# NOTIZIARIO PRIVACY 2025



→ AI innovare senza perdere il controllo

EURISTICA

NOTIZIARIO PRIVACY EURISTICA
Novembre 2026

*Fonte articoli*
**Federprivacy** | federprivacy.org
**Garante Privacy** | garanteprivacy.it
**Rödl** | roedl.it

*Layout*
**Euristica**

*Crediti fotografici*
**Freepik**

Euristica è iscritta a Federprivacy dal 2018

# INDICE

**SMS promozionali**
Richiesta di cancellazione valida anche se inviata a una email aziendale diversa da quella indicata nell'informativa privacy ..... pag 5

**IA e lavoro**
Il Garante Privacy avverte una start-up italiana. Sotto la lente dell'Autorità il plug-in che può rilevare linguaggio, emozioni e livello di stress dei dipendenti ..... pag 7

**Telemarketing aggressivo**
Agcom ha bloccato 191 milioni di chiamate nei primi 8 mesi del 2026 ..... pag 8

**Piano ispettivo privacy 2026**
Il valore del monitoraggio del DPO ..... pag 10

**Deepfake, cosa ha fatto il Garante**
Dalla fattispecie di reato introdotta dalla Legge 132/2025 ai recenti interventi del Garante: rischi, responsabilità e limiti ..... pag 13

**I dati aziendali nell'era dell'AI**
Tra opportunità, privacy e sicurezza: cosa devono sapere oggi le imprese ..... pag 16

**5 accorgimenti per proteggere i dati aziendali** ..... pag 19

**La vera sfida è innovare senza perdere il controllo** ..... pag 20

EURISTICA

# NEXT STEP




Se usi Excel, procedure manuali o un gestionale che non si è evoluto con la tua azienda, **stai pagando ogni giorno il costo dell'inefficienza.**

## È IL MOMENTO DI CAMBIARE

**Next Step è attivo fino al 31/12/2026**

Euristica analizza, progetta e realizza l'evoluzione del sistema gestionale della tua azienda: **dal modo in cui lavori oggi a un sistema integrato, efficiente e pronto per il futuro.**

## TI RICONOSCI IN QUESTI SEGNALI?

- Utilizzi Excel paralleli per gestire informazioni e processi
- Inserisci gli stessi dati più volte
- Prepari report manualmente
- Fai fatica a trovare o incrociare i dati che ti servono
- I tuoi sistemi non comunicano tra loro
- Hai procedure che funzionano solo perché qualcuno "sa come si fa"
- Dipendi da ticket, assistenza o attese per modificare il gestionale
- Il tuo gestionale non evolve più insieme alla tua azienda
- Sai che ci sono inefficienze, ma non sai quanto ti costano

## SE TI RICONOSCI, FORSE NON HAI SOLO UN PROBLEMA DI SOFTWARE.

**Hai un sistema di gestione che non è più adeguato alla tua azienda.**

## "Cambiare gestionale? Adesso? Impossibile."

- *E i dati? Quanto costerà? Quanto tempo servirà?*
- *E la formazione? E se qualcosa non funziona?*
- *Possiamo permetterci di fermare l'azienda?*

La paura di cambiare spesso è il motivo per cui si continua a lavorare come prima, ma anche non cambiare ha un costo.

***IL CAMBIAMENTO NON DEVE ESSERE UN SALTO NEL BUIO, MA UN PROGETTO***

## NEXT STEP È IL PRIMO PASSO

***Richiedi il check-up gestionale***

Un primo confronto di 45–60 minuti per capire come lavori oggi, dove si concentrano le inefficienze e quali possibilità di evoluzione esistono.

## EURISTICA PROPONE

- **6 PROGETTI** GESTIONALI
- FINO AL **31/12/2026**
- A **CONDIZIONI AGEVOLATE**

**EURISTICA S.R.L.**
P.IVA 02432270540

Via Brunelleschi, snc
06024 Gubbio | PG

+39 075 922 1401
euristica.com

info@euristica.com
commerciale@euristica.com

# SMS PROMOZIONALI

## Richiesta di cancellazione valida anche se inviata a una email aziendale diversa da quella indicata nell'informativa privacy




Gli sms promozionali devono dare la possibilità all'utente di poter cancellare facilmente gli invii indesiderati.  Sono tenuti, pertanto, a indicare un recapito idoneo che consenta ai destinatari di esercitare facilmente i propri diritti.

Le aziende devono garantire che tali richieste siano gestite correttamente, anche quando vengono inviate a un indirizzo email aziendale diverso da quello posto nell'informativa privacy.
È quanto ribadito dal Garante della Privacy

che, con provvedimento n. 644 del 23 settembre 2026, ha inflitto una sanzione di 5mila euro a Barbuti Spa, società di abbigliamento maschile, per non aver dato seguito a una richiesta di cancellazione dei dati e aver continuato a inviare sms promozionali indesiderati.

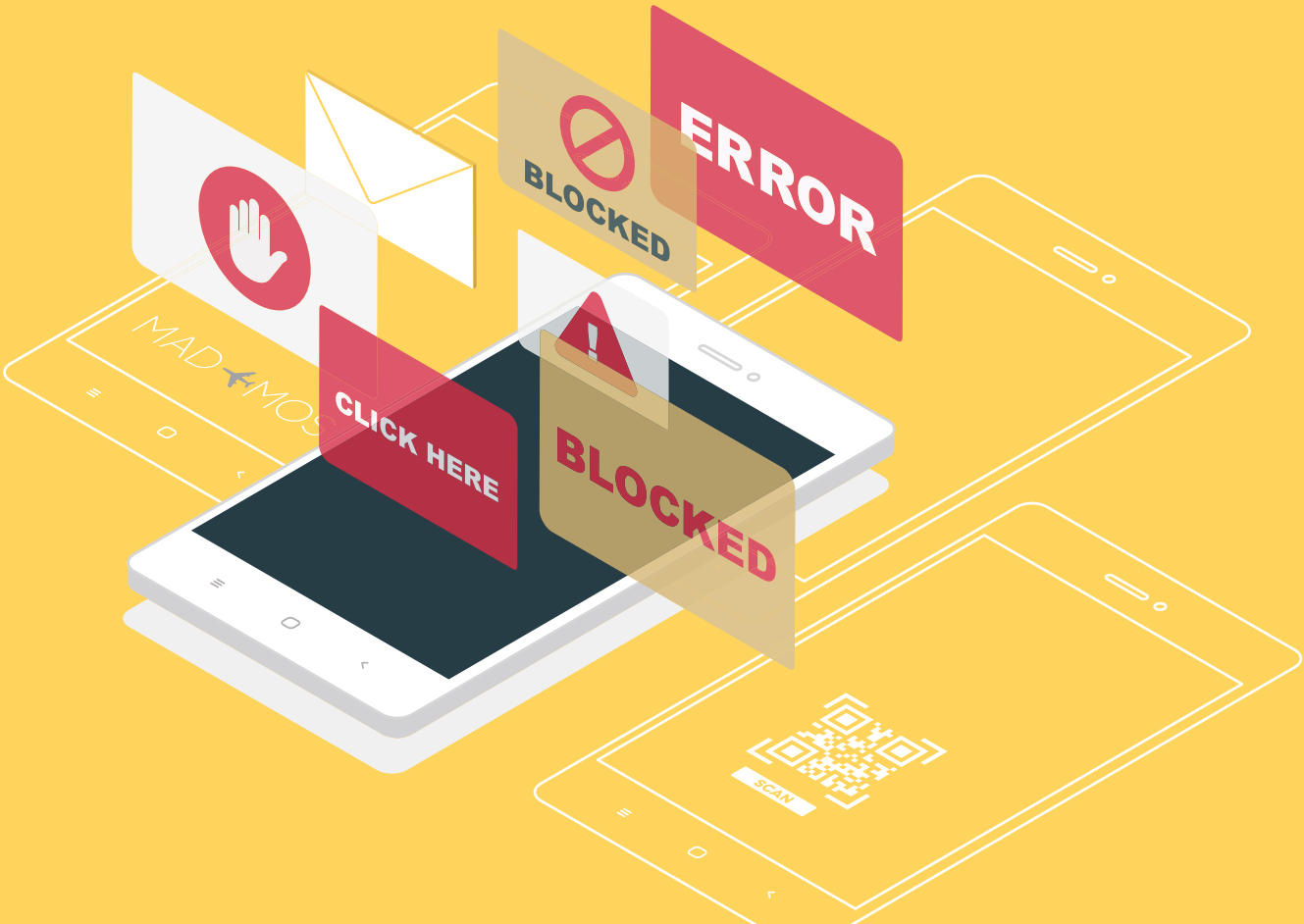
Il procedimento è nato dal reclamo di un interessato il quale, non trovando negli sms ricevuti indicazioni su come esercitare il proprio diritto di opposizione al marketing, aveva scritto all'indirizzo email aziendale dedicato ai contatti con il pubblico. Nonostante una risposta automatica di presa in carico, la richiesta era rimasta senza seguito e gli sms pubblicitari erano continuati.

Nel corso dell'istruttoria, la società ha attribuito l'accaduto a un problema organizzativo: la casella email utilizzata per la richiesta non era presidiata da personale incaricato di gestire le istanze in materia di privacy.

Il Garante ha chiarito che la presenza di un indirizzo dedicato non esonera le aziende dall'obbligo di riconoscere e gestire le richieste ricevute tramite altri canali aziendali. Ha inoltre ricordato che gli sms promozionali devono indicare un recapito idoneo per consentire ai destinatari di esercitare facilmente i propri diritti, ad esempio attraverso un link, un indirizzo email o rispondendo al messaggio sms con la parola "stop".

Oltre alla sanzione, l'Autorità ha ordinato alla società di adeguare le comunicazioni promozionali al Codice Privacy e di riferire entro 30 giorni dalla notifica del provvedimento sulle misure adottate.

Fonte: Federprivacy



# IA E LAVORO

## Il Garante Privacy avverte una start-up italiana. Sotto la lente dell'Autorità il plug-in che può rilevare linguaggio, emozioni e livello di stress dei dipendenti

Il Garante per la protezione dei dati personali ha inviato un avvertimento a una start-up italiana che ha sviluppato un componente aggiuntivo (plug-in) per le piattaforme di messaggistica aziendale Slack e Teams, finalizzato a rilevare, tramite intelligenza artificiale e analisi semantica delle chat, il livello di stress psicologico dei lavoratori che decidano volontariamente di utilizzarlo per ricevere suggerimenti personalizzati.

Le verifiche dell'Autorità, avviate a seguito di notizie di stampa, hanno evidenziato che la start-up tratta i dati degli utenti del servizio in qualità di titolare del trattamento. Il datore di lavoro che acquista il servizio, invece, non può accedere né ai contenuti delle comunicazioni analizzate né ai risultati individuali elaborati dal sistema.

Considerata tuttavia la particolare delicatezza dei dati trattati, nonché la possibilità di fornire ai datori di lavoro report aggregati sul livello di stress dei dipendenti, il Garante ha invitato la società ad adottare, sin dalla progettazione del servizio, misure adeguate a prevenire ogni rischio di accesso, anche indiretto, a informazioni relative alla sfera emotiva dei lavoratori.



Si tratta, infatti, di informazioni che il datore di lavoro non può legittimamente acquisire o trattare, in base alla normativa privacy, allo Statuto dei lavoratori e al Regolamento europeo sull'intelligenza artificiale, che vieta l'uso di sistemi di IA destinati a dedurre o analizzare le emozioni delle persone nei contesti lavorativi.

Il Garante ha infine richiamato i rischi legati all'impiego di tecnologie basate su modelli linguistici e analisi semantica, che possono produrre risultati non sempre trasparenti, spiegabili o verificabili, con possibili effetti discriminatori o lesivi dei diritti dei lavoratori.

Fonte: Garante Privacy

# TELEMARKETING AGGRESSIVO

## Agcom ha bloccato 191 milioni di chiamate nei primi 8 mesi del 2026

Il contrasto al telemarketing aggressivo e alle telefonate con numeri contraffatti registra risultati significativi in Italia, mentre aumentano i controlli sulle responsabilità degli operatori telefonici. Nei primi otto mesi del 2026, i sistemi di filtraggio introdotti dall'Autorità per le Garanzie nelle Comunicazioni (Agcom) hanno bloccato circa 191 milioni di chiamate provenienti dall'estero e associate a numerazioni italiane falsificate o non conformi.

Una cifra che rappresenta il 7,2% del traffico telefonico complessivo considerato e che corrisponde a una media di circa 790 mila telefonate al giorno. Parallelamente, l'Autorità ha disposto nuove sanzioni per oltre 820 mila euro, rafforzando la vigilanza sulle reti e sull'impiego delle numerazioni da parte dei call center.

Secondo i dati diffusi dall'Agcom, tra gennaio e agosto 2026 i filtri anti-spoofing hanno impedito a milioni di telefonate sospette di raggiungere gli utenti italiani. Il sistema interviene sulle chiamate originate all'estero che utilizzano numerazioni italiane contraffatte, una tecnica impiegata per nascondere l'effettiva provenienza del contatto e rendere più difficile l'identificazione del chiamante. L'attività di filtraggio ha consentito anche di circoscrivere parte del fenomeno sul territorio nazionale, agevolando le verifiche sugli operatori coinvolti. I risultati evidenziano l'importanza dei controlli tecnologici nel contrasto alle pratiche commerciali illecite, pur senza rappresentare una soluzione definitiva al problema delle telefonate indesiderate.

Sanzioni per 822.500 euro, nel mirino Retelit e Tekmind - L'Autorità ha annunciato due provvedimenti sanzionatori per complessivi 822.500 euro, di cui 700 mila nei confronti di Retelit Digital Services e 122.500 a carico di Tekmind. Le contestazioni riguardano il mancato rispetto delle misure previste per verificare la correttezza delle numerazioni telefoniche utilizzate dai call center, comprese quelle generate attraverso tecniche di spoofing. Le indagini erano state avviate nel novembre 2025 dopo numerose segnalazioni relative a possibili irregolarità. Retelit ha contestato il



provvedimento, precisando di non svolgere direttamente attività di telemarketing e di limitarsi a concedere numerazioni ad altri operatori autorizzati.

La società ha inoltre definito la decisione inattesa, riservandosi ulteriori valutazioni sul provvedimento.
Codacons e associazioni: tutelare cittadini e imprese regolari - Le sanzioni hanno ricevuto il sostegno del Codacons, che considera il telemarketing illegale un problema non soltanto per i consumatori, ma anche per le imprese che rispettano le regole. Secondo l'associazione, le telefonate commerciali abusive producono un doppio danno economico, compromettendo la fiducia degli utenti e penalizzando gli operatori corretti. Anche l'Alleanza a tutela del mercato, che riunisce sette organizzazioni tra associazioni dei consumatori, imprese e rappresentanze dei lavoratori, ha accolto favorevolmente l'intervento dell'Autorità. La coalizione ha annunciato una piattaforma dedicata alle segnalazioni, pensata per raccogliere le denunce e agevolare il tracciamento delle numerazioni sospette.

Il crollo delle chiamate dall'estero e la nuova sfida dei controlli - L'efficacia dei filtri emerge anche dall'andamento del traffico internazionale: secondo l'Agcom, le chiamate dall'estero con numeri mobili italiani sono diminuite del 95%, passando da 26,8 a 1,2 milioni al giorno rispetto al periodo precedente all'estensione dei blocchi. Nello stesso confronto, il traffico internazionale complessivo è sceso da 34 a 11 milioni di chiamate quotidiane. Dei 191 milioni di contatti intercettati, 148 milioni presentavano numerazioni mobili italiane e circa 38 milioni numeri fissi.
La sfida riguarda ora il rafforzamento della vigilanza sulle reti telefoniche, attraverso controlli sulle numerazioni assegnate e una maggiore collaborazione tra autorità, operatori e associazioni dei consumatori.

Fonte: Federprivacy

# PIANO ISPETTIVO PRIVACY 2026

## Il valore del monitoraggio del DPO

**Con la deliberazione n. 545 del 23 luglio 2026, meglio nota come "piano ispettivo", il Garante privacy ha programmato almeno 35 accertamenti per il periodo che va da agosto a dicembre 2026, anche tramite il proprio Nucleo della Guardia di Finanza, con riferimento a diversi trattamenti e settori. Gli ambiti ispettivi vanno letti come opportunità sicuramente per imprese ed enti per verificare il proprio livello di compliance data protection, ma non solo per loro. Tenuto conto del nuovo piano, infatti, i Data Protection Officer ("DPO") saranno tenuti ad aggiornare i propri monitoraggi ed i relativi metodi di assurance. Si tratta di essere in grado di rapidamente individuare quali processi esaminare, quali evidenze raccogliere ed in che modo verificare che i presidi adottati da titolari e responsabili funzionino nella pratica e possano quindi dirsi idonei a governare i rischi (non solo privacy).**

**Le priorità dell'Autorità**

Il piano comprende geomarketing, neuromarketing e dynamic pricing; fascicoli sanitari elettronici e app mediche; servizi socio-assistenziali comunali, inclusi i fornitori degli applicativi; impiego dell'intelligenza artificiale da parte di Comuni e ASL. Sono inoltre previste verifiche sull'attuazione delle Linee guida del 17 aprile 2026 sui tracking pixel nelle email e sui trattamenti svolti dai fornitori del servizio di DPO agli enti pubblici. Proseguono i controlli sui data breach delle banche dati pubbliche più delicate, con attenzione alla sicurezza, agli accessi abusivi e alla rivendita di informazioni riservate. Si aggiungono approfondimenti sulle violazioni notificate, specie quelle più estese e delicate, nel pubblico e nel privato, e verifiche sui sistemi informativi dei visti (VIS) e doganale. Alcuni di questi processi (e trattamenti) potrebbero coesistere presso la stessa organizzazione. Anzitutto occorrerà domandarsi se i titolari (e responsabili) del trattamento abbiano adeguatamente mantenuto aggiornato il proprio registro dei trattamenti, presidio data protection introdotto dal GDPR per le realtà con oltre 250 dipendenti che negli anni si è dimostrato concretamente lo strumento per agevolare la mappatura dei data flows, anche a prescindere dalla struttura societaria. La mappatura del registro dovrebbe essere in grado

di indicare lo status di implementazione ed aggiornamento dei relativi presidi dei trattamenti in questione: informative privacy per gli interessati, valutazioni di impatto e di legittimo interesse, misure tecniche ed organizzative, conservazione e cancellazione dei dati, per citarne alcuni. Se per il titolare del trattamento l'aggiornamento di tale mappatura è sintomatico di un robusto modello di governance data protection (oltre che di consapevolezza aziendale), per il DPO esso costituisce uno scenario per l'esercizio del proprio monitoraggio.

**Dalle priorità ispettive al monitoraggio concreto**

Come noto, infatti, l'art. 39 GDPR prevede che al DPO spettino consulenza e sorveglianza sull'osservanza della disciplina e delle politiche interne, anche rispetto a responsabilità, formazione e controlli. Il DPO fornisce, se richiesto, un parere sulla valutazione d'impatto e ne sorveglia lo svolgimento; coopera inoltre con l'Autorità. Il suo lavoro deve tenere conto dei rischi dei trattamenti e ciò non può non sostanziarsi nella verifica periodica della mappatura dei processi ad impatto privacy.

Sul piano operativo, il programma ispettivo può orientare un piano di audit calibrato sui trattamenti effettivi dell'organizzazione. Un primo passaggio utile consiste nel confrontare registro dei trattamenti, procedure, contratti e funzionamento dei sistemi, attraverso interviste alle funzioni coinvolte e verifiche a campione. Questo confronto può rivelare raccolte ulteriori, accessi troppo ampi, conservazioni prolungate o utilizzi non valutati.
Per marketing e profilazione, ad esempio, il DPO può ricostruire quali informazioni siano raccolte, da quali fonti e per quali impieghi, verificando la coerenza tra basi giuridiche, informative, consensi ove necessari e configurazioni delle piattaforme. Nel tracciamento delle email è utile esaminare il funzionamento degli strumenti utilizzati e le evidenze delle scelte degli utenti.
Per il dynamic pricing, occorre ricostruire l'eventuale impiego di dati personali, i profili elaborati e gli effetti sulle persone.
In sanità e nei servizi socio-assistenziali, il monitoraggio può concentrarsi sui presupposti di liceità, sulla pertinenza dei dati richiesti, sulle autorizzazioni all'accesso e sui flussi verso i fornitori. Per rendere concreta la verifica, il DPO può chiedere evidenze della revisione delle abilitazioni e della tracciabilità delle consultazioni, esaminando anche la corrispondenza tra istruzioni contrattuali e operatività degli applicativi. Il dialogo con funzioni tecniche e responsabili dei servizi collega rischi giuridici e configurazioni effettive.

Per i sistemi di intelligenza artificiale, un audit può partire dal censimento degli utilizzi, dei dati immessi e dei fornitori, per verificare trasparenza, valutazione dei rischi e necessità della DPIA. Il DPO può inoltre esaminare come siano stati considerati i rischi di risultati inesatti o discriminatori e come siano organizzati gli interventi umani. Le valutazioni vanno documentate dalla progettazione e riesaminate quando cambiano finalità, dati o funzionalità.
Sul fronte della sicurezza, è utile verificare a campione la gestione degli account privilegiati, la revoca delle utenze e la capacità di rilevare consultazioni anomale. Una simulazione di data breach può poi mettere alla prova i flussi di segnalazione interna, il coinvolgimento del DPO, la raccolta delle evidenze e il percorso decisionale per notifiche e comunicazioni. La simulazione permette di individuare ritardi e passaggi incerti su cui intervenire.
Ogni verifica dovrebbe tradursi in rilievi comprensibili, raccomandazioni



motivate e azioni correttive assegnate dall'organizzazione a referenti e scadenze. Il DPO ne segue l'avanzamento e porta al vertice le criticità irrisolte, conservando traccia delle proprie valutazioni. Il monitoraggio assume così continuità e consente di rappresentare, anche durante un'ispezione, quali problemi siano stati individuati, quali decisioni siano state assunte e quali interventi restino da completare.

**Le competenze per il monitoraggio: la DPO Academy**

Quelli fin qui riportati sono solo alcuni spunti operativi per realizzare il monitoraggio del DPO, attività che tuttavia nella pratica richiede esperienza in contesti strutturati, competenze specialistiche non solo data protection, strumenti adatti all'erogazione del controllo ed alla sua documentazione, nonché una composizione sinergica del team a supporto (che non potrà non contemplare figure tecniche) ed una forte flessibilità gestionale.

Anche considerato l'impatto privacy dell'utilizzo di nuove tecnologie (come A.I. ed IoT, per citare alcune macro categorie) e l'entrata in vigore di normative parallele ma ugualmente cogenti (come l'AI Act o il Data Act, per esempio), al DPO è oggi richiesto un approccio – oltre che flessibile – integrato. Ed è su questa integrazione che si sviluppa la settima edizione della DPO Academy di Rödl: 88 ore articolate in 25 moduli, dal 6 novembre 2026 al 28 maggio 2027, in live streaming, con registrazioni e materiali disponibili sulla piattaforma e-learning durante il corso.

Fonte: roedl.it



# DEEPFAKE, COSA HA FATTO IL GARANTE PRIVACY

## Dalla fattispecie di reato introdotta dalla Legge 132/2025 ai recenti interventi del Garante: rischi, responsabilità e limiti

La legge 23 settembre 2025, n.132, Disposizioni e deleghe al Governo in materia di intelligenza artificiale, all'art. 26, comma 1, lett. c), ha previsto l'introduzione, all'art. 612-quater c.p., del reato di "Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale" secondo il quale: "Chiunque cagiona un danno ingiusto ad una persona, cedendo, pubblicando o altrimenti diffondendo,



senza il suo consenso, immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità, è punito con la reclusione da uno a cinque anni. Il delitto è punibile a querela della persona offesa. Si procede tuttavia d'ufficio se il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio ovvero se è commesso nei confronti di persona incapace, per età o per infermità, o di una pubblica autorità a causa delle funzioni esercitate".

Ecco alcuni dei provvedimenti recenti e delle attività svolte dal Garante riguardo al tema dei deepfake.
1) Nei confronti di Clothoff, il 1° ottobre 2025 il Presidente ha firmato un provvedimento di limitazione provvisoria dei trattamenti di dati personali. La Società non avrebbe infatti adottato adeguate misure per impedire a soggetti minori di età di accedere ai servizi o per impedire a utenti anche maggiorenni di caricare immagini di minori o di altri soggetti, in assenza di una valida condizione di liceità. Infine, è stata contestata anche l'assenza di un meccanismo efficiente di watermarking al fine di rendere palese la natura artefatta delle immagini di nudo prodotte.

Con il provvedimento n.789 del 18 dicembre 2025 l'Autorità ha emanato un nuovo avvertimento.



Un'approfondita istruttoria ha riscontrato la presenza sul mercato di servizi che consentono di utilizzare la voce o le immagini anche di terze persone per la generazione di contenuti audio, fotografici e/o audiovisivi basati su tali voci o immagini (tra i quali, appunto, Clothoff).

Pertanto, ha avvertito tutti i titolari e responsabili del trattamento che utilizzano servizi di generazione di contenuti basati sull'intelligenza artificiale partendo da voci o immagini reali di terze persone che tale trattamento dei dati personali può verosimilmente violare le disposizioni del Regolamento, con tutte le conseguenze, anche di carattere sanzionatorio, previste dalla disciplina in materia di protezione dei dati personali. Questo, quando sia effettuato in assenza di un'idonea condizione di liceità e senza che siano preliminarmente fornite agli interessati informazioni corrette e trasparenti.

2) Il 2 gennaio 2026 il Garante si è attivato con un'istruttoria nei confronti di Grok, sistema di AI di X, che consentiva di generare immagini recanti contenuti sessualmente espliciti poi diffusi sul social media X in assenza del consenso delle persone ritratte.

Poiché X ha sede in Irlanda, la procedura è confluita in quella posta in essere dall'autorità Irlandese che, l'8 gennaio 2026, ha confermato che X stesse collaborando attivamente fino ad arrivare alla disattivazione della funzione di nudification di Grok.

3) Il 23 luglio 2026, con un provvedimento di ammonimento nei confronti di R.T.I. Spa, (caso Mentana) il Garante ha affermato che l'impiego di deepfake, anche a fini satirici, deve rispettare la dignità delle persone e i princìpi di liceità, correttezza e trasparenza stabiliti dalla normativa sulla privacy.

Nel caso di specie è stata censurata la lesione dell'immagine professionale di giornalista al fine di introdurre, nel corso di alcune puntate del programma "Striscia la notizia", servizi costruiti prendendo come spunto fatti che hanno coinvolto diversi personaggi pubblici e accompagnandoli con commenti di vario genere pronunciati dal deepfake del reclamante doppiato con sistemi di intelligenza artificiale

Il Garante ha infine inviato richieste di informazioni nei confronti di altri soggetti, tutti residenti al di fuori dell'UE.

Fonte: Garante Privacy



# I DATI AZIENDALI NELL'ERA DELL'AI

## Tra opportunità, privacy e sicurezza: cosa devono sapere oggi le imprese

L'intelligenza artificiale è entrata rapidamente nella quotidianità delle aziende. Viene utilizzata per scrivere email, elaborare documenti, analizzare dati, preparare offerte commerciali, gestire informazioni e velocizzare numerose attività operative.

Strumenti come ChatGPT, Gemini e Copilot rappresentano un'opportunità concreta per migliorare produttività ed efficienza. Ma insieme ai vantaggi emerge una questione che non può essere sottovalutata: **che fine fanno i dati aziendali quando vengono affidati a un sistema di intelligenza artificiale?**

È una domanda che riguarda tutte le imprese, indipendentemente dalle dimensioni o dal settore di appartenenza

## Quando l'efficienza può trasformarsi in un rischio

Immaginiamo una situazione comune: un dipendente deve preparare una risposta a un cliente e decide di utilizzare un sistema di intelligenza artificiale per velocizzare il lavoro. Per ottenere un risultato più preciso, carica una conversazione email, un contratto commerciale o un documento contenente informazioni riservate. L'operazione sembra innocua, ma potrebbe comportare la condivisione di informazioni che l'azienda non avrebbe mai autorizzato a divulgare. Tra i dati che possono finire involontariamente all'interno di una piattaforma AI troviamo:

- Anagrafiche e recapiti dei clienti.
- Contratti, preventivi e condizioni commerciali.
- Dati economici, bilanci e informazioni finanziarie.
- Documenti relativi ai dipendenti.
- Credenziali, configurazioni tecniche e informazioni sui sistemi aziendali.
- Strategie commerciali e informazioni riservate.

Il problema non riguarda soltanto la possibile divulgazione dei dati. Occorre considerare anche le modalità con cui vengono raccolti, conservati, elaborati e utilizzati dai fornitori dei servizi AI.
Non tutte le piattaforme funzionano allo stesso modo: le condizioni di utilizzo, le impostazioni di privacy, le modalità di conservazione e l'eventuale utilizzo dei contenuti per il miglioramento dei modelli possono variare in base al servizio e al tipo di account.
Per questo motivo, utilizzare uno strumento di AI senza averne prima verificato le condizioni può esporre l'impresa a rischi che non sono immediatamente visibili.

## GDPR e intelligenza artificiale: le regole non scompaiono

L'introduzione dell'intelligenza artificiale non mette in secondo piano il GDPR. Al contrario, rende ancora più importante applicarne correttamente i principi.
Quando un sistema AI tratta dati personali, l'azienda deve continuare a garantire il rispetto dei principi fondamentali della protezione dei dati:

- **Liceità e trasparenza**
  Deve esistere una base giuridica adeguata e le persone devono essere informate correttamente.

- **Limitazione delle finalità**
  I dati devono essere utilizzati per finalità determinate e legittime.

- **Minimizzazione**
  Non devono essere condivise più informazioni di quelle effettivamente necessarie.

- **Sicurezza**
  Devono essere adottate misure tecniche e organizzative adeguate a proteggere le informazioni.

- **Responsabilizzazione**
  L'azienda deve essere in grado di dimostrare di aver valutato e gestito correttamente i rischi.

Un aspetto importante riguarda anche i fornitori delle piattaforme AI. Prima di introdurre uno strumento nei processi aziendali è necessario comprenderne il ruolo nel trattamento dei dati, verificare le condizioni contrattuali e valutare gli eventuali trasferimenti di informazioni verso Paesi extraeuropei.

## AI Act: non basta utilizzare l'intelligenza artificiale, bisogna saperla governare

Accanto al GDPR, il Regolamento europeo sull'intelligenza artificiale (AI Act) introduce un quadro di regole specifico per lo sviluppo e l'utilizzo dei sistemi AI.
Tra gli aspetti da considerare c'è l'AI Literacy, ovvero la necessità di promuovere competenze e consapevolezza nell'utilizzo dell'intelligenza artificiale.
L'articolo 4 del Regolamento richiede a fornitori e utilizzatori di sistemi AI di adottare misure per favorire un adeguato livello di alfabetizzazione sull'intelligenza artificiale del personale coinvolto, tenendo conto delle conoscenze e del contesto di utilizzo.
Questo significa che la formazione non dovrebbe essere considerata un'attività accessoria, ma una componente della gestione aziendale. Non è sufficiente mettere a disposizione dei dipendenti uno strumento tecnologico: occorre anche spiegare come utilizzarlo, quali informazioni possono essere condivise e quali comportamenti devono essere evitati.

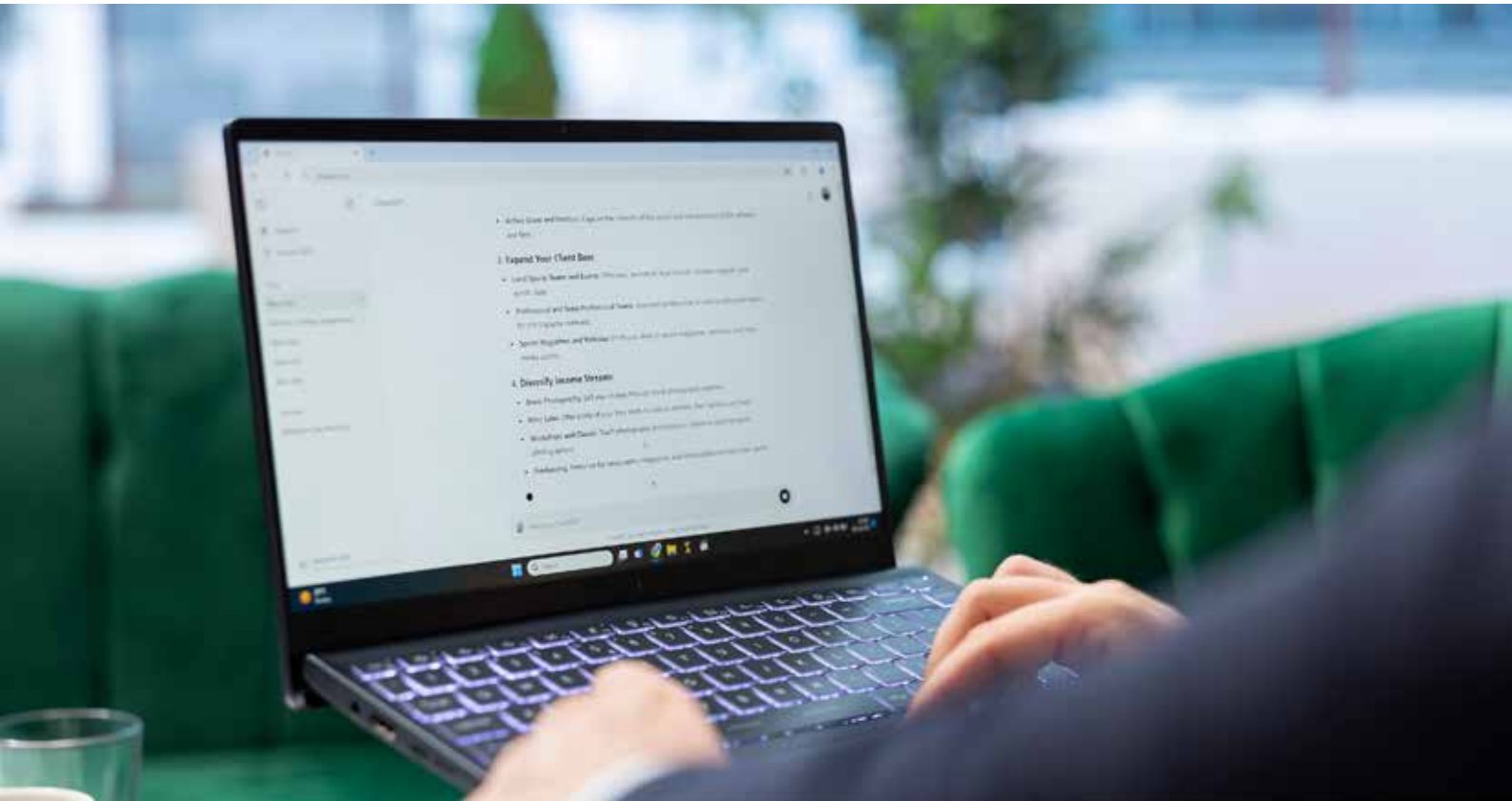
## Shadow AI: quando l'AI entra in azienda senza che l'azienda lo sappia

C'è un fenomeno che merita particolare attenzione: la cosiddetta Shadow AI.
Si verifica quando dipendenti e collaboratori utilizzano strumenti di intelligenza artificiale senza che la direzione o il reparto IT ne siano a conoscenza o ne abbiano autorizzato l'utilizzo.

Può accadere attraverso account personali, applicazioni gratuite, estensioni del browser o piattaforme online.
Il rischio è che informazioni aziendali vengano trasferite verso servizi esterni senza alcuna valutazione preventiva, senza procedure condivise e senza un controllo sulle modalità di trattamento.

In questi casi, il problema non è necessariamente la tecnologia utilizzata, ma l'assenza di regole e di consapevolezza.

Fonte: Webinar Euristica del 06/10/2026



# 5 ACCORGIMENTI PER PROTEGGERE I DATI AZIENDALI

## 1.
### Definire una policy aziendale sull'utilizzo dell'AI

Stabilire quali strumenti possono essere utilizzati, per quali finalità e con quali limitazioni.

## 2.
### Classificare le informazioni

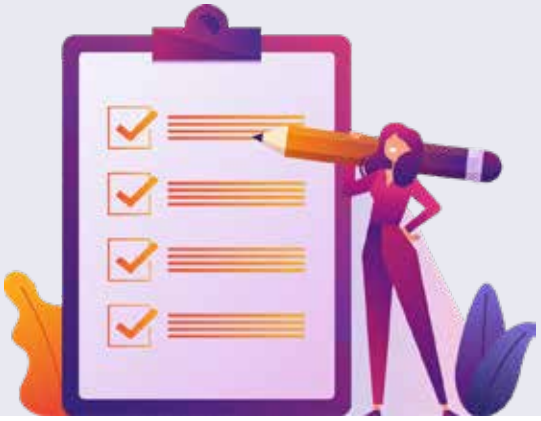
Distinguere tra dati pubblici e interni, riservati, personali e particolarmente sensibili, definendo cosa può essere condiviso con le piattaforme AI.

## 3.
### Verificare i fornitori

Analizzare condizioni contrattuali, informative privacy, modalità di conservazione, sicurezza e utilizzo dei dati da parte delle piattaforme.

## 4.
### Formare dipendenti e collaboratori

Fornire indicazioni pratiche sui rischi, sulle modalità di utilizzo e sulle informazioni da non inserire nei prompt.



## 5.
### Aggiornare le procedure

L'intelligenza artificiale evolve rapidamente. Le regole aziendali devono essere periodicamente riviste insieme alle misure di sicurezza e alla valutazione dei rischi.

# LA VERA SFIDA È INNOVARE SENZA PERDERE IL CONTROLLO

L'intelligenza artificiale non rappresenta soltanto una nuova tecnologia da introdurre in azienda. È un cambiamento che coinvolge persone, processi, informazioni e responsabilità.

La possibilità di lavorare più velocemente e prendere decisioni supportate dai dati è un'opportunità importante, ma non può prescindere dalla protezione del patrimonio informativo aziendale.

La sicurezza non deve diventare un ostacolo all'innovazione, così come la privacy non deve essere percepita esclusivamente come un obbligo normativo.

La domanda, quindi, non è più se introdurre l'intelligenza artificiale nei processi aziendali, ma se siamo davvero pronti a utilizzarla in modo sicuro e responsabile.

Un'azienda che conosce i propri dati, governa gli strumenti che utilizza e forma le proprie persone è un'azienda più preparata ad affrontare il cambiamento digitale.

EURISTICA

# FORMAZIONE AI

L'AI sta trasformando il lavoro e le competenze richieste.
Senza formazione, il rischio è di rimanere indietro.




## LA FORMAZIONE È IL TUO VANTAGGIO COMPETITIVO

In Euristica crediamo che la conoscenza sia il primo passo per innovare. Offriamo percorsi di formazione sull'intelligenza artificiale per aziende e professionisti, pensati per sviluppare competenze pratiche e consapevoli.

**Formarsi oggi significa essere pronti al domani.**

### PERCORSI PRATICI E APPLICATIVI

**Formazione concreta e orientata ai risultati, per utilizzare l'AI nel lavoro quotidiano.**

- strumenti e casi d'uso reali
- esercitazioni guidate
- contenuti aggiornati e subito applicabili

### IN PRESENZA E ONLINE

**Scegli la modalità più adatta alla tua organizzazione:**

- formazione in presenza su tutto il territorio
- corsi online interattivi in diretta
- flessibilità e massima

### PER AZIENDE E PROFESSIONISTI

**Percorsi su misura per team, reparti e singoli professionisti.**

- formazione personalizzata per ogni esigenza
- team building e aggiornamento delle competenze
- supporto continuo e

### COMPETENZE OGGI VALORE DOMANI

**Investire nella formazione AI significa aumentare produttività, innovazione e competitività.**

- migliori decisioni e processi più efficienti
- maggiore consapevolezza e autonomia
- prepararsi al futuro,

## PERCHÉ SCEGLIERE LA FORMAZIONE AI DI EURISTICA

- → **Formazione AI in presenza e online**
- → **Docenti esperti e casi reali**
- → **Percorsi su misura per ogni esigenza**
- → **Approccio pratico e orientato ai risultati**
- → **Aggiornamento continuo sulle novità AI**
- → **Supporto e consulenza anche dopo il corso**

**EURISTICA S.R.L.**
P.IVA 02432270540

Via Brunelleschi, snc
06024 Gubbio | PG

+39 075 922 1401
euristica.com

info@euristica.com
commerciale@euristica.com

EURISTICA

**Euristica srl**
Via Brunelleschi, snc
Gubbio | PG

+39 075 922 1401
euristica.com
privacy@euristica.com