AIPIA
ASSOCIAZIONE ITALIANA PROFESSIONISTI DELL'INTELLIGENZA ARTIFICIALE

GUIDA AIPIA · RISORSE PER PROFESSIONISTI

AI e Privacy
Usare l'AI rispettando il GDPR

Dati personali, basi giuridiche, valutazioni d'impatto e fornitori: come introdurre l'intelligenza artificiale senza violare il GDPR.

A cura del **Comitato Tecnico-Scientifico AIPIA**
Versione 1.0 — Giugno 2026

EUROPEAN AI ALLIANCE · ROME CALL FOR AI ETHICS · EUROPEAN DIGITAL CREDENTIALS · EIDAS · AI ACT READY

Documento realizzato da AIPIA per i propri soci e per la community.

Tutti i materiali: aipia.it/risorse-utili

Indice

AI e privacy non sono due mondi separati: quasi ogni uso concreto dell'intelligenza artificiale tocca dati personali, e quindi ricade sotto il GDPR. Questa guida AIPIA spiega in modo pratico come usare l'AI rispettando la protezione dei dati: quando un trattamento esiste davvero, su quale base giuridica poggia, come scrivere l'informativa, quando serve una valutazione d'impatto e cosa pretendere dai fornitori di strumenti AI. L'obiettivo non è spaventare, ma darti un metodo per introdurre l'AI senza violare il Regolamento UE 2016/679.

Vuoi ricevere le prossime guide AIPIA appena escono? **Iscriviti alla newsletter** o **diventa socio** e accedi a tutti i materiali.

La guida si rivolge a chi deve decidere e rispondere: responsabili della protezione dei dati, IT e compliance, titolari e manager di PMI, professionisti, responsabili HR e marketing, dirigenti della pubblica amministrazione. Non serve una formazione giuridica per leggerla, ma ogni capitolo presuppone che dietro l'uso dell'AI ci sia una responsabilità reale verso le persone i cui dati vengono trattati.

Una precisazione doverosa prima di cominciare. Questo è un documento divulgativo, non una consulenza legale. Descrive principi e prassi del GDPR (Regolamento UE 2016/679), dell'AI Act (Regolamento UE 2024/1689) e della normativa italiana di adeguamento, inclusa la Legge 132/2025, e richiama il ruolo del Garante per la protezione dei dati personali. Dove la tua situazione è specifica, in particolare su trattamenti delicati o ad alto rischio, la valutazione va fatta con un consulente, perché i dettagli cambiano il risultato.

PARTE I

AI e dati personali: il quadro

Prima di scegliere strumenti e basi giuridiche, serve sapere quando un uso dell'AI tratta dati personali, quali principi si applicano e come il GDPR si incastra con l'AI Act.

AI e privacy: perché il GDPR riguarda quasi ogni uso dell'AI

Un assistente che riassume le email dei clienti tratta dati personali. Un modello che classifica i curriculum tratta dati personali. Uno strumento che genera testi a partire dalle note di una riunione, se in quelle note compaiono nomi, tratta dati personali. La regola pratica è semplice: appena nell'uso dell'AI entra un'informazione che riguarda una persona identificata o identificabile, il GDPR si applica, e si applica per intero.

Molti progetti AI partono con la convinzione opposta: che la privacy sia un problema di un secondo momento, una formalità da sistemare prima del lancio. È l'errore che genera i guai più costosi, perché le scelte che contano, quali dati usare, dove farli passare, con quale fornitore, si fanno all'inizio, e correggerle dopo significa rifare il lavoro.

Perché l'AI alza la posta

Il GDPR esiste dal 2018 e le aziende lo conoscono. Cosa cambia con l'AI? Cambiano tre cose, e tutte e tre aumentano il rischio.

La prima è la quantità. Gli strumenti di AI invogliano a dargli in pasto più dati di quanti servano, perché "funzionano meglio con più contesto". Questo confligge in modo diretto con il principio di minimizzazione, che chiede di trattare solo i dati necessari.

La seconda è l'opacità. Un foglio di calcolo lo capisci: vedi la formula. Un modello di AI, spesso, no. Spiegare perché ha prodotto un certo risultato è difficile, e questa difficoltà entra in tensione con l'obbligo di trasparenza e con il diritto delle persone a capire come vengono trattate.

La terza è la dispersione. Quando usi uno strumento AI di terzi, i dati che gli passi escono dal tuo perimetro ed entrano in quello del fornitore, a volte fuori dall'Unione Europea, a volte in sistemi che li usano per addestrare altri modelli. Sapere dove finiscono i dati diventa una domanda concreta, non

teorica.

Un caso che mette a fuoco il problema

Prendiamo un ufficio del personale che adotta uno strumento di AI per leggere i curriculum e proporre una rosa di candidati. Sembra un'innovazione organizzativa, e lo è. Ma sotto, dal punto di vista della protezione dati, succedono molte cose insieme.

I curriculum sono pieni di dati personali, a volte particolari: stato di salute dedotto da un'aspettativa, appartenenze deducibili da associazioni citate, dati di contatto. Lo strumento li tratta tutti. La proposta della rosa è una profilazione, perché valuta le persone. La decisione su chi chiamare, se presa solo dalla macchina, tocca il diritto a non subire decisioni puramente automatizzate. E se lo strumento è di un fornitore extra-UE, i dati dei candidati escono dall'Unione.

Un solo strumento, adottato per fare prima, attiva la base giuridica, la minimizzazione, la trasparenza, la profilazione, i trasferimenti e spesso la DPIA. Nessuno di questi temi è un cavillo: ognuno protegge una persona reale che ha mandato il suo curriculum fidandosi. È questo intreccio che la guida aiuta a sciogliere, un nodo alla volta.

La privacy come vantaggio, non come freno

Si tende a vedere la protezione dei dati come un costo che rallenta l'adozione dell'AI. È una lettura miope. Un'organizzazione che sa quali dati tratta, dove finiscono e perché, non ha solo meno rischi legali: ha più controllo sui propri processi, risponde più in fretta alle domande dei clienti, e si fida dei propri sistemi perché ne conosce il funzionamento.

C'è poi un effetto sulla fiducia. I clienti, i dipendenti, i cittadini notano la differenza tra un'organizzazione che tratta i loro dati con cura e una che li dà in pasto al primo strumento comodo. In un periodo in cui la diffidenza verso l'AI è alta, poter dimostrare un uso corretto dei dati è un argomento commerciale, non solo un obbligo. Chi tratta bene i dati delle persone costruisce un capitale di fiducia che vale più del tempo risparmiato con una scorciatoia.

Chi risponde: l'organizzazione, non lo strumento

Un equivoco da sciogliere subito riguarda la responsabilità. Quando si usa uno strumento di AI di terzi e qualcosa va storto sui dati, la tentazione è pensare che risponda il fornitore. Non è così, o non solo. Chi decide di usare l'AI per le proprie finalità è il titolare del trattamento, e davanti alle persone e all'autorità risponde lui delle scelte fatte: quali dati, con quale strumento, su quale base.

Il fornitore ha i suoi obblighi, ma non assorbe i tuoi. "Lo fa lo strumento" non è una difesa: lo strumento lo hai scelto tu, e l'hai alimentato con i dati delle persone che ti hanno dato fiducia. Questa è una buona ragione per non delegare le decisioni importanti alla comodità di un servizio, e per scegliere con cura chi tratta i dati al posto tuo. La responsabilità non si esternalizza insieme al trattamento.

In sintesi. Il GDPR non è un adempimento da spuntare alla fine di un progetto AI: è il vincolo che orienta le scelte iniziali. Quantità di dati, opacità dei modelli e dispersione verso i fornitori sono i tre punti in cui l'AI mette sotto pressione le regole esistenti.

C'è anche un motivo di convenienza, non solo di obbligo. Un uso dell'AI costruito bene dal punto di vista della protezione dati è anche un uso più solido sul piano operativo: sai quali dati tratti, con chi, per quanto tempo e perché. Chi salta questi passaggi non guadagna tempo, lo prende in prestito a un tasso alto.

Quando un uso dell'AI tratta dati personali

La domanda da cui parte tutto è una: questo uso dell'AI tratta dati personali, sì o no? La risposta decide se il GDPR si applica, e la risposta è "sì" molto più spesso di quanto si creda.

Un dato personale è qualsiasi informazione relativa a una persona fisica identificata o identificabile. Non solo il nome: un indirizzo email, un numero di telefono, un identificativo di dispositivo, la combinazione di dati che insieme puntano a una persona. "Identificabile" è la parola che allarga il campo: anche un dato che da solo non dice chi è, ma che incrociato con altri permette di risalire alla persona, è un dato personale.

I casi che sembrano innocui e non lo sono

Vale la pena elencare situazioni che molti considerano fuori dal GDPR e che invece ci rientrano in pieno.

- **Incollare una email in un chatbot** per farsi aiutare a rispondere. Se la email contiene il nome o i dati del mittente, stai trattando dati personali con uno strumento di terzi.
- **Caricare un elenco clienti** in uno strumento di analisi AI per segmentarlo. Ogni riga è una persona.
- **Far trascrivere e riassumere una riunione** in cui si parla di colleghi, clienti o candidati.
- **Generare immagini o testi a partire da foto o profili di persone reali.**
- **Usare un assistente per scrivere una valutazione di un dipendente** a partire dai suoi dati.

In tutti questi casi il fatto che lo strumento sia comodo, gratuito o "usato da tutti" non cambia nulla: il trattamento esiste, e con esso gli obblighi.

Il caso particolare dei dati anonimi e pseudonimi

Un dato veramente anonimo, da cui è impossibile risalire alla persona con mezzi ragionevoli, non è un dato personale, e il GDPR non si applica. Ma l'anonimizzazione vera è difficile: togliere il nome non basta se restano elementi che, combinati, identificano qualcuno. La pseudonimizzazione, cioè

sostituire gli identificativi con codici tenendo separata la chiave, riduce il rischio ma non fa uscire dal GDPR: i dati pseudonimi restano dati personali.

Il test in tre domande

Quando hai un dubbio se un'informazione è un dato personale, tre domande lo sciolgono quasi sempre. L'informazione riguarda una persona fisica? Quella persona è identificata, oppure identificabile mettendo insieme i dati che hai o che potresti ragionevolmente ottenere? L'informazione, da sola o combinata, permette di distinguere quella persona dalle altre?

Se la risposta alle prime due è sì, sei dentro il GDPR, e la terza ti dice quanto il dato è "puntato" su quell'individuo. Il punto da non sottovalutare è "ragionevolmente ottenere": non conta solo quello che hai adesso, ma quello a cui potresti arrivare con mezzi alla tua portata. È per questo che un identificativo apparentemente neutro, incrociato con una tabella che possiedi, torna a essere un dato personale a tutti gli effetti.

Identificabile non vuol dire facile

Un equivoco diffuso è pensare che un dato sia personale solo se l'identificazione è immediata. Non è così. Conta la ragionevole possibilità di risalire alla persona, anche con un po' di lavoro e incrociando fonti diverse. Un codice cliente, una targa, un indirizzo IP, la posizione di un dispositivo a una certa ora: presi singolarmente sembrano neutri, ma chi possiede la tabella di corrispondenza, o può ottenerla, identifica la persona senza sforzo.

Per chi usa l'AI questo ha un effetto pratico immediato. Pulire un dataset togliendo i nomi e lasciando tutto il resto raramente lo rende anonimo: spesso restano combinazioni che puntano a un singolo. Prima di considerare "sicuro" un insieme di dati perché privo di nomi, vale la pena chiedersi quante persone, nel mondo, corrispondono a quella precisa combinazione di attributi. Se la risposta è "una", non hai un dato anonimo, hai un dato personale travestito.

Anonimizzare sul serio è difficile

Si parla spesso di anonimizzazione come di un interruttore: tolgo i dati identificativi e il problema sparisce. La realtà è più ostica. Un'anonimizzazione vera deve resistere ai tentativi ragionevoli di re-identificazione, anche incrociando il dato con altre fonti disponibili. Toglierne una parte non basta se le restanti, combinate, restringono il campo a una sola persona.

Esistono tecniche serie per ridurre il rischio, dall'aggregazione alla generalizzazione dei valori, fino all'aggiunta deliberata di rumore. Ma sono lavoro specialistico, non un clic. La regola prudente, per chi non è un esperto, è non dare per anonimo un dato solo perché ha perso il nome, e trattare come personale tutto ciò che, con uno sforzo plausibile, potrebbe ricondurre a qualcuno. Sbagliare in eccesso di prudenza, qui, costa molto meno che sbagliare al contrario.

> **Attenzione.** "Ho tolto il nome, quindi è anonimo" è una delle convinzioni più pericolose. Se con i dati rimasti, da soli o incrociati con altri, si può ancora risalire a una persona, il dato è personale e il GDPR si applica per intero.

I principi del GDPR applicati all'AI

Il GDPR poggia su alcuni principi che valgono per ogni trattamento, AI compresa. Non sono buoni propositi: sono criteri rispetto ai quali un trattamento è lecito o non lo è. Vederli applicati all'AI aiuta a capire dove stanno i punti critici.

Minimizzazione: solo i dati che servono

Devi trattare i dati adeguati, pertinenti e limitati a quanto necessario per la finalità. Con l'AI questo principio è sotto pressione costante, perché la tentazione è dare al modello tutto il contesto disponibile. La domanda da farsi prima di passare un dato a uno strumento è secca: serve davvero a questo scopo? Se la risposta è "non si sa mai", il dato non va passato.

Limitazione della finalità: un dato, uno scopo dichiarato

I dati raccolti per una finalità non si possono usare per un'altra incompatibile senza una base che lo giustifichi. Un esempio frequente: i dati raccolti per erogare un servizio non possono essere riusati per addestrare un modello AI solo perché sono lì e fa comodo. Il riuso per addestramento è una nuova finalità, e va trattato come tale.

Trasparenza ed esattezza: spiegabile e corretto

Le persone hanno diritto di sapere che i loro dati vengono trattati e, in termini comprensibili, come. Con l'AI questo si traduce nel dire che uno strumento automatico è coinvolto e con quale logica generale. L'esattezza, poi, è un tema spesso ignorato: un modello che produce informazioni errate su una persona viola il principio di esattezza, e l'azienda che lo usa ne risponde. Un assistente che "inventa" un dato su un cliente non è un dettaglio tecnico, è un dato personale inesatto trattato dalla tua organizzazione.

Responsabilizzazione: devi poterlo dimostrare

Il GDPR non chiede solo di rispettare le regole, chiede di poterlo provare. Questo principio, l'accountability, è quello che trasforma le buone intenzioni in documenti: registri, valutazioni, contratti, policy. Su un uso dell'AI significa che, se domani il Garante o un interessato fa una domanda, devi avere le carte che mostrano cosa tratti, perché e con quali tutele.

I principi come lista di controllo

Letti tutti insieme, i principi sembrano astratti. Usati come domande prima di avviare un uso dell'AI, diventano una griglia operativa. Sto trattando solo i dati che servono, o ne sto dando di più per comodità? Sto usando i dati per la finalità per cui li ho raccolti, o per una nuova? La persona sa, e capisce, cosa sta succedendo ai suoi dati? L'output che riguarda individui è verificato, o lo do per buono? E se domani mi viene chiesto conto di tutto questo, ho le carte per dimostrarlo?

Cinque domande, cinque principi. Un uso dell'AI che risponde bene a tutte è quasi sempre lecito; uno che inciampa su una sola merita di fermarsi prima di partire. La griglia non sostituisce il giudizio, lo ordina, e si impara ad applicarla nei percorsi formativi di AIPIA.

Esattezza e contenuti inventati

Il principio di esattezza incontra, con l'AI generativa, un problema nuovo: i modelli producono a volte affermazioni false con la stessa sicurezza con cui ne producono di vere. Quando l'affermazione riguarda una persona, un dato sbagliato sulla sua storia, una qualifica che non ha, un fatto mai accaduto, quel contenuto inesatto, se lo usi o lo conservi, è un trattamento di dati personali non conforme.

La conseguenza pratica è netta: l'output che riguarda individui non si copia e incolla a fiducia. Va verificato contro una fonte affidabile prima di entrare in un documento, in una decisione, in una comunicazione. Non è diffidenza verso lo strumento, è applicazione di una regola: non puoi trattare dati che sai, o dovresti sapere, forse errati. La comodità di una risposta immediata non sospende l'obbligo di esattezza, lo rende solo più facile da violare.

> **In sintesi.** Minimizzazione, limitazione della finalità, trasparenza, esattezza e responsabilizzazione non cambiano con l'AI: cambia quanto è facile violarli. Tieni questi cinque principi come griglia di controllo su ogni nuovo uso dell'intelligenza artificiale.

GDPR e AI Act: due regole che si parlano

Dal 2024 il quadro europeo ha un secondo pilastro: l'AI Act, il Regolamento UE 2024/1689. Non sostituisce il GDPR, gli si affianca. Capire come si dividono il lavoro evita due errori opposti: pensare che basti il GDPR e ignorare l'AI Act, o pensare che l'AI Act assorba la privacy e dimenticare il GDPR.

La distinzione di fondo è questa. Il GDPR protegge i dati personali: si attiva quando ci sono persone identificabili coinvolte. L'AI Act regola i sistemi di intelligenza artificiale in base al rischio che pongono, a prescindere dal fatto che trattino o meno dati personali. Quando un sistema AI tratta dati personali, e succede quasi sempre, le due regole si applicano insieme.

ASPETTO	GDPR (REG. UE 2016/679)	AI ACT (REG. UE 2024/1689)
Cosa protegge	I dati personali delle persone fisiche	La sicurezza e i diritti rispetto ai sistemi di AI
Quando si applica	Quando si trattano dati personali	Quando si usa o si fornisce un sistema di AI
Logica di fondo	Liceità, minimizzazione, diritti degli interessati	Classificazione per livello di rischio
Valutazione preventiva	DPIA per i trattamenti ad alto rischio	Obblighi specifici per i sistemi ad alto rischio
Trasparenza	Informativa agli interessati	Obblighi di informazione su contenuti e sistemi AI
Chi vigila in Italia	Garante per la protezione dei dati personali	Autorità designate per la sorveglianza sull'AI

I punti di contatto pratici

Tre incroci contano nella vita di tutti i giorni. Il primo è la valutazione preventiva: il GDPR chiede la DPIA quando il trattamento è ad alto rischio, e molti sistemi AI ad alto rischio sotto l'AI Act trattano dati personali, quindi le due valutazioni si parlano e conviene farle insieme. Il secondo è la trasparenza: l'obbligo del GDPR di informare gli interessati si somma a quello dell'AI Act di segnalare che certi contenuti o decisioni vengono da un sistema AI. Il terzo è l'alfabetizzazione: l'AI Act, all'articolo 4, chiede che chi usa l'AI in azienda abbia un livello adeguato di competenza, e questo include il personale che tratta dati personali con quegli strumenti.

Su quest'ultimo punto si gioca molto, perché un obbligo di competenza diffusa non si soddisfa con una circolare. Per inquadrare l'AI Act nel dettaglio, la guida AIPIA all'AI Act è il riferimento da cui partire.

Cosa cambia in pratica per chi adotta l'AI

Per un'organizzazione che introduce l'AI oggi, la convivenza tra GDPR e AI Act si traduce in tre abitudini. La prima è non separare le valutazioni: quando un sistema AI tratta dati personali ed è ad alto rischio, la valutazione d'impatto privacy e gli obblighi dell'AI Act si analizzano nello stesso lavoro, non in due pratiche scollegate.

La seconda è curare la trasparenza su due fronti: dire alle persone che i dati sono trattati, come chiede il GDPR, e segnalare che certi contenuti o decisioni vengono da un sistema AI, come chiede l'AI Act. La terza è investire sulla competenza del personale, perché l'obbligo di alfabetizzazione non è un consiglio ma una richiesta normativa, e perché una squadra che capisce gli strumenti commette meno errori sui dati.

I tempi di applicazione

Un aspetto pratico dell'AI Act è che non si applica tutto nello stesso momento: gli obblighi entrano in vigore in fasi successive, alcuni prima, altri dopo. Questo significa che chi adotta l'AI oggi si muove in un quadro che si completa per gradi, e conviene sapere quali obblighi sono già pienamente operativi e quali stanno arrivando, per non trovarsi impreparati quando scattano.

Il messaggio per chi pianifica è di non aspettare l'ultima scadenza per organizzarsi. Costruire fin da subito un uso dell'AI conforme al GDPR e attento ai principi dell'AI Act significa farsi trovare pronti man mano che gli obblighi diventano pienamente esigibili, invece di rincorrerli sotto pressione. Anticipare costa meno che adeguarsi all'ultimo, e lascia tempo per fare le cose con ordine anziché in emergenza.

Le categorie di rischio che toccano i dati

L'AI Act ordina i sistemi per livello di rischio, e diversi tra quelli classificati ad alto rischio sono proprio quelli che trattano dati personali in modo delicato: la selezione del personale, la valutazione dell'accesso al credito, certi usi in ambito biometrico, alcuni impieghi nei servizi pubblici essenziali. Non è un caso: sono gli usi in cui una decisione automatica può incidere pesantemente sulla vita di una persona.

Per chi adotta l'AI, la lettura combinata è utile come bussola. Se il tuo uso rientra tra quelli che l'AI Act considera ad alto rischio, quasi sempre tratta anche dati personali in modo che richiede attenzione sotto il GDPR, DPIA compresa. Le due valutazioni illuminano lo stesso oggetto da angoli diversi, e farle insieme evita sia doppioni sia buchi. Riconoscere presto che un uso è ad alto rischio è il primo passo per trattarlo con la cura che merita.

> **In sintesi.** GDPR e AI Act non si sovrappongono, si completano: uno protegge i dati, l'altro governa il rischio dei sistemi. Quando un'AI tratta dati personali, le due valutazioni vanno fatte insieme, e la competenza del personale diventa un obbligo, non un di più.

PARTE II

Le scelte da fare

Le decisioni che rendono lecito, o illecito, un uso dell'AI: la base giuridica, l'informativa, cosa dai in pasto allo strumento, cosa fai con l'output e come tratti i dati delicati.

Basi giuridiche: su quale fondamento usare i dati

Nessun trattamento di dati personali è lecito senza una base giuridica. È il primo controllo, non l'ultimo: prima di chiederti se l'AI è sicura o accurata, chiediti su quale fondamento stai trattando quei dati. Il GDPR ne prevede sei, e per un uso aziendale dell'AI tre sono quelle che ricorrono.

Le tre basi più frequenti

Il **consenso** è la base più conosciuta e la più fraintesa. Deve essere libero, specifico, informato e revocabile. "Libero" significa che la persona deve poter dire di no senza conseguenze: un consenso imposto come condizione per un servizio che non lo richiede non è valido. Per molti usi interni dell'AI il consenso non è la base giusta, perché tra datore di lavoro e dipendente la libertà di rifiutare è dubbia.

Il **contratto** giustifica i trattamenti necessari per eseguire un accordo con l'interessato. Se l'AI serve a erogare il servizio che il cliente ha richiesto, questa può essere la base. Il limite è "necessari": un uso dell'AI accessorio, che si potrebbe evitare, non rientra nell'esecuzione del contratto.

Il **legittimo interesse** è la base più flessibile e la più impegnativa da usare bene. Permette trattamenti che servono a un interesse legittimo del titolare, a patto che non prevalgano i diritti e le libertà degli interessati. Usarlo richiede un bilanciamento documentato, il cosiddetto test di legittimo interesse, in cui scrivi nero su bianco perché il tuo interesse regge il confronto con l'impatto sulle persone.

BASE GIURIDICA	QUANDO SI ADATTA ALL'AI	PUNTO CRITICO
Consenso	Usi non necessari, rivolti a clienti, dove la persona può scegliere	Deve essere libero e revocabile: difficile coi dipendenti
Contratto	L'AI serve a erogare il servizio richiesto dall'interessato	Solo i trattamenti davvero necessari all'accordo
Legittimo interesse	Usi interni utili al titolare, a basso impatto sulle persone	Richiede un bilanciamento scritto, non basta affermarlo
Obbligo legale	Quando una norma impone il trattamento	Va individuata la norma specifica

Una cosa da fissare: la base giuridica si sceglie prima, non si cerca dopo. Avviare un uso dell'AI e poi domandarsi su quale fondamento poggiava è il modo più rapido per scoprire che non ne aveva uno.

Il test di legittimo interesse, in concreto

Scegliere il legittimo interesse come base non significa scriverlo e andare avanti: significa fare e conservare un bilanciamento in tre passaggi. Primo, individua l'interesse: qual è il vantaggio legittimo che persegui, in termini concreti e non generici. Secondo, verifica la necessità: quell'interesse si può ottenere con un trattamento meno invasivo? Se sì, devi scegliere quello. Terzo, pesa l'impatto sulle persone: cosa rischiano, se lo aspettano, possono opporsi facilmente.

Se al termine il tuo interesse regge il confronto con i diritti delle persone, hai una base solida e documentata. Se non regge, il legittimo interesse non è la strada, e insistere significa costruire su un fondamento che cade alla prima verifica. Il bilanciamento scritto non è burocrazia: è la prova che la scelta è stata ponderata, ed è la prima cosa che un'autorità chiede di vedere.

Le altre basi, utili soprattutto nella PA

Oltre alle tre più frequenti, il GDPR ne prevede altre che contano in contesti specifici. L'obbligo legale copre i trattamenti imposti da una norma: qui non scegli, devi, e la base è la legge stessa, da individuare con precisione. L'interesse vitale riguarda situazioni eccezionali in cui è in gioco la vita di una persona, raro nell'uso ordinario dell'AI. Il compito di interesse pubblico è la base tipica della pubblica amministrazione, che tratta dati per svolgere funzioni assegnate dalla legge.

Per un ente pubblico che introduce l'AI, il punto non è inventare una base, ma ricondurre l'uso a una funzione che già gli compete, verificando che lo strumento resti dentro quei confini. Un comune che usa l'AI per organizzare pratiche dei cittadini si muove su un fondamento diverso da un'azienda privata, e le valutazioni di proporzionalità, in ambito pubblico, sono se possibile più stringenti, perché il cittadino non può scegliere un altro fornitore del servizio.

La revoca del consenso e le sue conseguenze

Se scegli il consenso come base, devi fare i conti con una sua caratteristica: si può revocare, e la revoca deve essere facile come la concessione. Quando una persona ritira il consenso, il trattamento basato su di esso deve fermarsi, e i dati trattati solo grazie a quel consenso vanno cancellati, salvo che un'altra base ne giustifichi la conservazione.

Con l'AI questo crea un problema concreto: se i dati di quella persona sono già finiti in cronologie, in sistemi collegati o, peggio, nell'addestramento di un modello, la revoca diventa difficile da onorare davvero. È un altro motivo per cui il consenso, scelto con leggerezza, può rivelarsi una base fragile. Prima di adottarlo, chiediti se sapresti onorare una revoca fino in fondo. Se la risposta è no, forse il consenso non era la base giusta, o lo strumento non era quello adatto.

> **Attenzione.** Il consenso non è la risposta a tutto. Spesso viene scelto per abitudine quando sarebbe più solido il legittimo interesse o il contratto. Un consenso non valido, perché non libero o non informato, fa cadere la liceità dell'intero trattamento.

Informativa e trasparenza verso gli interessati

Le persone hanno il diritto di sapere che i loro dati vengono trattati e come. Questo diritto non si sospende quando entra in gioco l'AI: semmai diventa più impegnativo, perché spiegare un trattamento automatico in modo comprensibile richiede uno sforzo in più.

L'informativa è lo strumento con cui assolvi questo obbligo. Deve dire chi tratta i dati, per quali finalità, su quale base giuridica, per quanto tempo, a chi vengono comunicati e quali diritti ha l'interessato. Quando c'è di mezzo l'AI, vanno aggiunti alcuni elementi.

Cosa aggiungere quando c'è l'AI

- **Che è coinvolto un trattamento automatizzato**, in termini che una persona normale capisce, senza gergo tecnico.
- **La logica generale** del trattamento: non il codice del modello, ma a cosa serve e su che basi opera.
- **Le conseguenze previste** per l'interessato, soprattutto se dall'uso dell'AI derivano decisioni che lo riguardano.
- **I fornitori coinvolti**, almeno per categoria, se i dati passano da strumenti di terzi.

Il principio guida è la comprensibilità. Un'informativa scritta per non essere letta, lunga e in burocratese, non assolve l'obbligo di trasparenza: lo aggira sulla carta. Meglio poche frasi chiare che dieci pagine illeggibili.

> *La trasparenza non si misura dalla lunghezza dell'informativa, ma da quanto la persona ha capito dopo averla letta. Un testo che nessuno comprende non informa: nasconde con metodo.*
>
> PRINCIPIO GUIDA DEI CORSI AIPIA

Un esempio concreto. Un'azienda introduce un assistente che analizza le richieste dei clienti per smistarle. L'informativa esistente parlava di "gestione delle richieste"; ora deve dire, in una riga, che le richieste sono analizzate anche con uno strumento automatico per indirizzarle all'ufficio giusto, e che resta possibile chiedere un intervento umano. Poche parole, ma cambiano la sostanza.

L'informativa a livelli

Conciliare completezza e leggibilità sembra impossibile, ma una tecnica funziona: l'informativa a livelli. Al primo livello, poche frasi che dicono l'essenziale nel punto in cui la persona interagisce: chi tratta i dati, per fare cosa, con quale strumento, quali diritti ha. Al secondo livello, un testo esteso, raggiungibile da chi vuole sapere di più, con tutti i dettagli richiesti.

Così non costringi nessuno a leggere dieci pagine per usare un servizio, ma le metti a disposizione di chi le cerca. È il modo migliore per rispettare la trasparenza senza trasformarla in un muro di testo che protegge solo chi lo ha scritto. La trasparenza vera si vede da qui: la persona, dopo il primo livello, ha capito cosa conta.

Un'informativa prima e dopo

Per vedere la differenza, confrontiamo due versioni. La prima dice: "I suoi dati saranno trattati per le finalità connesse all'erogazione del servizio, anche mediante strumenti automatizzati, nel rispetto della normativa vigente." Tecnicamente corretta, praticamente inutile: nessuno capisce cosa succede davvero.

La seconda dice: "Per rispondere più in fretta, analizziamo la sua richiesta con uno strumento automatico che la indirizza all'ufficio giusto. Nessuna decisione importante viene presa solo dalla macchina: può sempre chiedere di parlare con una persona." Stesse poche righe, ma ora la persona sa cosa accade, cosa fa lo strumento e quale via d'uscita ha. La seconda informa, la prima si limita a coprirsi. La trasparenza vera costa qualche parola di chiarezza in più, non una pagina di formule in più.

Il momento giusto per informare

La trasparenza non è solo questione di cosa scrivi, ma di quando lo dici. L'informazione va data prima o nel momento in cui il dato viene raccolto, non dopo che il trattamento è già avvenuto. Avvisare una persona che i suoi dati sono stati analizzati da un'AI quando ormai la decisione è presa svuota il diritto di significato: la trasparenza serve a permettere una scelta, e una scelta a cose fatte non è una scelta.

Per gli usi dell'AI questo significa integrare l'informazione nei punti di contatto reali: il modulo che la persona compila, la pagina del servizio, la comunicazione con cui si avvia il rapporto. Aggiornare l'informativa quando si introduce un nuovo strumento, e farlo prima di accenderlo, è parte del lavoro, non un adempimento da rimandare a quando si avrà tempo.

Dati in input: cosa puoi dare a uno strumento e cosa no

Il momento più rischioso nell'uso quotidiano dell'AI è quello in cui qualcuno copia qualcosa e lo incolla in uno strumento. Lì, in un gesto di due secondi, si decide se un dato esce o resta dentro il perimetro dell'organizzazione. Per questo i dati in input meritano una regola esplicita, conosciuta da chi usa gli strumenti.

La gerarchia del "cosa puoi dare"

Non tutti i dati sono uguali e non tutti gli strumenti sono uguali. La combinazione delle due cose decide. Una griglia mentale utile distingue tre livelli di dato.

- **Dati non personali**, già pubblici o aggregati senza riferimento a persone: il rischio privacy è basso, restano gli altri rischi (riservatezza aziendale, segreti).
- **Dati personali comuni**, come nomi, contatti, contenuti di comunicazioni: si possono trattare con uno strumento solo se c'è una base giuridica e il fornitore offre garanzie adeguate.
- **Dati particolari e ad alto impatto**, come salute, dati di minori, valutazioni che incidono su una persona: di norma non vanno passati a strumenti generici, e comunque mai senza una valutazione preventiva.

La regola che evita la maggior parte dei guai

C'è una domanda che, posta prima di incollare, previene quasi tutti gli incidenti: questo strumento, con questo dato, è autorizzato? Se l'organizzazione non ha deciso quali strumenti sono ammessi per quali dati, la decisione finisce nelle mani del singolo, nel momento sbagliato, sotto pressione di una scadenza. Una policy chiara, di cui parliamo nella Parte IV, sposta la decisione dove deve stare.

Un caso tipico da evitare: un dipendente usa un chatbot personale e gratuito per riscrivere una lettera che contiene i dati sanitari di un cliente. Strumento non autorizzato, dato particolare, nessuna base verificata, nessun contratto col fornitore. Quattro violazioni in un gesto, fatto in buona fede per fare prima.

Lo shadow AI: il rischio che non vedi

Esiste un fenomeno che ogni organizzazione sottovaluta: lo shadow AI, cioè l'uso di strumenti di intelligenza artificiale fatto dal personale senza che l'azienda lo sappia. Nasce sempre per buone ragioni, qualcuno vuole lavorare meglio o più in fretta, e proprio per questo è difficile da fermare con i divieti.

Il problema è che lo shadow AI tratta dati personali fuori da ogni controllo: senza contratto col fornitore, senza base giuridica verificata, senza sapere dove finiscono i dati. Un divieto secco raramente funziona, perché spinge l'uso ancora più nell'ombra. Funziona meglio dare un'alternativa: strumenti ammessi, chiari e comodi, così che usare quelli giusti sia la via più semplice, non un ostacolo. La domanda da porsi non è "come vieto", ma "perché le persone sentono il bisogno di usare strumenti non autorizzati", e rimuovere quel bisogno alla radice.

Una matrice dati per strumenti

Il modo più chiaro per dare regole sui dati in input è una matrice: in riga il tipo di dato, in colonna il tipo di strumento, e in ogni casella un sì, un no o un "solo con condizioni". Costruirla obbliga a decidere in anticipo, una volta per tutte, invece di lasciare la scelta al singolo nel momento sbagliato.

TIPO DI DATO	STRUMENTO GENERICO PUBBLICO	STRUMENTO AZIENDALE CON CONTRATTO
Dati non personali	Ammesso	Ammesso
Dati personali comuni	No	Sì, con base giuridica
Dati particolari (salute, ecc.)	No	Solo dopo valutazione e su base rafforzata
Dati di minori	No	Solo con tutela rafforzata

Una matrice come questa, affissa dove si lavora, risolve in un colpo solo la domanda che altrimenti torna ogni giorno. Non serve che sia complicata: serve che sia chiara e che chi usa gli strumenti la conosca a memoria per i casi che incontra più spesso.

Se un dato è già uscito

Quando ci si accorge che un dato è finito dove non doveva, conta la reazione. Il primo riflesso giusto non è nascondere l'accaduto, ma valutarne la portata: quali dati, quante persone, quale strumento, cosa può farne. Da lì si decide se è un fastidio gestibile internamente o un evento che richiede di attivare la procedura per le violazioni dei dati, con eventuale notifica.

Per questo conviene che chi usa gli strumenti sappia a chi segnalare un errore senza temere una punizione. Un'organizzazione che colpevolizza chi segnala ottiene solo che gli errori vengano taciuti, ed è esattamente il modo in cui un piccolo incidente diventa un caso serio. Premiare la segnalazione tempestiva, non punirla, è la scelta che riduce i danni nel lungo periodo.

> **In sintesi.** Il rischio dei dati in input non è teorico: vive nel copia-incolla quotidiano. Decidi a monte quali dati possono entrare in quali strumenti, scrivilo, e fai in modo che chi lavora lo sappia. La buona fede non sostituisce una regola.

Dati in output e profilazione: rischi e cautele

Quello che l'AI produce è importante quanto quello che riceve. L'output di un sistema può contenere dati personali nuovi, può essere inesatto, e può alimentare decisioni che incidono sulle persone. Tre rischi distinti, da maneggiare separatamente.

Output inesatto: l'errore che diventa tuo

I modelli generativi producono talvolta informazioni false con tono sicuro. Se un sistema afferma un dato sbagliato su una persona, e la tua organizzazione lo usa, quel dato inesatto è un trattamento di cui rispondi. Il principio di esattezza impone di non trattare dati errati: verificare l'output che riguarda persone, prima di usarlo o conservarlo, non è prudenza facoltativa, è applicazione di una regola.

Profilazione: quando l'AI valuta le persone

La profilazione è il trattamento automatizzato che valuta aspetti di una persona per prevederne comportamenti, preferenze, rendimento, affidabilità. L'AI la rende facile e diffusa. Il GDPR la consente, ma con cautele: trasparenza rafforzata, base giuridica solida, e tutele particolari quando dalla profilazione derivano decisioni rilevanti.

Un esempio frequente in azienda è la valutazione automatica dei candidati o dei dipendenti. Far ordinare i curriculum a un modello è profilazione, e se l'esito orienta chi viene chiamato o promosso, le tutele si alzano. Non è vietato, è regolato: serve sapere cosa fa il sistema, poterlo spiegare e lasciare spazio a un controllo umano reale.

Output che diventa input: il ciclo nascosto

Un rischio meno ovvio: l'output di un sistema che rientra come input in un altro, accumulando errori e perdendo tracciabilità. Una valutazione generata da un'AI che viene usata per addestrare o alimentare un secondo strumento crea una catena in cui, a un certo punto, nessuno sa più da dove viene un certo giudizio su una persona. Tenere separati e tracciati i passaggi è ciò che permette di rispondere alle domande degli interessati.

Il diritto di contestare, in pratica

Quando dall'AI deriva una decisione che incide su una persona, quella persona deve poterla contestare a un essere umano in grado di rivederla. Tradurre questo principio in un processo richiede di pensarci prima. Chi riceve la contestazione? Ha accesso ai dati e alla logica per capire come si è arrivati a quell'esito? Ha l'autorità di ribaltarlo?

Un esempio rende il punto. Un sistema scarta automaticamente una richiesta di un cliente. Il cliente protesta. Se in azienda nessuno sa spiegare perché il sistema ha deciso così, e nessuno può rivedere la decisione, il diritto a contestare esiste solo sulla carta. Progettare l'uso dell'AI significa anche progettare la via d'uscita umana, non solo l'automazione.

Quando l'output discrimina senza volerlo

Un rischio specifico dell'output AI merita attenzione: la discriminazione involontaria. Un sistema addestrato su dati che riflettono squilibri del passato tende a riprodurli, anche senza che nessuno lo voglia. Un modello che valuta candidati può penalizzare in modo sistematico un certo gruppo, semplicemente perché nei dati storici quel gruppo compariva meno tra gli assunti.

Questo intreccia la protezione dei dati con il divieto di discriminazione. Un output che colpisce sempre lo stesso tipo di persone non è solo un problema di qualità: può ledere diritti. Per chi usa l'AI su decisioni che riguardano individui, controllare non solo il singolo esito ma anche se il sistema tratta in modo sistematicamente diverso gruppi di persone diventa parte della diligenza richiesta. L'oggettività della macchina è apparente: eredita gli errori di chi l'ha addestrata.

Quando l'output è un dato personale nuovo

Un aspetto sottile: l'AI non si limita a trattare i dati che riceve, ne crea di nuovi. Una valutazione, un punteggio, una previsione su una persona sono dati personali a tutti gli effetti, generati dal sistema, e ricadono sotto il GDPR come e più di quelli di partenza. Un giudizio sintetico su un cliente, prodotto da un modello, è un dato che lo riguarda, che va trattato con base giuridica, conservato per il tempo giusto e cancellabile su richiesta.

Questo amplia il perimetro di ciò di cui rispondi. Non basta governare i dati che entrano: vanno governati anche quelli che escono, soprattutto quando sono giudizi o previsioni destinati a influenzare come tratterai quella persona. Un punteggio dimenticato in un sistema, che orienta decisioni senza che nessuno sappia da dove viene, è esattamente il tipo di dato che crea problemi quando l'interessato chiede conto di come è stato valutato.

> **Attenzione.** Un dato inesatto prodotto dall'AI su una persona diventa, nel momento in cui lo usi, un tuo trattamento illecito. Controllare l'output che riguarda individui non è un controllo di qualità opzionale: è un obbligo che discende dal principio di esattezza.

Dati particolari e categorie a rischio

Alcuni dati ricevono dal GDPR una protezione rafforzata, perché il loro uso improprio può ferire le persone in modo grave. Sono le categorie particolari: dati che rivelano origine, opinioni politiche, convinzioni religiose, appartenenza sindacale, dati genetici, biometrici, relativi alla salute, alla vita sessuale o all'orientamento. Per questi, il trattamento è vietato salvo eccezioni precise.

Con l'AI il tema è delicato per una ragione specifica: questi dati possono entrare di nascosto. Una foto può rivelare dati biometrici o di salute, un testo libero può contenere riferimenti a opinioni o condizioni, una richiesta di assistenza può svelare una diagnosi. Lo strumento non distingue: tratta quello che riceve.

CATEGORIA A RISCHIO	DOVE PUÒ ENTRARE NELL'AI	CAUTELA MINIMA
Dati di salute	Richieste assistenza, testi liberi, immagini	Eccezione esplicita richiesta, di norma fuori dagli strumenti generici
Dati biometrici	Foto e video dati a strumenti di analisi	Valutazione preventiva, evitare l'uso per identificare
Opinioni e convinzioni	Testi, post, comunicazioni analizzate	Non dedurle né registrarle senza base rafforzata
Dati di minori	Servizi rivolti a famiglie, scuola, sanità	Tutela rafforzata, attenzione al consenso
Dati giudiziari	Verifiche, valutazioni di affidabilità	Trattamento soggetto a condizioni stringenti

La regola operativa è prudente per scelta: i dati particolari non vanno passati a strumenti AI generici, e quando il loro trattamento è necessario va preceduto da una valutazione, spesso da una DPIA, e poggiato su una delle eccezioni previste. In sanità e in ambito sociale, dove questi dati sono il pane quotidiano, la cautela non è un freno burocratico: è ciò che separa un uso difendibile da uno indifendibile.

Un esempio dal settore sanitario

In sanità i dati particolari sono il lavoro quotidiano, e l'AI offre aiuti concreti, dalla gestione delle prenotazioni all'organizzazione documentale. Ma la linea va tenuta ferma. Un assistente che riorganizza le agende tratta dati comuni e, con le giuste cautele, è gestibile. Un assistente a cui si chiede di leggere referti, sintetizzare diagnosi o suggerire valutazioni cliniche tratta dati di salute, e cambia tutto.

In questo secondo caso servono una base rafforzata, una valutazione d'impatto, strumenti che trattino i dati dentro l'Unione e con garanzie verificate, e la supervisione di un professionista sanitario su ogni esito che riguarda un paziente. Non perché l'AI non possa aiutare, ma perché qui un errore non è un fastidio: tocca la salute di una persona. La prudenza, in questo ambito, è competenza, non timidezza, e si nutre di studio: i libri AIPIA sull'intelligenza artificiale affrontano anche questi nodi.

Come i dati delicati entrano senza permesso

Il pericolo dei dati particolari, con l'AI, sta nel fatto che entrano senza essere annunciati. Una foto caricata per un'analisi può contenere informazioni sulla salute visibili a occhio, o tratti che diventano dati biometrici se elaborati per riconoscere la persona. Un testo libero, una mail, una richiesta di

assistenza, può rivelare una diagnosi, un orientamento, un'opinione politica, senza che chi lo incolla ci pensi.

Lo strumento non distingue: elabora tutto ciò che riceve, e una volta elaborato il dato delicato è stato trattato. Per questo la cautela non può limitarsi a "non trattare dati particolari di proposito": deve includere il chiedersi, prima di passare un contenuto, se al suo interno potrebbero nascondersi categorie protette. Nei testi liberi e nelle immagini la risposta è spesso sì, ed è lì che la disciplina di chi usa lo strumento fa la differenza tra un uso prudente e uno scoperto.

> **In sintesi.** I dati particolari pretendono una soglia di attenzione più alta e spesso entrano nell'AI senza che ce ne si accorga, dentro foto e testi liberi. La regola sicura è tenerli fuori dagli strumenti generici e trattarli solo dopo una valutazione e su una base rafforzata.

PARTE III

Fornitori, DPIA, sicurezza

Qui l'AI esce dal tuo perimetro: chi tratta i dati al posto tuo, dove finiscono, come valuti il rischio prima di partire e come proteggi tutto questo.

I fornitori di AI: responsabile, nomine e contratti

Quasi nessuno costruisce l'AI in casa. Si usano strumenti di terzi, e nel momento in cui passi dati personali a uno strumento esterno, quel fornitore tratta dati per conto tuo. Questo fatto, ovvio una volta detto, ha conseguenze contrattuali precise che molte organizzazioni scoprono troppo tardi.

Nel linguaggio del GDPR, tu che decidi finalità e mezzi sei il titolare del trattamento; il fornitore che tratta i dati seguendo le tue istruzioni è il responsabile del trattamento. Questo rapporto non può essere informale: va regolato da un contratto, l'accordo sul trattamento dei dati, che il GDPR rende obbligatorio.

Cosa deve esserci nel contratto

L'accordo con il fornitore deve dire, come minimo, cosa tratta, per quali finalità, per quanto tempo, con quali misure di sicurezza, se e quali sub-fornitori usa, dove si trovano i dati e cosa succede alla fine del rapporto. Per gli strumenti di AI un punto è decisivo e va verificato esplicitamente: i tuoi dati vengono usati per addestrare i modelli del fornitore? Se la risposta è sì e tu non l'hai autorizzato, hai un problema.

Titolare, responsabile, contitolare

Tre ruoli da non confondere. Il titolare decide. Il responsabile esegue per conto del titolare. La contitolarità esiste quando due soggetti decidono insieme finalità e mezzi, e allora le responsabilità vanno ripartite per iscritto. Sbagliare l'inquadramento del fornitore, trattarlo da semplice strumento quando in realtà decide qualcosa sui dati, lascia scoperti entrambi.

Un esempio: un'azienda adotta una piattaforma AI che, oltre a erogare il servizio, usa i dati per migliorare i propri modelli a beneficio di tutti i clienti. Su quella seconda finalità il fornitore non è più un semplice responsabile: decide per conto proprio. Quel passaggio va capito e regolato, non subìto leggendo le condizioni dopo la firma.

I sub-fornitori: la catena che non vedi

Un fornitore di AI raramente lavora da solo. Dietro lo strumento che adotti ci sono quasi sempre altri soggetti: chi fornisce l'infrastruttura, chi sviluppa il modello, chi gestisce parti del servizio. Sono i sub-responsabili, e i tuoi dati passano anche da loro. Il GDPR chiede che il fornitore non ne aggiunga di nuovi senza informarti e che li vincoli agli stessi obblighi che ha verso di te.

Tradotto in pratica, prima di firmare devi sapere chi c'è nella catena e dove si trova. Un fornitore che non sa o non vuole dirti quali sub-responsabili usa ti chiede di fidarti al buio di soggetti che non conosci. Per dati che contano, è una richiesta a cui rispondere con un no, o almeno con altre domande.

Un esempio frequente: uno strumento di trascrizione che, dietro le quinte, manda l'audio a un servizio terzo per l'elaborazione. Le registrazioni delle riunioni, con le voci e i contenuti di persone reali, passano da un soggetto in più di cui spesso il cliente ignora persino l'esistenza. La mappa della catena non è un dettaglio contrattuale: è sapere dove vanno davvero le voci dei tuoi interlocutori.

Quando il fornitore decide per conto suo

La linea tra responsabile e titolare autonomo si sposta nel momento in cui il fornitore usa i tuoi dati per finalità proprie. Migliorare i suoi modelli a beneficio di tutti i clienti, costruire statistiche commerciali, sviluppare nuovi servizi: in questi casi il fornitore non sta più solo eseguendo le tue istruzioni, sta perseguendo un interesse suo. E allora la responsabilità verso gli interessati non è più solo tua.

Il problema è che questo passaggio spesso non è dichiarato a chiare lettere: vive in una clausola delle condizioni d'uso, scritta per non essere notata. Leggerla prima di firmare è ciò che ti permette di sapere se stai affidando i dati a un esecutore o se li stai consegnando a qualcuno che ne farà anche altro. Le due situazioni hanno conseguenze molto diverse per le persone i cui dati tratti, e per la tua responsabilità verso di loro.

Una nomina sbagliata, e cosa comporta

Capita spesso di vedere fornitori usati senza alcun inquadramento formale: si attiva il servizio, si caricano i dati, e del rapporto contrattuale sui dati nessuno si occupa. È una nomina mancante, e lascia scoperti entrambi. Se domani quel fornitore subisce un incidente o usa i dati oltre il dovuto, manca il documento che definisce chi doveva fare cosa, e la responsabilità ricade per intero sul titolare che ha trascurato il passaggio.

Il rimedio è semplice e va fatto prima, non dopo: nessun dato personale a un fornitore senza un accordo sul trattamento che lo vincoli. Non è un formalismo da legali, è ciò che trasforma una promessa commerciale in un obbligo esigibile. Un fornitore serio lo propone lui stesso; uno che non ce l'ha, o che fatica a fornirlo, sta dicendo qualcosa di sé che conviene ascoltare prima di affidargli i dati delle persone.

In sintesi. Ogni strumento AI esterno a cui dai dati è un responsabile del trattamento, e va legato da un contratto che dica cosa fa con quei dati, soprattutto se li usa per addestrare i suoi modelli. Senza quel contratto, il trasferimento di dati è scoperto.

Trasferimenti extra-UE: dove finiscono i dati

Molti strumenti di AI hanno server e società fuori dall'Unione Europea. Quando i tuoi dati personali finiscono su quei server, stai facendo un trasferimento verso un paese terzo, e il GDPR pone condizioni precise perché sia lecito.

La logica è semplice: i dati delle persone non possono uscire dall'Unione verso luoghi che non garantiscono una protezione equivalente, a meno che non si adottino strumenti che colmano la differenza. Tradotto in pratica, prima di usare uno strumento devi sapere dove tratta i dati.

Le domande da porsi

- **Dove sono i server** che trattano i dati? Dentro o fuori dall'Unione Europea?
- **Quale meccanismo di trasferimento** usa il fornitore per i dati che escono? Esiste e lo dichiara?
- **Quali garanzie aggiuntive** offre rispetto ad accessi da parte di autorità di paesi terzi?
- **Esiste un'opzione di trattamento solo dentro l'Unione**, e a quali condizioni?

La questione non è teorica. Per un'organizzazione europea, scegliere uno strumento che tiene i dati nell'Unione, o che offre garanzie serie sui trasferimenti, è spesso la differenza tra un uso difendibile e uno costantemente a rischio. Non sempre l'opzione più comoda è quella più sicura, e la scelta va fatta con i dati alla mano, non per inerzia.

Perché la posizione dei dati conta davvero

Sembra un tecnicismo, ma ha conseguenze concrete. Quando i dati personali si trovano fuori dall'Unione, possono essere soggetti a richieste di accesso da parte di autorità di quel paese, con regole diverse e tutele inferiori a quelle europee. La persona i cui dati hai affidato a uno strumento non sa, e non ha scelto, di esporsi a quel rischio.

Per questo la scelta di uno strumento che tratta i dati dentro l'Unione, dove possibile, non è un capriccio di conformità: riduce in modo concreto l'esposizione. Molti fornitori offrono ormai l'opzione di trattamento europeo, a volte come impostazione, a volte da attivare. Verificarlo prima costa una domanda; scoprirlo dopo, quando i dati sono già usciti, costa molto di più.

La regola pratica per chi adotta: dove finiscono i dati è una delle prime cose da chiarire, non l'ultima. Un uso dell'AI che non sa rispondere a "dove sono i miei dati in questo momento" è un uso che naviga senza strumenti, e prima o poi incontra lo scoglio.

Le opzioni di trattamento europeo

La buona notizia è che il mercato si è mosso. Molti fornitori offrono oggi configurazioni che tengono i dati dentro l'Unione, e alcuni propongono soluzioni pensate apposta per chi ha requisiti stringenti, dalla pubblica amministrazione alla sanità. Non sempre sono l'impostazione predefinita: spesso vanno scelte e a volte costano un po' di più.

La valutazione, allora, non è solo tecnica ma anche di priorità. Quanto valgono i dati che tratti? Chi sono le persone dietro quei dati e cosa rischiano? Per trattamenti che toccano molte persone o dati delicati, l'opzione europea, anche se meno comoda o più cara, è quasi sempre la scelta che regge nel tempo. Risparmiare sulla posizione dei dati è uno di quei risparmi che si pagano con gli interessi quando arriva la prima richiesta a cui non sai rispondere.

Gli strumenti di trasferimento, in parole semplici

Quando i dati devono uscire dall'Unione, il GDPR non lo vieta in assoluto: chiede di colmare la differenza di protezione con strumenti adeguati. Senza entrare nei tecnicismi, esistono meccanismi riconosciuti che il fornitore deve adottare e dichiarare: decisioni che riconoscono certi paesi come adeguati, clausole contrattuali tipo, garanzie aggiuntive caso per caso.

Per chi adotta uno strumento, la verifica pratica è duplice: il fornitore usa uno di questi meccanismi, e lo dichiara nero su bianco? E quel meccanismo regge davvero rispetto ai rischi del paese in cui i dati finiscono? Un fornitore che cita una clausola ma non spiega come protegge i dati dagli accessi delle autorità locali offre una garanzia di facciata. La sostanza, non l'etichetta, è ciò che rende lecito il trasferimento.

La valutazione d'impatto (DPIA): quando e come

La valutazione d'impatto sulla protezione dei dati, la DPIA, è lo strumento con cui analizzi un trattamento rischioso prima di avviarlo. Non è un adempimento formale: è il momento in cui ti fermi a guardare cosa potrebbe andare storto e decidi come ridurre il rischio. Per molti usi dell'AI è obbligatoria.

Quando serve davvero

Il GDPR la richiede quando un trattamento può presentare un rischio elevato per i diritti delle persone. Tre situazioni la rendono quasi sempre necessaria, e l'AI le tocca spesso: la valutazione sistematica di aspetti personali tramite trattamenti automatizzati, il trattamento su larga scala di dati particolari, la sorveglianza sistematica. Se il tuo uso dell'AI rientra in una di queste, la DPIA non è opzionale.

Cosa contiene

Una DPIA descrive il trattamento, ne valuta la necessità e la proporzionalità, analizza i rischi per le persone e individua le misure per ridurli. Non è un documento per il cassetto: è la traccia che dimostra di aver pensato prima di agire, e che guida le scelte tecniche e organizzative. Ecco uno schema essenziale da adattare.

```
DPIA - Uso di AI per [nome del trattamento]

1. DESCRIZIONE
   - Cosa fa il sistema, quali dati usa, da dove arrivano
   - Finalità e base giuridica
   - Fornitori coinvolti e dove trattano i dati

2. NECESSITÀ E PROPORZIONALITÀ
   - Il trattamento serve davvero allo scopo?
   - Si può ottenere lo stesso risultato con meno dati?
   - Le persone se lo aspettano?

3. RISCHI PER LE PERSONE
   - Cosa succede se i dati escono o sono errati?
   - Decisioni automatizzate che incidono su qualcuno?
   - Categorie particolari coinvolte?

4. MISURE PER RIDURRE IL RISCHIO
   - Minimizzazione, pseudonimizzazione, accessi
   - Controllo umano sulle decisioni rilevanti
   - Contratto col fornitore e garanzie sui trasferimenti

5. ESITO
   - Rischio residuo accettabile? Si / No
   - Se no: consultazione del Garante prima di partire
```

Un punto spesso trascurato: se al termine della DPIA il rischio resta elevato nonostante le misure, il GDPR chiede di consultare il Garante prima di avviare il trattamento. Saltare questo passaggio quando serve è un errore che pesa.

Chi la fa, e quando rifarla

La DPIA non è un esercizio per specialisti chiusi in una stanza. La fa il titolare, con il contributo di chi conosce il trattamento, di chi gestisce la tecnologia e, dove c'è, del DPO, che il GDPR vuole sia consultato. Coinvolgere queste figure insieme è ciò che la rende utile: ognuna vede un rischio che le altre non vedono.

Un punto spesso dimenticato è che la DPIA non si fa una volta sola. Va rivista quando il trattamento cambia in modo rilevante: un nuovo strumento, una nuova finalità, più dati, un fornitore diverso, un cambio nel paese in cui i dati sono trattati. Un sistema AI che evolve in fretta, e quasi tutti lo fanno,

rende la revisione periodica una necessità, non un di più. Una DPIA ferma a due anni fa descrive un trattamento che forse non esiste più.

Una DPIA non è un modulo da riempire

L'errore più comune con la DPIA è trattarla come un modulo da compilare per mettersi a posto. Compilata così, in mezza giornata, senza coinvolgere chi conosce davvero il trattamento, non serve a niente: descrive un trattamento ideale che non corrisponde a quello reale, e non riduce nessun rischio. La sua utilità sta nel processo, non nel documento.

Fatta bene, la DPIA fa emergere cose scomode prima che diventino incidenti. Costringe a chiedersi se quel dato serve davvero, se la persona se lo aspetta, cosa succede nel caso peggiore. A volte il risultato è scoprire che il trattamento, così com'è pensato, non regge, e va ridisegnato. Non è un fallimento: è esattamente ciò per cui la DPIA esiste, fermare in tempo ciò che andrebbe a sbattere. Il documento è solo la traccia di quel ragionamento.

Quando consultare il Garante

C'è un esito della DPIA che molti preferiscono ignorare: se, dopo aver individuato tutte le misure ragionevoli, il rischio residuo per le persone resta elevato, il GDPR chiede di consultare l'autorità di controllo, in Italia il Garante per la protezione dei dati personali, prima di avviare il trattamento. Non è un fallimento, è una valvola di sicurezza per i casi più delicati.

Saltare questo passaggio quando ne ricorrono le condizioni, e partire comunque, è un errore che pesa, perché significa aver riconosciuto un rischio elevato e aver deciso di ignorarlo. Per i trattamenti AI più impegnativi, quelli che valutano molte persone o toccano dati sensibili su larga scala, mettere in conto anche questa possibilità fa parte di una pianificazione onesta. Meglio una domanda in più prima, che una giustificazione in meno dopo.

Proporzionalità: la domanda che pesa di più

Dentro la DPIA c'è una domanda che vale tutte le altre: questo trattamento è proporzionato allo scopo, o sto usando più dati e più capacità di calcolo di quanto serva? È la domanda che le organizzazioni saltano più volentieri, perché spesso la risposta onesta obbliga a ridimensionare un progetto su cui si è già investito entusiasmo.

Eppure è qui che la DPIA dà il meglio. Scoprire che lo stesso risultato si ottiene con meno dati, o con uno strumento meno invasivo, non è una rinuncia: è un trattamento migliore, più difendibile e spesso anche più semplice da gestire. La proporzionalità non è un freno all'ambizione, è la disciplina che tiene un progetto dentro i confini di ciò che è lecito e necessario.

> **In sintesi.** La DPIA non rallenta il progetto, lo mette al riparo: è il documento che mostra di aver valutato il rischio prima di partire. Per i trattamenti AI che profilano persone o toccano dati particolari su larga scala, è un obbligo, non una scelta.

Sicurezza del trattamento con l'AI

Trattare dati con l'AI in modo lecito non basta se poi quei dati non sono protetti. Il GDPR chiede misure tecniche e organizzative adeguate al rischio, e l'uso dell'AI introduce vie di fuga dei dati che i sistemi tradizionali non avevano.

Le tre vie di fuga tipiche

La prima è il contenuto stesso delle interazioni. Quello che scrivi a uno strumento resta da qualche parte: nelle cronologie, nei log, a volte nei dati di addestramento. Un dato delicato incollato in una chat può sopravvivere ben oltre il momento in cui ti serviva.

La seconda sono gli accessi. Chi può usare lo strumento? Con quali credenziali? Un account condiviso senza tracciabilità rende impossibile sapere chi ha fatto cosa, e questo da solo viola il principio di responsabilizzazione.

La terza è l'integrazione. Quando colleghi uno strumento AI ai tuoi sistemi, gli dai accesso a dati che vanno oltre la singola richiesta. Un collegamento configurato male è una porta aperta su molto più di quanto immagini.

Le misure che contano

- **Controllo degli accessi**: account nominali, permessi minimi, nessun account condiviso per trattamenti che contano.
- **Registrazione delle attività**: poter ricostruire chi ha trattato cosa e quando.
- **Limitazione dei dati conservati**: cancellare cronologie e dati che non servono più.
- **Separazione degli ambienti**: i dati reali non si danno in pasto a strumenti in prova.
- **Formazione di chi usa**: la misura di sicurezza più efficace è una persona che sa cosa non incollare.

Un esempio di data leakage

Per capire quanto sia concreto il rischio, un caso tipico. Un collaboratore incolla in uno strumento di AI un documento per farsi aiutare a riscriverlo. Il documento contiene, in fondo, una tabella con nomi e dati di clienti che lui non aveva notato. In quel gesto, quei dati sono usciti dall'organizzazione ed entrati in un sistema di terzi, forse conservati nelle cronologie, forse, a seconda del fornitore e delle impostazioni, utilizzabili per altri fini.

Nessun attacco, nessuna falla tecnica: solo una persona che non sapeva dove fosse il confine. È la ragione per cui le misure di sicurezza tecniche, da sole, non bastano. Servono impostazioni che limitino cosa viene conservato, ma serve soprattutto che chi usa lo strumento riconosca un dato sensibile prima di premere invio. La sicurezza, con l'AI, passa più dalle persone che dai firewall.

Le misure essenziali, in ordine di efficacia

Non tutte le misure di sicurezza rendono allo stesso modo. Vale la pena ordinarle per impatto reale, perché le risorse sono limitate e conviene partire da ciò che protegge di più.

MISURA	COSA PREVIENE	SFORZO
Formazione di chi usa	Il dato incollato per errore, la causa numero uno	Medio, continuo
Strumenti ammessi definiti	Lo shadow AI e i dati fuori controllo	Basso
Accessi nominali e permessi minimi	Usi impropri e perdita di tracciabilità	Medio
Limitare ciò che si conserva	La permanenza dei dati oltre il necessario	Basso
Separare prova e produzione	I dati reali in ambienti di test	Medio

Il dato interessante è che la misura più efficace, la formazione, non è tecnica. Si possono spendere risorse in protezioni sofisticate e lasciare scoperto il punto da cui i dati escono davvero: la persona che non sa dove sta il confine. La sicurezza dell'AI è un problema di tecnologia e di cultura, e la seconda parte pesa più di quanto si creda.

Quando i dati scappano: la violazione

Prima o poi qualcosa va storto, e bisogna essere pronti. Una violazione dei dati personali, un data breach, è qualsiasi evento che porta a perdita, accesso non autorizzato o divulgazione di dati. Con l'AI può assumere forme nuove: un dato incollato per errore in uno strumento pubblico, un account compromesso, un'integrazione mal configurata che espone più di quanto doveva.

Il GDPR impone reazioni rapide. Le violazioni che possono mettere a rischio i diritti delle persone vanno notificate all'autorità di controllo entro tempi stretti, e nei casi più gravi va informato anche chi ne è colpito. Tradotto in pratica, devi sapere in anticipo chi fa cosa quando succede: chi se ne accorge, a chi segnala, chi decide se notificare, in quali tempi. Improvvisare nel momento della crisi è il modo migliore per trasformare un incidente gestibile in un problema serio. Una procedura semplice, decisa a freddo, vale più di qualsiasi rassicurazione.

> **Attenzione.** La fuga di dati più comune con l'AI non è un attacco sofisticato: è qualcuno che incolla in uno strumento un dato che non doveva uscire. Nessuna misura tecnica regge se chi usa lo strumento non sa dove sta il confine.

Diritti degli interessati e decisioni automatizzate

Dietro ogni dato c'è una persona con dei diritti, e l'AI non li sospende. Le persone possono chiedere di accedere ai propri dati, di correggerli, di cancellarli, di opporsi a certi trattamenti. Quando questi dati passano da sistemi di AI, rispondere a queste richieste richiede di aver progettato i sistemi per poterlo fare.

Il diritto a non subire decisioni solo automatiche

Il GDPR riconosce un diritto specifico che con l'AI diventa centrale: la persona ha diritto, salvo eccezioni, a non essere sottoposta a una decisione basata unicamente su un trattamento automatizzato che produca effetti giuridici o incida in modo rilevante su di lei. Tradotto: se un'AI decide da sola se assumere qualcuno, concedere un credito, erogare un servizio, e quella decisione conta, l'interessato ha diritto a un intervento umano, a esprimere la propria posizione, a contestare.

Il punto delicato è la parola "unicamente". Mettere una persona a fare da timbro su decisioni già prese dalla macchina non basta: il controllo umano deve essere reale, con la possibilità e la competenza di ribaltare l'esito. Un'approvazione automatica travestita da revisione umana non soddisfa il diritto, lo aggira.

Rispondere alle richieste in pratica

Se una persona chiede quali suoi dati tratti con l'AI, devi poterlo dire. Se chiede di cancellarli, devi poterlo fare, anche dove sono finiti dentro strumenti di terzi. Questo significa che la capacità di rispondere ai diritti va pensata quando progetti l'uso dell'AI, non improvvisata quando arriva la richiesta. Un sistema da cui non puoi estrarre o cancellare i dati di una persona è un sistema che ti mette in difficoltà per costruzione.

Quando la decisione conta: credito e lavoro

Due ambiti rendono il tema palpabile. Nel credito, un sistema che valuta automaticamente se concedere un finanziamento prende una decisione con effetti rilevanti sulla vita di una persona: rientra in pieno nelle tutele rafforzate, con diritto a spiegazione, a intervento umano, a contestazione. Nel lavoro, un sistema che seleziona o valuta dipendenti tocca diritti e aspettative legittime, e va trattato con la stessa cura.

In entrambi i casi la tentazione è la stessa: lasciare decidere la macchina perché è più veloce e sembra più oggettiva. Ma la velocità non vale la rinuncia ai diritti, e l'oggettività apparente di un sistema può nascondere errori sistematici che colpiscono sempre lo stesso tipo di persone. Il controllo umano reale, qui, non è un freno all'efficienza: è la garanzia che una decisione importante resti contestabile da chi la subisce.

Spiegabilità: cosa devi poter dire

Quando una decisione automatizzata incide su una persona, questa ha diritto a una spiegazione comprensibile della logica seguita. Non significa consegnarle il codice del modello o i suoi parametri interni, cosa che non capirebbe nessuno. Significa poter dire, in parole chiare, quali fattori contano e in che modo si è arrivati a quell'esito.

Questo ha una conseguenza nella scelta degli strumenti. Un sistema così opaco che nemmeno chi lo usa sa spiegare perché ha deciso in un certo modo mette l'organizzazione in difficoltà strutturale: non potrà mai onorare il diritto alla spiegazione. Per le decisioni che contano sulle persone, la capacità di spiegare non è un di più tecnico, è un requisito. Uno strumento che non la consente, su quei trattamenti, è uno strumento sbagliato a prescindere da quanto sia bravo.

Conservazione e cancellazione dei dati

I dati personali non si conservano per sempre. Vanno tenuti per il tempo necessario alla finalità, poi cancellati o resi anonimi. Con l'AI questo principio incontra un ostacolo pratico: i dati hanno la tendenza a depositarsi in posti da cui è difficile toglierli.

Le chat con uno strumento conservano cronologie. I log registrano le interazioni. I sistemi collegati copiano i dati in più punti. E la domanda più scomoda riguarda l'addestramento: se i tuoi dati sono stati usati per addestrare un modello, cancellarli dal modello è tecnicamente complesso, a volte impossibile. È un altro motivo per cui sapere in anticipo se un fornitore usa i dati per addestrare è una verifica che precede l'adozione, non la segue.

Cosa decidere a monte

- **Per quanto tempo** conservare i dati di ogni uso dell'AI, finalità per finalità.
- **Dove si depositano** i dati lungo il percorso: chat, log, sistemi collegati, fornitore.
- **Come si cancellano** davvero, non solo dalla vista, ma da tutti i punti in cui sono finiti.
- **Cosa succede alla fine del rapporto** con il fornitore: restituzione e cancellazione dei dati.

Definire questi punti prima di partire costa qualche ora. Scoprirli dopo, quando un interessato chiede la cancellazione e i dati sono sparsi in sei sistemi diversi, costa molto di più, e a volte costa la fiducia.

Il nodo dell'addestramento

C'è una domanda che vale la pena isolare, perché è quella che crea i problemi più difficili da risolvere a posteriori: i dati che do a uno strumento finiscono nell'addestramento dei suoi modelli? Se la risposta è sì, quei dati non sono più solo "conservati": diventano parte di qualcosa da cui estrarli o cancellarli è tecnicamente arduo, a volte impraticabile.

Questo capovolge l'ordine delle verifiche. La domanda sull'addestramento non va fatta quando un interessato chiede la cancellazione, ma prima di adottare lo strumento, perché è una di quelle scelte che, una volta prese, non si disfano facilmente. Molti fornitori seri permettono di escludere l'uso dei dati per addestramento, spesso è un'impostazione da attivare. Verificarla e attivarla è uno dei gesti che separano un uso governato da uno che si scopre ingovernabile quando è troppo tardi.

I dati che restano nelle chat

Un punto concreto che sfugge a molti: le conversazioni con gli strumenti di AI non spariscono quando chiudi la finestra. Restano nelle cronologie, a volte per impostazione predefinita, consultabili da chi ha accesso a quell'account, talvolta utilizzate dal fornitore. Una richiesta scritta in fretta a mezzogiorno, con dentro il nome e il problema di un cliente, può sopravvivere per mesi in un posto che non controlli.

Le contromisure ci sono, ma vanno attivate: impostazioni che limitano la conservazione, pulizia periodica delle cronologie, scelta di strumenti che permettono di non conservare nulla. La prima difesa, però, resta non mettere nelle chat ciò che non deve restarci. Trattare ogni messaggio a uno strumento AI come se fosse permanente è un'abitudine prudente che evita gran parte dei problemi di conservazione a monte, invece che rincorrerli a valle.

Cancellare davvero, non solo dalla vista

Cancellare un dato sembra banale finché non lo si deve fare sul serio. Con l'AI, lo stesso dato può trovarsi in più posti contemporaneamente: la conversazione, i log, un sistema collegato che ne ha tenuto copia, l'archivio del fornitore. Toglierlo da uno solo di questi punti dà l'illusione di averlo cancellato, mentre altrove sopravvive.

Per onorare davvero una richiesta di cancellazione, devi sapere in anticipo dove il dato si deposita lungo tutto il suo percorso. È un'altra ragione per mappare i flussi prima di partire: la capacità di cancellare non si improvvisa quando arriva la richiesta, si costruisce quando si progetta l'uso dello strumento. Un dato che non sai dove sia è un dato che non potrai mai garantire di aver eliminato.

> **In sintesi.** Conservare significa anche saper cancellare. Mappa dove finiscono i dati lungo l'uso dell'AI, fissa tempi di conservazione per ogni finalità e verifica prima dell'adozione se il fornitore usa i dati per addestrare, perché da lì tornare indietro è difficile.

PARTE IV

Metodo e avvio

Dalla teoria alla pratica: gli strumenti organizzativi che rendono governabile l'uso dell'AI, gli errori da evitare e un piano concreto per i primi mesi.

Un registro degli usi dell'AI che trattano dati

Non puoi proteggere quello che non sai di avere. La prima mossa concreta, prima di policy e valutazioni, è sapere dove l'AI tratta dati personali nella tua organizzazione. Quasi sempre la realtà supera le aspettative: gli usi sono più di quelli che il vertice immagina, perché nascono dal basso, da chi cerca di lavorare meglio.

Il registro degli usi dell'AI è un elenco vivo che risponde a domande semplici per ogni uso: chi lo fa, con quale strumento, su quali dati, per quale finalità, su quale base giuridica, con quale fornitore. Non è il registro dei trattamenti del GDPR, ma lo alimenta e spesso ne fa parte.

Cosa annotare

```
REGISTRO USI AI - voce tipo

Uso:            Smistamento richieste clienti
Ufficio:        Assistenza
Strumento:      [nome] - versione/piano
Dati trattati:  Nome, contatto, contenuto richiesta
Categorie:      Dati comuni (no dati particolari)
Finalità:       Indirizzare la richiesta all'ufficio giusto
Base giuridica: Legittimo interesse (test eseguito)
Fornitore:      [nome] - responsabile, contratto del [data]
Dati fuori UE:  No / Si + garanzia adottata
Conservazione:  [periodo] poi cancellazione
DPIA:           Necessaria? Si/No - se si, riferimento
Controllo:      Revisione umana sui casi dubbi
Responsabile:   [nome ruolo]
```

Compilare la prima voce richiede mezz'ora e fa emergere subito i buchi: l'uso senza base giuridica, lo strumento senza contratto, il dato che esce dall'Unione senza che nessuno lo sapesse. Il registro non è burocrazia: è la mappa senza la quale ogni altra decisione si prende al buio.

Come tenerlo aggiornato

Un registro fotografato una volta e dimenticato invecchia in fretta, perché gli usi dell'AI cambiano ogni mese. Conviene legarne l'aggiornamento a un momento fisso, ad esempio una revisione trimestrale, e a una regola: nessun nuovo strumento AI su dati personali senza una voce nel registro. Così la mappa resta fedele al territorio.

Far emergere gli usi nascosti

Compilare il registro ha un effetto collaterale prezioso: porta alla luce usi dell'AI che il vertice ignorava. Quasi sempre, chiedendo in giro con onestà e senza spirito punitivo, emergono strumenti adottati dai singoli per lavorare meglio, dati passati a servizi mai valutati, scorciatoie nate dalla buona volontà. Non sono sabotaggi: sono il segnale che le persone hanno bisogni che gli strumenti ufficiali non coprono.

Per questo il censimento iniziale conviene farlo in modo collaborativo, spiegando che lo scopo è mettere in sicurezza, non sanzionare. Una persona che teme una punizione nasconde; una persona che capisce il senso aiuta a mappare. Il registro più completo non nasce da un'ispezione, ma da una conversazione franca con chi l'AI la usa davvero, ogni giorno.

Dal registro alle priorità

Una volta compilato, il registro non è un archivio da chiudere: è uno strumento per decidere dove intervenire prima. Scorrendolo, alcuni usi salteranno all'occhio come più urgenti: quelli che trattano dati particolari, quelli che mandano dati fuori dall'Unione, quelli senza base giuridica chiara, quelli da cui derivano decisioni sulle persone. Sono questi a meritare attenzione immediata.

Il registro, in altre parole, trasforma un'ansia generica ("non so se siamo a posto con l'AI") in una lista di azioni concrete e ordinate. È la differenza tra sentirsi sopraffatti e sapere esattamente da dove cominciare lunedì. Una mappa non riduce il territorio, ma permette di attraversarlo senza perdersi, e di affrontare prima i tratti più pericolosi.

Chi tiene il registro, e perché conta

Un registro senza un responsabile diventa un file dimenticato. Conviene assegnarne la cura a una persona o a una funzione precisa, che lo aggiorna, lo confronta con la realtà e segnala quando qualcosa non torna. Dove c'è un DPO, è il candidato naturale a sovrintendere, anche se l'alimentazione concreta spetta a chi gli usi li fa.

Il valore di avere un responsabile non è formale. È la differenza tra un documento che riflette quello che succede davvero e uno che descrive una situazione di due anni fa. In un campo che cambia ogni mese, qualcuno deve avere il compito esplicito di tenere la mappa fedele al territorio, altrimenti la

mappa, lentamente, mente.

> **In sintesi.** Prima di governare l'AI devi vederla. Un registro degli usi che trattano dati, aggiornato con regolarità, fa emergere gli usi nascosti e i buchi di conformità, e diventa la base per ogni decisione successiva.

Una policy privacy-by-design per l'AI

La privacy-by-design è il principio per cui la protezione dei dati si costruisce dentro i processi, non si aggiunge dopo. Tradotto sull'AI, significa una policy che dica al personale cosa può fare e cosa no, prima che lo decida da solo nel momento sbagliato. Una buona policy non è un documento legale illeggibile: è un insieme di regole chiare che chi lavora capisce e applica.

Cosa deve dire una policy utile

```
POLICY USO AI E DATI PERSONALI - struttura

1. STRUMENTI AMMESSI
   - Elenco degli strumenti approvati
   - Per ciascuno: quali dati sono ammessi
   - Strumenti vietati per dati personali

2. REGOLE SUI DATI
   - Mai dati particolari in strumenti generici
   - Minimizzare: solo i dati necessari
   - Verificare l'output che riguarda persone

3. PRIMA DI USARE UN NUOVO STRUMENTO
   - Chi autorizza
   - Verifica contratto e dove tratta i dati
   - Voce nel registro usi AI

4. COSA FARE IN CASO DI ERRORE
   - A chi segnalare un dato uscito per sbaglio
   - Tempi e modalità di segnalazione

5. FORMAZIONE E RESPONSABILITÀ
   - Chi ha letto e accettato la policy
   - Riferimento per le domande (DPO)
```

Il valore di una policy non sta nella sua esistenza, ma nel fatto che le persone la conoscano e la usino. Una policy perfetta che nessuno ha letto protegge meno di tre regole semplici appese accanto allo schermo. Per questo la formazione non è un capitolo a parte: è ciò che fa vivere la policy.

Le tre regole che valgono più di dieci pagine

Se una policy completa rischia di restare nel cassetto, tre regole semplici, ripetute finché entrano nelle abitudini, proteggono più di un manuale. Mai dati particolari, come salute o dati di minori, dentro strumenti generici. Mai uno strumento non autorizzato per dati personali di lavoro. Sempre un controllo umano sull'output che riguarda una persona, prima di usarlo.

Queste tre frasi coprono la maggior parte degli incidenti reali. Sono facili da ricordare, si applicano in un secondo, e non richiedono di consultare un documento mentre si lavora sotto scadenza. La policy estesa resta, perché serve a dimostrare il metodo, ma sono le tre regole appese accanto allo schermo che evitano il guaio nel momento in cui sta per accadere.

Chi decide e chi applica

Una policy vive solo se è chiaro chi fa cosa. Servono pochi ruoli definiti: chi autorizza un nuovo strumento, chi tiene il registro, chi forma il personale, chi si occupa di un incidente. Non servono organigrammi complessi, serve che, davanti a una domanda concreta, sia ovvio a chi rivolgerla. L'ambiguità sui ruoli è ciò che fa cadere le buone intenzioni nel vuoto.

Nelle piccole organizzazioni questi ruoli possono concentrarsi in poche persone, e va bene: l'importante è che siano assegnati, non sparsi. "Lo fa qualcuno" è il modo più sicuro perché non lo faccia nessuno. Scrivere accanto a ogni regola il nome del responsabile trasforma una policy da dichiarazione di principio a strumento che funziona davvero quando arriva il momento di usarlo.

> **In sintesi.** Privacy-by-design sull'AI significa decidere a monte quali strumenti e quali dati sono ammessi, e metterlo in una policy che il personale capisce. Una regola chiara conosciuta da tutti vale più di un documento perfetto che nessuno legge.

Il ruolo del DPO e la formazione del personale

Dove esiste un responsabile della protezione dei dati, il DPO, l'introduzione dell'AI lo riguarda da vicino. Non perché debba bloccare, ma perché è la figura che sorveglia, consiglia e fa da punto di contatto. Coinvolgerlo dopo aver scelto lo strumento è un errore frequente: il suo apporto serve quando le scelte si possono ancora orientare, non quando sono fatte.

Il DPO aiuta a inquadrare la base giuridica, a decidere se serve una DPIA, a valutare i contratti con i fornitori, a tenere il registro. In molte organizzazioni che adottano l'AI in fretta, il DPO scopre gli usi a cose fatte: è esattamente la situazione che genera i rischi maggiori.

La formazione non è un optional

L'AI Act, all'articolo 4, introduce un obbligo che molti sottovalutano: chi sviluppa o usa sistemi di AI deve garantire un livello adeguato di competenza al proprio personale. Per la protezione dei dati questo si salda con una verità operativa: la misura di sicurezza più efficace è una persona che sa riconoscere un dato che non deve uscire.

La formazione utile non è una lezione teorica una tantum. È mostrare casi concreti, far vedere cosa succede quando un dato esce, dare regole che si applicano lunedì mattina. La formazione AI per aziende e PA di AIPIA è pensata per questo: tracciabile, orientata alla pratica, con rilascio di credenziali europee verificabili. Chi vuole partire dai fondamenti individuali trova nel Corso Base e nel Corso Advanced due livelli con la European AI Professional Credential firmata eIDAS.

La formazione che funziona davvero

Una formazione utile sull'AI e i dati non somiglia a una lezione di diritto. Parte dai gesti reali del lavoro: questo dato posso incollarlo qui? Questo strumento è ammesso per questa informazione? Chi avviso se è uscito qualcosa per sbaglio? Mostra casi concreti, fa vedere cosa è andato storto altrove e perché, e lascia regole che si applicano il giorno dopo.

Conta anche la tracciabilità. L'obbligo di competenza dell'AI Act non si soddisfa affermando di aver formato il personale: si dimostra. Una formazione documentata, con il riscontro di chi ha partecipato e cosa ha appreso, è anche la prova che assolvi quell'obbligo. Per questo la formazione tracciabile non è un dettaglio organizzativo: è parte della conformità, oltre che della sicurezza.

Il DPO nella pubblica amministrazione

Nella pubblica amministrazione il DPO è una figura obbligatoria, e l'introduzione dell'AI ne mette alla prova il ruolo. Gli enti pubblici trattano dati dei cittadini che non possono scegliere un altro fornitore del servizio, e questo alza l'asticella: la proporzionalità va dimostrata con cura, la trasparenza deve essere reale, e l'uso dell'AI non può ridursi a una scorciatoia per fare prima a scapito dei diritti.

Coinvolgere il DPO fin dalla scelta dello strumento, e non a valle, è ancora più importante nel pubblico, dove un uso mal impostato non danneggia un cliente che può andarsene, ma un cittadino che dipende da quel servizio. La formazione del personale, qui, ha lo stesso peso: un dirigente pubblico che introduce l'AI senza che chi la usa sappia maneggiare i dati espone l'ente e le persone che dovrebbe servire.

> **In sintesi.** Coinvolgi il DPO quando le scelte si possono ancora orientare, non dopo. E tratta la formazione come una misura di sicurezza, non come un adempimento: una persona competente previene più incidenti di qualsiasi regola scritta.

Gli errori tipici e come correggerli

Chi introduce l'AI senza metodo cade quasi sempre negli stessi errori. Conoscerli in anticipo vale più di molte pagine di teoria, perché sono prevedibili e quasi tutti evitabili con una correzione semplice.

ERRORE TIPICO	PERCHÉ È UN PROBLEMA	CORREZIONE
Pensare alla privacy alla fine	Le scelte che contano si fanno all'inizio	Valutare base giuridica e fornitore prima di partire
"Ho tolto il nome, è anonimo"	Spesso resta identificabile: è ancora dato personale	Verificare la re-identificabilità, non solo il nome
Consenso usato per tutto	Con i dipendenti non è libero, quindi non valido	Scegliere la base corretta caso per caso
Strumenti personali sui dati di lavoro	Nessun contratto, dati fuori controllo	Elenco di strumenti ammessi nella policy
Nessun contratto col fornitore	Trasferimento di dati scoperto	Accordo sul trattamento prima dell'uso
Output AI usato senza verifica	Dati inesatti diventano un tuo trattamento	Controllo umano sull'output che riguarda persone
Dati fuori UE senza saperlo	Trasferimento illecito verso paesi terzi	Verificare dove il fornitore tratta i dati

Il filo che lega quasi tutti questi errori è uno: la fretta. La voglia di vedere subito un risultato spinge a saltare i controlli iniziali, che sono proprio quelli che evitano i guai. Chi rallenta all'inizio va più veloce dopo, perché non deve tornare indietro a smontare quello che ha costruito male.

Il denominatore comune degli errori

Guardando la tabella nel suo insieme, emerge uno schema. Quasi nessuno di questi errori nasce da cattiva fede: nascono dal voler andare veloci e dal non sapere che un certo passaggio andava fatto. Sono errori di metodo, non di volontà, e questa è una buona notizia, perché gli errori di metodo si correggono con il metodo.

La correzione, in tutti i casi, ha la stessa forma: spostare i controlli all'inizio. Decidere la base prima di trattare, scegliere lo strumento prima di incollare, firmare il contratto prima di passare i dati, verificare dove finiscono i dati prima di adottare. Non è prudenza eccessiva: è l'ordine giusto delle operazioni. Fare le cose nell'ordine sbagliato è il vero errore di fondo, da cui discendono tutti gli altri.

L'errore che costa di più

Tra tutti gli errori, uno merita un posto a parte perché è il più costoso e il più frequente: usare strumenti personali e gratuiti sui dati di lavoro. Nasce sempre bene, qualcuno vuole fare prima, ma le conseguenze si accumulano. Nessun contratto con il fornitore, quindi un trasferimento di dati scoperto. Nessun controllo su dove finiscono i dati. Spesso l'uso di quei dati per addestrare modelli altrui. E nessuna tracciabilità di chi ha fatto cosa.

La correzione non è un divieto urlato, che spinge l'uso nell'ombra, ma un'alternativa migliore: strumenti aziendali ammessi, comodi almeno quanto quelli personali, con i contratti a posto. Quando usare lo strumento giusto è più facile che usare quello sbagliato, il problema si risolve quasi da solo. Le persone scelgono la via comoda: il lavoro di chi governa è fare in modo che la via comoda sia anche quella sicura.

Fidarsi delle impostazioni predefinite

Un errore meno ovvio degli altri merita una nota: dare per buone le impostazioni predefinite di uno strumento. I valori preimpostati sono spesso pensati per la comodità del fornitore o per la massima funzionalità, non per la protezione dei tuoi dati. La conservazione delle cronologie attiva, l'uso dei dati per migliorare il servizio, il trattamento fuori dall'Unione: a volte sono il comportamento di partenza, da disattivare di proposito.

Adottare uno strumento senza guardarne le impostazioni significa accettare scelte fatte da altri sui propri dati. Mezz'ora dedicata a rivedere le opzioni, prima di mettere lo strumento al lavoro su dati reali, evita la sorpresa di scoprire mesi dopo che i dati seguivano una strada che nessuno aveva scelto. Il default non è una decisione neutra: è una decisione presa da qualcun altro al posto tuo.

Cosa chiedere a un fornitore prima di firmare

La scelta del fornitore decide gran parte della conformità, perché molte tutele dipendono da cosa il fornitore fa con i dati. Arrivare alla firma con le domande giuste è il modo più economico per evitare problemi che dopo si pagano cari. Ecco la lista di controllo da tenere a portata.

- **Dove trattate i miei dati?** Dentro o fuori dall'Unione Europea, e con quale meccanismo per i trasferimenti.
- **Usate i miei dati per addestrare i vostri modelli?** Se sì, con quali limiti e come posso escluderlo.
- **Firmate un accordo sul trattamento dei dati** come responsabili, con le clausole richieste dal GDPR?
- **Quali sub-fornitori** usate, e dove si trovano?
- **Quali misure di sicurezza** applicate, e come le posso verificare?
- **Quanto conservate i dati** e come li cancellate alla fine del rapporto?
- **Come mi aiutate a rispondere** alle richieste degli interessati, comprese cancellazioni?

- **Cosa succede in caso di violazione dei dati**: tempi e modalità di notifica.

Se un fornitore evita le risposte, dà risposte vaghe o rimanda a condizioni generali che dicono il contrario di quanto promette a voce, è già un'informazione. La chiarezza su questi punti prima della firma è il primo indice di affidabilità.

Leggere le risposte, non solo riceverle

Le domande della checklist contano per le risposte che generano, ma anche per come vengono date. Un fornitore affidabile risponde in modo preciso, mette per iscritto quello che afferma a voce, e non si irrita davanti alle verifiche. Un fornitore che minimizza, che rimanda a condizioni generali contraddittorie, o che tratta le tue domande come un fastidio, ti sta già dicendo come si comporterà quando avrai un problema.

Vale la pena, prima di firmare, confrontare ciò che è stato promesso a voce con ciò che è scritto nel contratto e nelle condizioni. È lì, nella lettera dell'accordo, che vivono gli obblighi reali. Le rassicurazioni che non finiscono nero su bianco hanno il valore della carta su cui non sono scritte.

I segnali di un fornitore da evitare

Alcuni comportamenti, in fase di trattativa, valgono più di mille promesse. Diffida del fornitore che non sa dirti dove tratta i dati, o che risponde in modo vago e cambia versione. Diffida di chi presenta come "standard" condizioni che permettono usi ampi dei tuoi dati, addestramento incluso, sepolti in clausole che speri di non leggere. Diffida di chi tratta le tue domande di conformità come un ostacolo commerciale invece che come una richiesta legittima.

Al contrario, un fornitore che mette per iscritto quello che afferma, che offre opzioni di trattamento europeo, che ti dà gli strumenti per rispondere alle richieste degli interessati, ti sta mostrando con i fatti come si comporterà. Se internamente le competenze non bastano, la directory dei professionisti AI di AIPIA aiuta a trovare chi sa leggere questi contratti. La scelta del fornitore è una delle poche decisioni che, fatta bene all'inizio, ti risparmia decine di problemi dopo. Vale la pena spenderci il tempo che merita, prima della firma, non dopo il primo incidente.

Un piano per i primi 90 giorni

Mettere ordine nell'uso dell'AI rispetto alla privacy sembra un cantiere enorme. Diviso in tre mesi, con priorità chiare, diventa gestibile. Questo piano parte dal vedere e arriva al governare, nell'ordine che riduce prima i rischi maggiori.

```
PRIMI 90 GIORNI - AI e protezione dati

GIORNI 1-30 - VEDERE
  - Censire gli usi dell'AI che trattano dati
  - Compilare il registro usi AI
  - Individuare gli usi più rischiosi (dati particolari,
    decisioni automatizzate, dati fuori UE)
  - Fermare gli usi chiaramente illeciti

GIORNI 31-60 - METTERE IN REGOLA
  - Base giuridica per ogni uso che resta
  - Contratti coi fornitori (accordo sul trattamento)
  - Verificare dove finiscono i dati (UE / extra-UE)
  - DPIA dove serve
  - Aggiornare le informative

GIORNI 61-90 - GOVERNARE
  - Pubblicare la policy uso AI
  - Formare il personale (obbligo art. 4 AI Act)
  - Definire conservazione e cancellazione
  - Fissare la revisione trimestrale del registro
  - Coinvolgere il DPO nel processo stabile
```

Il piano non chiede di fare tutto e subito: chiede di partire dai rischi più alti e procedere con ordine. Trenta giorni per vedere, trenta per mettere in regola ciò che conta, trenta per costruire il metodo che tiene. Alla fine non avrai eliminato ogni rischio, nessuno può, ma avrai un uso dell'AI difendibile e una macchina che si mantiene.

Partire dai rischi, non dalla perfezione

La tentazione, davanti a un piano, è volerlo completare tutto perfettamente prima di sentirsi a posto. È la strada per non partire mai. La logica dei novanta giorni è opposta: si comincia da ciò che riduce subito il rischio maggiore, gli usi chiaramente illeciti e i dati particolari fuori controllo, e si procede per priorità decrescente.

Alla fine del primo ciclo non avrai un sistema perfetto, e va bene così: avrai un uso dell'AI difendibile, una mappa aggiornata e un metodo che si mantiene da solo con la revisione periodica. La conformità non è uno stato che si raggiunge una volta, è una pratica che si tiene. Chi la imposta come pratica smette di rincorrere e comincia a governare.

Dopo i primi novanta giorni

Chiuso il primo ciclo, il lavoro non finisce, cambia natura. Da progetto diventa abitudine. La revisione trimestrale del registro tiene la mappa aggiornata, l'arrivo di ogni nuovo strumento passa per le stesse domande, la formazione si ripete per chi entra e si aggiorna per chi resta. Non è un peso aggiuntivo: è il ritmo normale di un'organizzazione che ha smesso di subire l'AI e ha cominciato a guidarla.

Il segnale che il metodo ha attecchito è semplice: quando qualcuno propone un nuovo uso dell'AI, le domande sulla base giuridica, sul fornitore, sui dati, vengono prima e in modo naturale, non dopo e per imposizione. A quel punto la protezione dei dati non è più un ufficio che dice di no, ma un modo di lavorare che fa parte di come si fanno le cose. È lì che conformità e operatività smettono di essere in conflitto.

> **In sintesi.** Non serve un progetto monumentale: servono tre mesi con priorità chiare. Prima vedere dove l'AI tratta dati, poi mettere in regola gli usi che restano, infine costruire policy, formazione e revisione periodica che reggano nel tempo.

Il punto fermo: l'AI non aggira il GDPR

Gira, nelle organizzazioni che adottano l'AI in fretta, una convinzione tacita: che la velocità e l'utilità di questi strumenti giustifichino qualche scorciatoia sulla protezione dei dati, che le regole valgano "un po' meno" quando di mezzo c'è l'innovazione. È una convinzione comoda e sbagliata.

Il GDPR non fa eccezioni per gli strumenti nuovi. Un dato personale trattato male da un'AI resta un dato personale trattato male, con le stesse conseguenze di sempre, anzi spesso amplificate dalla quantità e dalla dispersione che l'AI introduce. Le organizzazioni che lo hanno capito non vanno più piano delle altre: vanno più sicure, perché non costruiscono su fondamenta che dovranno demolire.

C'è una simmetria utile da tenere a mente. Le stesse domande che rendono lecito un uso dell'AI, quali dati servono davvero, su quale base, con chi, per quanto tempo, sono anche le domande che lo rendono solido sul piano operativo. Conformità e qualità, qui, tirano nella stessa direzione.

L'intelligenza artificiale è uno strumento, e come ogni strumento si giudica da come lo si usa. Chi la introduce trattando le persone i cui dati maneggia come titolari di diritti, e non come righe di un foglio, non sta rinunciando a niente: sta costruendo l'unico tipo di uso dell'AI che dura. Le scorciatoie sulla privacy non fanno arrivare prima, fanno solo arrivare in un posto da cui poi bisogna tornare indietro.

Vale la pena dirlo senza giri di parole, perché è il cuore del discorso: nessuna utilità dell'AI compensa la perdita di fiducia che deriva dal trattare male i dati delle persone. La fiducia si costruisce lentamente e si perde in un attimo, e un'organizzazione che la brucia per guadagnare qualche

settimana scopre presto di aver fatto un pessimo affare. Chi vuole restare aggiornato su questi temi e accedere ai materiali può associarsi ad AIPIA.

AIPIA
ASSOCIAZIONE ITALIANA PROFESSIONISTI DELL'INTELLIGENZA ARTIFICIALE

Continua con AIPIA

Sei un professionista, un'azienda o un ricercatore che lavora con l'intelligenza artificiale? Ecco cosa mette a disposizione la prima associazione italiana dei professionisti AI.

Diventa socio — €24/anno

Contributo associativo annuale. Accesso alla Credenziale Europea, alla directory pubblica, alla tessera socio e alle convenzioni.

Iscriviti ora →

Formazione con credenziale

Corso Base (€249) e Corso Advanced (€399) con rilascio della European AI Professional Credential firmata eIDAS.

Scopri i percorsi →

Libri AIPIA

I volumi dell'associazione sull'intelligenza artificiale, dalla pratica all'etica.

Vai al catalogo →

RC Professionale AI

Polizza di Responsabilità Civile professionale dedicata a chi lavora con l'AI, riservata ai soci.

Scopri la copertura →

CONTATTI

Via Ostiense, 92 — 00154 Roma
Tel / WhatsApp: +39 06 56547987
Email: segreteria@aipia.it
PEC: aipia@altapec.it
CF: 96628540583 · aipia.it

SEGUICI

LinkedIn · Instagram · Facebook · X · YouTube · TikTok · Pinterest · Bluesky