

Guida alla compilazione della circolare IA, con le domande più frequenti

Questo documento accompagna il modello di circolare sull'uso dell'intelligenza artificiale. Ti serve per capire cosa adattare alla realtà del tuo ente, dove stare attento, e per rispondere ai dubbi che arrivano più spesso quando il personale legge la circolare.

Una cosa prima di tutto: questo file resta sulla tua scrivania, non si allega all'atto. La circolare che protocolli e diffondi è l'altro documento, quello pulito. Qui ci sono le istruzioni di lavoro, che nell'atto non devono comparire.

Parte prima: come adattare la circolare, sezione per sezione

Finalità e ambito.

Va bene così com'è per la maggior parte degli enti. Se la tua amministrazione ha già avviato un percorso strutturato sull'IA o ha già un regolamento in lavorazione, puoi dirlo qui, ma non è obbligatorio.

Quadro normativo.

Lascialo come lo trovi. I riferimenti e le date sono verificati e tarati per restare validi anche se cambia qualcosa sui sistemi ad alto rischio, che è la parte di normativa ancora in movimento. Non aggiungere date sull'alto rischio: oggi sarebbero un terreno scivoloso.

Principi.

Non toccarli. Il doppio richiamo all'art. 3 e all'art. 14 della legge 132 è il punto che dà solidità al documento, ed è proprio quello che distingue una circolare fatta bene da una copiata male.

Strumenti utilizzabili.

Qui si concentra la decisione più delicata, e ci ho messo una nota apposta nel testo. Te la spiego sotto, nella prima FAQ, perché è la domanda numero uno che ricevi. In sintesi: se non avete già valutato strumenti specifici, tieni la formula "l'ente sta valutando" e non elencare nomi.

Regole per l'uso quotidiano.

Adatta solo i riferimenti agli uffici e ai canali interni. Il resto è trasversale.

Rischi da conoscere.

Lascialo. È la parte che fa capire al personale perché certe regole esistono, e funziona meglio se resta asciutta.

Cosa è consentito, vietato, raccomandato.

Questa tabella adattala ai vostri casi reali. Se il tuo ente fa molte pratiche edilizie, aggiungi un esempio edilizio tra i consentiti. Se gestite servizi sociali, l'esempio sulle graduatorie tra i vietati parla la vostra lingua. Più la cali sui vostri processi, più il personale la usa.

Ricognizione degli utilizzi.

Indica il referente vero (nome, ufficio, email) e il canale con cui ricevere le comunicazioni. È l'unico punto dove la circolare chiede qualcosa di concreto al personale, quindi rendi facile rispondere.

Parte seconda: le domande più frequenti

Sono le domande che gli enti pongono più spesso dopo aver adottato la circolare. Le risposte sono pensate perché tu possa girarle quasi così come sono a chi te le fa.

Strumenti e autorizzazioni

"Possiamo elencare ChatGPT, Claude e Gemini tra gli strumenti autorizzati?"

No, non a freddo. Autorizzare uno strumento vuol dire avere verificato prima le sue condizioni d'uso, il modo in cui tratta i dati, e avere deciso come va impiegato. Scriverne soltanto il nome in un elenco non basta. Se quel lavoro non l'avete fatto, elencare i tre nomi più noti vi espone invece di proteggervi. La formula corretta in questa fase è quella che trovi nella circolare: l'ente sta valutando, e nel frattempo chi usa uno strumento se ne assume la responsabilità.

"Abbiamo già Copilot in ambiente Microsoft (o Gemini con Google Workspace). Cambia qualcosa?"

Sì, è una situazione diversa. Chi ha attivato Copilot o Gemini di solito lo ha fatto perché quegli strumenti erano già dentro un ambiente che aveva passato le verifiche privacy dell'ente. Se è il vostro caso, potete indicarli come strumenti ammessi, precisando per quali usi. La differenza con la domanda precedente è tutta qui: un conto è uno strumento già valutato dentro il vostro ambiente, un altro è un'app pubblica che qualcuno apre dal browser.

"Chi autorizza uno strumento, in concreto?"

Nella fase della circolare, l'indirizzo lo dà l'Ufficio per la Transizione Digitale, che raccoglie le richieste e istruisce la valutazione. L'autorizzazione vera, quella che mette nero su bianco condizioni d'uso e limiti, arriva con il regolamento e con la valutazione del singolo strumento. Tenere distinte le due cose evita di promettere oggi quello che si può dare solo dopo.

"Un dipendente usa ChatGPT dal suo account personale per scrivere documenti di lavoro. È un problema?"

Dipende da cosa ci mette dentro. Se usa uno strumento non valutato per riformulare un testo generico, senza dati personali né documenti riservati, rientra in quel "sotto la propria responsabilità" che la circolare prevede in questa fase. Se invece ci carica nomi di cittadini, pratiche, allegati riservati, lì il problema c'è, ed è di protezione dei dati prima ancora che di IA. La circolare serve proprio a rendere chiara questa linea.

Responsabilità e uso quotidiano

"Se un atto preparato con l'aiuto dell'IA contiene un errore, di chi è la responsabilità?"

Della persona che firma l'atto. La legge 132 è esplicita: chi adotta il provvedimento resta l'unico responsabile, anche se il testo è stato preparato con l'IA. L'IA ti fa risparmiare tempo, ma resta uno strumento che devi controllare prima di firmare. Non è un parere che ti mette al riparo.

"Devo annotare nei fascicoli che ho usato l'IA?"

Dove l'IA ha contribuito in modo significativo a un procedimento, sì, conviene tenerne traccia: serve a garantire la conoscibilità e la tracciabilità che la legge chiede per la PA. Non vuol dire compilare un modulo per ogni email riformulata. Vuol dire che, se l'IA ha pesato su un'istruttoria o su un atto, deve restare chiaro a posteriori come e quanto.

Dati personali

"Cosa posso inserire e cosa no?"

La linea è semplice da ricordare: niente dati che identificano una persona, niente categorie particolari (salute, opinioni, appartenenze e simili), niente documenti riservati o protocollati, dentro strumenti che l'ente non ha valutato. Per testi generici, bozze, riformulazioni di contenuti tuoi, nessun problema. Nel dubbio, toglì i nomi e rendi il testo anonimo prima di darlo in pasto allo strumento.

"Che differenza c'è tra un dato personale e una categoria particolare?"

Il dato personale è qualsiasi informazione che identifica una persona, anche solo il nome e cognome. La categoria particolare è un sottoinsieme più sensibile: dati su salute, vita sessuale, opinioni politiche, convinzioni religiose, appartenenza sindacale, dati genetici e biometrici. Le seconde meritano cautela ancora maggiore, perché un loro uso improprio fa più danno e la normativa le protegge di più.

"Usiamo uno strumento a pagamento che dichiara di non addestrare sui nostri dati. Possiamo inserire dati personali?"

La promessa di non usare i dati per l'addestramento è un pezzo del puzzle, ma non è tutto il puzzle. Restano da valutare dove finiscono quei dati, chi vi ha accesso, con quale base giuridica li trattate, se serve un accordo sul trattamento con il fornitore. Sono le domande di una valutazione vera, che è un passo a sé. Finché quella valutazione non c'è, la prudenza sui dati personali resta quella della circolare.

Trasparenza verso il cittadino

"Dobbiamo scrivere sul sito che usiamo l'IA?"

Quando il cittadino interagisce direttamente con un sistema di IA, ad esempio un chatbot, deve potersi rendere conto che sta parlando con una macchina e non con una persona. Lo prevede l'art. 50 dell'AI Act. Non serve un avviso generico su tutto il sito. Basta rendere riconoscibile l'IA nel punto in cui il cittadino la incontra.

"Da quando scatta questo obbligo?"

Gli obblighi di trasparenza dell'art. 50 si applicano dal 2 agosto 2026. C'è un trattamento a parte, con tempi tecnici suoi, per la marcatura dei contenuti generati dall'IA, ma il principio per cui un chatbot deve dichiararsi tale ha quella data come riferimento.

"Il nostro chatbot deve dire di essere un'IA?"

Sì, è esattamente il caso tipico dell'art. 50. Un assistente virtuale che risponde ai cittadini deve far capire fin dal primo contatto che è un sistema automatico. La forma può essere semplice, una riga all'avvio della conversazione, ma l'informazione deve esserci.

Valutazioni del rischio e FRIA

"Quando dobbiamo fare la FRIA?"

La FRIA, la valutazione d'impatto sui diritti fondamentali prevista dall'art. 27 dell'AI Act, è dovuta quando l'ente utilizza un sistema classificato ad alto rischio tra quelli dell'Allegato III dell'AI Act. Non è un adempimento che scatta su qualsiasi uso dell'IA: scatta sulla classificazione. Il punto difficile, quindi, è prima: capire se un certo sistema è davvero alto rischio. Quella valutazione si fa caso per caso, ed è il cuore del lavoro di affiancamento. Fin qui l'orientamento, oltre la soglia c'è il percorso: trovi come su painregola.it/supporto.

"Usare ChatGPT per scrivere le bozze ci obbliga alla FRIA?"

Di norma no. Un assistente generalista usato per riformulare testi non è di per sé un sistema ad alto rischio, quindi non fa scattare la FRIA. Attenzione però a due cose diverse che spesso si confondono con la FRIA: la trasparenza verso il cittadino se quei contenuti vanno all'esterno, e la protezione dei dati se nei testi finiscono dati personali. Sono tre verifiche distinte, e averne risolta una non chiude le altre.

"Il nostro chatbot è 'alto rischio'?"

Quasi sempre no: un chatbot che dà informazioni ai cittadini rientra di solito negli obblighi di trasparenza, non nell'alto rischio. Diverso è un sistema che decide o pesa su graduatorie, ammissioni, benefici, dove l'esito incide sui diritti delle persone: lì si entra nel campo dell'alto rischio e la classificazione va fatta sul serio. A distinguere i due casi è quello che il sistema determina, non il nome che porta.

"Che differenza c'è tra FRIA e DPIA?"

Guardano due cose diverse. La FRIA, art. 27 AI Act, valuta l'impatto del sistema sui diritti fondamentali delle persone, e scatta sull'alto rischio. La DPIA, art. 35 GDPR, valuta i rischi per la

protezione dei dati personali, e scatta sui trattamenti a rischio elevato. Possono convivere sullo stesso sistema, e quando una DPIA c'è già la FRIA la richiama senza rifarla da capo. Restano però due strumenti distinti, con presupposti distinti.

Fornitori

"Un fornitore ci propone un gestionale 'con l'AI'. Come capiamo se è vero e cosa comporta per noi?"

Prima domanda da fargli: dov'è l'IA, esattamente, e cosa fa. Capita spesso che "con AI" sia un'etichetta di marketing su funzioni che IA non sono. Se invece l'IA c'è davvero, da quel momento avete delle responsabilità anche voi come utilizzatori: dovete sapere come è stato classificato il rischio, quali documenti e garanzie il fornitore può darvi, come gestite la trasparenza e i dati. Valutare cosa vi stanno realmente vendendo, e cosa ricade su di voi, è un lavoro di verifica strutturato. Se vuoi affrontarlo con metodo, da painregola.it/supporto parte l'affiancamento che serve proprio a questo.

Censimento

"Come partiamo con il censimento?"

Dalla cosa più semplice: chiedere al personale cosa sta già usando. Molti utilizzano strumenti di IA senza dirlo, non per nascondersi ma perché nessuno glielo ha mai chiesto. La circolare apre questo canale. Per ogni strumento bastano poche informazioni iniziali: cosa è, a cosa serve, se tratta dati personali.

"Cosa dobbiamo registrare, di preciso?"

Per partire, lo strumento, l'ufficio che lo usa, la finalità, e se vengono trattati dati personali. È l'avvio. La mappatura completa, quella che poi serve per classificare ogni sistema secondo il rischio e per collegare le valutazioni dovute, è un passo successivo e si gestisce con uno strumento dedicato, non a mano su un foglio sparso.

Quadro normativo, sanzioni, profili penali

"Ci sono sanzioni se sbagliamo?"

Il regime sanzionatorio per la PA italiana è ancora in costruzione: la legge 132 ha delegato il Governo a definirlo con i decreti attuativi, in coerenza con l'AI Act, e quei decreti non ci sono ancora. Quindi diffida da chi oggi ti agita cifre precise di multe per la pubblica amministrazione. Il punto pratico, in questa fase, non è la sanzione: è la responsabilità personale di chi firma un atto preparato con l'IA, che esiste già adesso.

"L'IA può creare problemi penali? Cosa rischia chi diffonde un deepfake?"

Sì, su un fronte preciso. La legge 132, all'art. 26, ha introdotto nel codice penale il nuovo art. 612-quater: chi diffonde senza consenso immagini, video o voci di una persona, falsificati o alterati con l'IA in modo da ingannare sulla loro autenticità, e così le procura un danno ingiusto, rischia la reclusione da uno a cinque anni. È un reato che di norma si procede su querela della

persona offesa. La stessa legge ha aggiunto un'aggravante generale per i reati commessi usando l'IA come mezzo insidioso. Per un ente il punto pratico è doppio: non produrre né diffondere contenuti falsificati, e sapere che oggi esiste una tutela specifica per chi ne è vittima.

"Le linee guida AGID sull'IA nella PA sono già obbligatorie?"

Non ancora. Sono in fase di definizione e finché non sono adottate in via definitiva restano un riferimento autorevole, non un obbligo cogente. Tenerne conto è saggio, perché indicano la direzione, ma presentarle al personale come legge già in vigore sarebbe scorretto.

"Cosa cambia quando arriveranno i decreti attuativi?"

I decreti previsti dalla legge 132 dovrebbero definire gli aspetti operativi che oggi mancano: procedure di valutazione della conformità, regime sanzionatorio, regole di dettaglio per i sistemi ad alto rischio. È il motivo per cui la circolare si presenta come strumento per la fase di transizione e non come regolamento definitivo. Quando il quadro si completa, si passa al regolamento.

Oltre la soglia

Questa circolare e queste risposte ti portano fino a un certo punto: ti fanno capire cosa è in gioco, cosa puoi fare subito, dove devi fermarti. I tre passaggi che richiedono una valutazione vera, classificare un sistema come alto rischio, fare la FRIA, verificare un fornitore, sono un lavoro che si fa sul caso concreto del tuo ente, non su un modello generico.

Se sei arrivato a quel punto, da painregola.it/supporto trovi il percorso di affiancamento, calibrato sulla dimensione e sul livello di rischio dell'ente. Senza fretta: la materia è ampia, e si parte da dove sei.