalità;
- Il diritto di rettifica, che permette di correggere dati personali inesatti o incompleti;
- Il diritto alla cancellazione, spesso indicato come diritto all'oblio, che permette, in determinate circostanze, di richiedere la cancellazione dei propri dati personali.

Un'implicazione pratica per l'uso di questi strumenti

Applicando quanto già presentato nella Dispensa 2 di questo percorso a proposito della memoria di questi strumenti, un professionista dovrebbe essere consapevole che, se dati personali di una persona vengono condivisi con uno strumento di AI generativa e questo strumento conserva memoria delle conversazioni secondo le funzionalità già presentate in quella dispensa, potrebbe risultare più complesso garantire pienamente l'esercizio di questi diritti su quei dati specifici, un elemento che rafforza ulteriormente il principio di minimizzazione già presentato nel capitolo 5 di questa dispensa.

Un principio pratico per gestire una richiesta di esercizio di questi diritti

Applicando quanto già presentato nella Dispensa 10 di questo percorso a proposito del ruolo di un referente interno, se un professionista riceve una richiesta di esercizio di questi diritti da parte di una persona i cui dati potrebbero essere stati trattati anche attraverso strumenti di AI generativa, dovrebbe coinvolgere tempestivamente la funzione aziendale competente o il proprio referente interno, secondo un processo strutturato che l'organizzazione dovrebbe aver già definito, piuttosto che gestire questa richiesta in autonomia senza il necessario supporto specialistico.

Un ultimo diritto rilevante: il diritto alla limitazione del trattamento

Un ultimo diritto, distinto dai tre già presentati in questo capitolo, permette a una persona di richiedere la limitazione temporanea del trattamento dei propri dati, ad esempio mentre è in corso una verifica sulla loro accuratezza, senza richiedere la cancellazione completa già presentata in questo capitolo. Questo diritto assume una rilevanza pratica specifica per i sistemi che coinvolgono strumenti di AI generativa: se un dato personale utilizzato come input per un compito automatizzato viene contestato dalla persona interessata, la limitazione temporanea di quel trattamento specifico, in attesa di verifica, rappresenta una risposta proporzionata che un'organizzazione dovrebbe essere in grado di applicare tempestivamente, un ulteriore motivo

per cui i processi già presentati in questo capitolo dovrebbero essere strutturati e non improvvisati caso per caso.

8. Un principio di sintesi: la privacy come pratica quotidiana

Concludiamo la parte teorica di questa dispensa con una riflessione di sintesi su un principio trasversale, già più volte richiamato nei capitoli precedenti: la protezione dei dati personali non è un adempimento burocratico separato, ma una pratica quotidiana da integrare nell'utilizzo di questi strumenti.

Un'integrazione naturale con i principi già presentati in questo percorso

Applicando quanto già presentato nella Dispensa 11 di questo percorso a proposito dell'integrazione naturale dei principi etici, i principi di protezione dei dati presentati in questa dispensa si integrano naturalmente con gli strumenti pratici già acquisiti nel corso di questo percorso: la stessa attenzione alla riservatezza già presentata nella Dispensa 6, lo stesso principio di responsabilità già presentato nella Dispensa 5, la stessa vigilanza etica già presentata nella Dispensa 11, tutti elementi che convergono naturalmente in una pratica quotidiana attenta e consapevole della protezione dei dati personali.

Un principio di sintesi per l'intera dispensa

Un principio di sintesi per l'intera dispensa

Il GDPR e la protezione dei dati, in tutte le dimensioni presentate in questa dispensa — la definizione di dato personale, i principi fondamentali, il ruolo del fornitore come responsabile del trattamento, la minimizzazione dei dati, le basi giuridiche, i diritti degli interessati — richiedono un'attenzione pratica costante che si integra naturalmente con gli strumenti già acquisiti in questo percorso, sempre nella consapevolezza che, per situazioni complesse, il supporto di un consulente legale qualificato resta indispensabile.

Un ultimo elemento: la fiducia come conseguenza della cura

Un'ultima riflessione conclude questa dispensa: un'attenzione genuina alla protezione dei dati personali, oltre a rappresentare un obbligo normativo, contribuisce a costruire e mantenere la fiducia dei clienti, dei colleghi, e di tutte le persone i cui dati un professionista tratta nel corso della propria attività lavorativa. Applicando quanto già presentato nella Dispensa 5 di questo percorso a proposito della fiducia costruita nel tempo, questa stessa logica si applica pienamente anche alla protezione dei dati: una cura costante e visibile di questi principi rappresenta un investimento nella qualità complessiva della propria relazione professionale con le persone coinvolte, non solo un adempimento normativo da rispettare per evitare conseguenze negative.

9. Caso pratico guidato

Concludiamo la parte teorica con un caso pratico semplificato, che applica gli strumenti presentati in questa dispensa.

Il contesto

Riprendiamo il caso già presentato nelle dispense precedenti di questo percorso: il responsabile amministrativo deve preparare un'analisi dell'andamento dei pagamenti dei clienti dell'azienda nell'ultimo trimestre, un compito che coinvolge dati potenzialmente personali secondo quanto già presentato in questa dispensa.

Passo 1 — Verifica della base giuridica

Applicando gli strumenti del capitolo 6, il responsabile amministrativo verifica, secondo le linee guida già condivise dalla propria organizzazione secondo quanto già presentato nella Dispensa 10 di questo percorso, che l'analisi dei pagamenti rientri tra i trattamenti già coperti da una base giuridica adeguata, legata all'esecuzione dei contratti commerciali in essere.

Passo 2 — Applicazione del principio di minimizzazione

Applicando gli strumenti del capitolo 5, invece di condividere l'elenco completo dei nomi dei clienti con i relativi importi, il responsabile amministrativo prepara un'analisi basata su dati aggregati, sufficiente per il compito di riepilogo richiesto, evitando di condividere informazioni personali non strettamente necessarie.

Passo 3 — Verifica del fornitore dello strumento utilizzato

Applicando gli strumenti del capitolo 4, il responsabile amministrativo verifica di utilizzare uno strumento già approvato dalla propria organizzazione secondo un accordo contrattuale adeguato, coerentemente con le linee guida già condivise nel proprio ufficio.

Passo 4 — Gestione di un'eccezione che richiede dati specifici

Applicando gli strumenti del capitolo 5, per un'analisi più approfondita relativa a tre clienti specifici con ritardi significativi nei pagamenti, il responsabile amministrativo condivide solo i dati strettamente necessari per quei tre casi specifici, non l'intero database clienti, applicando lo stesso principio di minimizzazione anche a questa eccezione specifica.

Passo 5 — Documentazione delle scelte effettuate

Applicando quanto già presentato nella Dispensa 10 di questo percorso a proposito della documentazione dei modelli riutilizzabili, il responsabile amministrativo documenta brevemente le scelte effettuate per la gestione dei dati in questo compito specifico, un materiale utile per

future occorrenze simili e per la verifica periodica delle linee guida già presentata in quella dispensa.

Che cosa insegna questo caso

Il caso mostra come i principi di protezione dei dati presentati in questa dispensa si traducano in pratiche concrete e non eccessivamente onerose, applicabili nella gestione quotidiana di compiti che coinvolgono dati personali, senza rinunciare all'efficienza offerta da questi strumenti già presentata nelle dispense precedenti di questo percorso.

10. Glossario dei termini chiave

Come per le dispense precedenti di questo percorso, riportiamo un glossario di sintesi dei principali termini introdotti.

Dato personale	Qualunque informazione che permette, direttamente o indirettamente, di identificare una persona fisica specifica.
Titolare del trattamento	Soggetto che decide le finalità e le modalità del trattamento di dati personali.
Responsabile del trattamento	Soggetto che tratta dati personali per conto del titolare, secondo le sue istruzioni.
Minimizzazione dei dati	Principio secondo cui dovrebbero essere trattati solo i dati personali effettivamente necessari per una finalità specifica.

11. Checklist finale e autoverifica

Come per le dispense precedenti, dedichiamo un momento all'autoverifica personale prima di proseguire.

Domande di autoverifica

1. Sapresti definire, in termini comprensibili, che cos'è un dato personale?
2. Ricordi i principi fondamentali del GDPR applicati a questi strumenti?
3. Sapresti spiegare il ruolo del fornitore come responsabile del trattamento?
4. Ricordi il principio pratico di minimizzazione dei dati condivisi?
5. Sapresti indicare almeno due basi giuridiche rilevanti in un contesto professionale?
6. Ricordi i principali diritti degli interessati e le loro implicazioni pratiche?

Come procedere

Se le risposte sono arrivate con sicurezza, si può proseguire con la Dispensa 13, dedicata all'AI Act europeo. In caso di incertezza, si consiglia di rileggere i capitoli corrispondenti, in particolare quelli relativi alla minimizzazione dei dati e alle basi giuridiche.

12. Riferimenti e risorse aggiornate al 2026

Per approfondimenti autonomi, si segnalano alcune categorie di risorse utili:

- Il testo integrale del Regolamento generale sulla protezione dei dati, disponibile sui siti istituzionali dell'Unione Europea;
- Le linee guida pubblicate dalle autorità di controllo nazionali competenti in materia di protezione dei dati;
- Le politiche sulla privacy e le condizioni contrattuali specifiche dei principali strumenti di AI generativa oggi disponibili;
- Il confronto diretto con un consulente legale qualificato, risorsa indispensabile per situazioni di particolare complessità o rilevanza.

Chiusura della Dispensa 12

Con questa dispensa prosegue il percorso AI Generativa Applicata, fornendo una comprensione di base dei principi di protezione dei dati personali. La dispensa successiva affronterà l'AI Act europeo, il secondo grande tema normativo di questo percorso.

Marco Consiglio

Formatore e Course Director — 2026