

D.Lgs. 179/2026: il secondo decreto di adeguamento all'AI Act e ciò che cambia per le imprese

Allinea

Avvera Compliance Review

Tracking pixel nelle e-mail: il Garante chiarisce gli obblighi per le imprese

Il Garante fissa il confine tra anonimizzazione e pseudonimizzazione

Ottobre 2026

Avvera al Convegno sulla Responsabilità Penale per la Violazione delle Misure Restrittive UE

Avvera al Convegno "e-privacy XXXIX" dedicato alla tutela dei diritti fondamentali e della privacy in Rete

Allinea
Avvera Compliance Review
Ottobre 2026

Tracking pixel nelle e-mail

Il Garante chiarisce gli obblighi per le imprese

Il monitoraggio delle aperture delle e-mail è una funzionalità ormai consolidata nelle piattaforme di marketing automation. Tuttavia, la possibilità di sapere chi ha aperto un messaggio, quante volte lo ha consultato e in quale momento pone questioni rilevanti in materia di protezione dei dati personali. Con il vademecum pubblicato il 5 ottobre 2026, il Garante per la protezione dei dati personali ha richiamato l'attenzione sulle Linee guida del 17 aprile 2026 dedicate all'utilizzo dei tracking pixel nelle comunicazioni di posta elettronica. Il termine previsto per l'adeguamento è fissato al 29 ottobre 2026.



"Verificare oggi gli strumenti di tracciamento significa ridurre il rischio di trattamenti illeciti"

Che cosa sono i tracking pixel e quale disciplina si applica?
I tracking pixel sono immagini di dimensioni minime, spesso trasparenti e invisibili al destinatario, inserite nel codice HTML di un'e-mail e richiamate da un server remoto. Quando il programma di posta scarica l'immagine, il server può registrare l'apertura del messaggio e raccogliere informazioni tecniche, come l'indirizzo IP, l'orario dell'evento e identificativi associati al destinatario. Il problema giuridico non riguarda soltanto l'eventuale profilazione commerciale. Il tracciamento può avvenire senza che l'interessato ne sia consapevole, consentendo al mittente di monitorarne il comportamento. Il Garante riconduce l'impiego di questi strumenti all'articolo 122 del Codice Privacy, che disciplina l'archiviazione di informazioni sul terminale dell'utente e l'accesso a informazioni già archiviate. Ne consegue che la liceità non può essere valutata esclusivamente sulla base dell'articolo 6 GDPR: occorre verificare anche le condizioni previste dalla disciplina speciale sulle comunicazioni elettroniche, oltre agli obblighi di trasparenza e responsabilizzazione del titolare.

Quando è necessario il consenso?
La regola generale è il consenso preventivo, libero, specifico e informato per l'utilizzo dei tracking pixel, fatte salve le eccezioni individuate dal Garante. Una distinzione essenziale riguarda la finalità e le modalità del trattamento. Il monitoraggio individuale delle aperture per misurare l'interesse verso prodotti, segmentare i destinatari o attivare successive campagne promozionali richiede una verifica specifica dell'obbligo di consenso. Diversamente, può essere ammessa la misurazione statistica aggregata quando siano adottate misure idonee a impedire l'identificazione dei singoli destinatari. Possono inoltre rilevare le deroghe previste per comunicazioni di servizio e finalità strettamente necessarie, da valutare in concreto. Non è quindi sufficiente che una piattaforma offra una funzione di tracciamento: il titolare deve verificare se l'uso effettivo sia compatibile con le condizioni di liceità previste.

Come devono adeguarsi le aziende?
L'adeguamento richiede interventi tecnici e documentali coordinati. In particolare, le imprese devono:

- verificare se gli strumenti in uso impiegano tracking pixel e quali dati raccolgono;
- rivedere informative e consensi;
- configurare correttamente gli strumenti in uso e privilegiare, ove possibile, statistiche aggregate e misure di minimizzazione;
- garantire una revoca effettiva, separando il consenso al tracciamento da quello alla ricezione delle comunicazioni promozionali.

La possibilità di revocare il solo consenso al tracciamento assume particolare importanza. L'interessato dovrebbe poter continuare a ricevere una newsletter anche senza essere monitorato, quando ciò sia compatibile con il servizio offerto. Il 29 ottobre 2026 rappresenta quindi una scadenza operativa per le imprese: verificare oggi gli strumenti di tracciamento significa ridurre il rischio di trattamenti illeciti e rendere le attività di e-mail marketing più trasparenti e sostenibili sotto il profilo della protezione dei dati personali.

Allinea
Avvera Compliance Review
Ottobre 2026

Il Garante fissa il confine tra anonimizzazione e pseudonimizzazione

Con il provvedimento n. 710 del 23 settembre 2026, pubblicato il 2 ottobre, il Garante per la protezione dei dati personali ha sanzionato un noto fornitore di servizi di ricerca clinica e informazioni commerciali per sette milioni di euro. Oggetto del procedimento è il database LPD (Longitudinal Patient Data), alimentato dai dati clinici di oltre un milione di pazienti di circa ottocento medici di medicina generale aderenti alla SIMG. La società sosteneva di trattare dati anonimi, e dunque fuori dall'ambito applicativo del Regolamento, richiamando anche la sentenza della Corte di giustizia del 4 settembre 2025, C-413/23 P (EDPS c. SRB). L'Autorità ha respinto la ricostruzione. Il provvedimento merita attenzione non per l'entità della sanzione, ma perché è tra le prime applicazioni nazionali della sentenza SRB e ne delimita il perimetro.



Il criterio: una valutazione, non un automatismo

Il metro è quello del parere WP29 05/2014, ribadito dalle linee guida EDPB 02/2026 sull'anonimizzazione, adottate il 7 luglio 2026 e ancora in consultazione pubblica. Un processo di anonimizzazione compiuto deve impedire, con i mezzi ragionevolmente disponibili, di isolare una persona (single-out), di collegarne i dati a un distinto insieme di dati (linkability) e di dedurne nuove informazioni (inference). I tre criteri non operano però in modo automatico. Come ricorda il Garante citando l'EDPB, se tutti sono soddisfatti i dati possono considerarsi anonimi; se uno non lo è, servono ulteriori analisi per stabilire se possano comunque esserlo (par. 88). Il fallimento di un criterio apre l'indagine, non la chiude. La pseudonimizzazione resta altra cosa. L'art. 4, n. 5, del Regolamento la definisce come un trattamento che impedisce l'attribuzione dei dati senza informazioni aggiuntive conservate separatamente. Il considerando 26 chiarisce che i dati pseudonimizzati restano personali, e già il WP29 la qualificava come misura di sicurezza utile, non come metodo di anonimizzazione (par. 84).

Destinatario o titolare: il perimetro della sentenza SRB

Il cuore del provvedimento è il confronto con la sentenza SRB. Il Garante ne accoglie l'impostazione relativa: lo stesso dataset può essere personale per chi dispone delle informazioni necessarie a reidentificare e anonimo per chi non ne dispone né può ragionevolmente procurarsele (par. 89). Perché i dati perdano carattere personale per il destinatario devono però ricorrere tre condizioni (par. 93). Il destinatario non deve poter incidere sulle misure di pseudonimizzazione, non deve poter reidentificare con altri mezzi, come l'incrocio con altri elementi, e non deve poter trasferire i dati ad altri. La società sanzionata non rientra in questo schema, perché non è un destinatario ma il titolare dell'intero trattamento, sin dalla raccolta presso i medici (parr. 81 e 99). La qualificazione discende dal criterio sostanziale dell'art. 4, n. 7, e dagli elementi di fatto: la proprietà del database, i contratti con i medici e con il fornitore del software, nominato responsabile ex art. 28, e le istruzioni sull'anonimizzazione impartite a quest'ultimo con l'allegato A al contratto del 26 febbraio 2020. Non rileva che la società non avesse modificato la struttura dei record dell'add-on: averne scelto e mantenuto l'uso senza verificarne la robustezza non esclude la titolarità (par. 77). Richiamando Fashion ID (C-40/17), il Garante tratta raccolta e anonimizzazione come fasi di un unico trattamento, che non possono essere valutate separatamente (par. 75).

Il Garante fissa il confine tra anonimizzazione e pseudonimizzazione

"L'anonimizzazione si svolge su dati ancora identificativi ed è essa stessa un trattamento di dati personali"

Perché i dati non erano anonimi

Ogni paziente era censito con lo stesso codice (Pat ID) per tutto il rapporto con il proprio medico; il codice cambiava solo al cambio di medico o di computer. In sede ispettiva la società ha mostrato un paziente presente 34 volte nella tabella delle prescrizioni, con la storia clinica ricostruibile (par. 7). A quel codice erano associati anno di nascita, sesso, stato civile, diagnosi, sintomi, allergie, prescrizioni, vaccinazioni, esami e dati di localizzazione (par. 101). Il Garante rileva due limiti strutturali delle misure adottate. La *k*-anonymity agisce solo sui quasi-identificatori: record formalmente indistinguibili restano unici se si considerano diagnosi, sequenze di ricoveri o pattern di assunzione di farmaci. L'hashing protegge l'identità diretta ma è costruito proprio per preservare l'unicità, così da riferire la storia clinica allo stesso soggetto (parr. 95-97). Ne segue che i pazienti erano reidentificabili con mezzi ragionevoli. Basta la capacità di reidentificare, a prescindere dall'intenzione di farlo (par. 100).

L'anonimizzazione è un trattamento

Il Garante ribadisce un principio già affermato dall'EDPB nel documento del 2 febbraio 2021 sulla ricerca sanitaria, dal WP29 nel 2014, dalle linee guida 02/2026 (par. 2.5.2) e dal Tribunale di Milano nella sentenza del 10 maggio 2024 sul caso THIN. L'anonimizzazione si svolge su dati ancora identificativi ed è essa stessa un trattamento di dati personali (par. 90). Come tale, pur essendo compatibile con la finalità iniziale della raccolta, richiede una propria base giuridica (par. 106). L'esito anonimo non sana l'assenza di un fondamento di liceità a monte. Nel caso di specie mancava sia una condizione dell'art. 6 sia un'eccezione al divieto dell'art. 9: il contratto con i medici non poteva valere come base giuridica, perché i pazienti non ne erano parte.

Le altre violazioni e il data breach

Il dispositivo accerta la violazione degli artt. 5, par. 1, lett. a), e) e f) e par. 2, 9, 13, 25, 28, 32 e 35 del Regolamento. Le contestazioni sono le seguenti:

- assenza di base giuridica per il trattamento di dati relativi alla salute;
- informativa priva degli elementi dell'art. 13;
- mancata definizione dei tempi di conservazione, con dati che risalivano fino al 2001;
- mancata nomina dei medici come responsabili ex art. 28;
- omessa valutazione d'impatto;
- misure di sicurezza inadeguate e violazione dei principi di accountability e privacy by design.

Al procedimento è stato riunito quello sulla violazione notificata dalla stessa società. Attraverso i campi a testo libero del gestionale, l'add-on aveva estratto i dati direttamente identificativi di 3.370 pazienti, per 3.080 dei quali insieme a dati sanitari, poi trasmessi alla SIMG. Il Garante ha escluso che la responsabilità ricadesse sui medici: spettava al titolare verificare che l'add-on non estraesse informazioni estranee al progetto (par. 80).

Misure correttive e sanzione

Se intende proseguire il progetto, la società dovrà individuare una base giuridica, anche per l'eventuale anonimizzazione, rendere l'informativa ai pazienti, svolgere la valutazione d'impatto e nominare i medici responsabili del trattamento. Entro centoventi giorni dalla notifica dovrà documentare al Garante le iniziative intraprese (par. 150). In alternativa, l'anonimizzazione dovrà essere svolta dai medici, con una propria base giuridica e una propria informativa ai pazienti, secondo garanzie precise (parr. 146-148):

- i medici determinano in autonomia la pseudonimizzazione, con una codifica casuale che per la società sia una sequenza priva di significato;
- le classi di equivalenza sui quasi-identificatori non possono avere meno di dieci unità;
- le variabili residue osservabili dalla società vanno incluse nelle classi, trattate con tecniche distribuite come la secure multiparty computation, oppure rimosse.

Il Garante fissa il confine tra anonimizzazione e pseudonimizzazione

La misura alternativa conferma la lettura della sentenza SRB: dati pseudonimizzati possono essere anonimi per la società, ma solo se è un soggetto diverso, che detiene legittimamente i dati identificativi, a progettare e applicare le misure. Il massimo edittale è stato calcolato sul fatturato consolidato della controllante statunitense. Tra le attenuanti il Garante ha considerato la cessazione dei flussi dai medici, l'assenza di reclami, la collaborazione prestata e il valore del database come risorsa di ricerca. La società ha dichiarato di riservarsi il ricorso.

Cosa ne discende per le imprese

Chi tratta dati sanitari per finalità secondarie deve fare tre verifiche.

- Il ruolo prima del dato. L'approccio relativo della sentenza SRB giova solo al destinatario che non incide sulle misure di pseudonimizzazione. Chi progetta o finanzia la pipeline, dà istruzioni al fornitore o è proprietario del database è titolare, e per lui i dati restano personali. La qualificazione non si costruisce con la clausola contrattuale: si accerta sui fatti.
- Il test di reidentificabilità sull'intero record. Un codice persistente associato a un payload clinico ricco rende i dati reidentificabili, anche quando la k-anonymity è rispettata sui soli quasi-identificatori. La valutazione va documentata con indicatori misurabili, come l'incidenza percentuale dei casi di single-out.
- La base giuridica dell'anonimizzazione. L'operazione di anonimizzazione va fondata e documentata autonomamente, a monte del suo esito.

Allinea
Avvera Compliance Review
Ottobre 2026

D. Lgs 179/2026

Il secondo Decreto di adeguamento all'AI Act e ciò che cambia per le imprese

Nella Gazzetta Ufficiale n. 234 dell'8 ottobre è stato pubblicato il decreto legislativo 7 ottobre 2026, n. 179, che adegua l'ordinamento al Regolamento (UE) 2024/1689 in materia di poteri delle autorità nazionali e di utilizzo dell'intelligenza artificiale nella formazione. Entra in vigore il 23 ottobre. È il secondo dei due decreti approvati in via definitiva ad agosto: il primo, su polizia, biometria e responsabilità, è il D.Lgs. 160/2026, in vigore dal 30 settembre. Cinquantaquattro articoli, cinque capi. Quattro profili meritano attenzione.

"AgID è autorità di notifica degli organismi di valutazione della conformità. L'ACN è autorità di vigilanza del mercato e punto di contatto unico con l'Unione"

Chi vigila, e su cosa

AgID è autorità di notifica degli organismi di valutazione della conformità. L'ACN è autorità di vigilanza del mercato e punto di contatto unico con l'Unione. ACN gestisce la registrazione nazionale dei sistemi ad alto rischio relativi alle infrastrutture critiche. Banca d'Italia, CONSOB e IVASS vigilano sui sistemi ad alto rischio impiegati nei rispettivi settori, con poteri ispettivi propri. Il Garante opera nei limiti dell'art. 74, par. 8, del Regolamento. Le modalità di esercizio dei poteri sono rinviate a un DPCM. Fino alla sua adozione la mappa delle competenze è definita, la procedura ispettiva non ancora. L'art. 23 fissa le sanzioni: fino a 35 milioni o al 7% del fatturato mondiale per le pratiche vietate; fino a 15 milioni o al 3% per gli obblighi di fornitori, importatori, distributori e deployer; fino a 7,5 milioni o all'1% per informazioni inesatte o fuorvianti rese alle autorità. Quest'ultima voce è quella da presidiare subito, perché riguarda la risposta alle richieste istruttorie, a prescindere dalla conformità sostanziale.

D. Lgs 179/2026
Il secondo Decreto di adeguamento all'AI Act e ciò che cambia per le imprese

L'art. 41: una disciplina più rigorosa dell'art. 22 GDPR
Le decisioni finali su assunzione, modifica e cessazione del rapporto, compresi provvedimenti disciplinari e valutazioni delle prestazioni, non possono fondarsi unicamente su un trattamento automatizzato. La decisione spetta a una persona fisica con potere effettivo e autonomo, e il lavoratore può ottenere una motivazione intelligibile che indichi l'incidenza del sistema e i principali parametri considerati. La violazione comporta la nullità. Due precisazioni cambiano la lettura. Il consenso del lavoratore non opera come eccezione: è uno scarto rispetto all'art. 22, par. 2, lett. c), del Regolamento generale, che lo ammette. La ricerca e selezione delle candidature non rientra fra le decisioni finali, anche quando esclude il candidato dalle fasi successive. Il filtro automatico in fase di screening resta quindi fuori dalla sanzione di nullità, ma non dall'art. 22 GDPR che continua ad applicarsi e che il decreto non può derogare.

Sicurezza sul lavoro
L'art. 42 impone di ponderare nel documento di valutazione dei rischi ex art. 28 del D.Lgs. 81/2008 i sistemi che incidono su organizzazione, ritmi, modalità della prestazione o decisioni rilevanti per la sicurezza, con correlati obblighi di informazione e formazione. I sistemi di AI escono dalla categoria del software gestionale ed entrano nel perimetro prevenzionistico.

Segreto commerciale e obbligo di esibizione
L'art. 52 introduce il comma 1-bis all'art. 98 del codice della proprietà industriale: dati, algoritmi e metodi di addestramento - architetture, funzioni di ottimizzazione, configurazioni - possono costituire segreto commerciale. Il punto va letto insieme all'art. 17 del D.Lgs. 160/2026, che consente al danneggiato di ottenere l'esibizione della documentazione tecnica, con i fatti allegati ritenuti ammessi in caso di inadempimento. Il segreto non è un argomento per rifiutare l'esibizione, ma per ottenerne le modalità protette. Chi non ha classificato in anticipo il proprio patrimonio tecnico come riservato non potrà invocarne la tutela nel momento in cui serve.

Indicazioni operative
L'organizzazione deve:
- mappare i sistemi in uso rispetto al nuovo riparto di competenze, individuando per ciascuno l'autorità di riferimento;
- rivedere i processi HR che impiegano AI, documentando l'intervento umano effettivo e predisponendo la motivazione da rendere su richiesta;
- valutare l'aggiornamento del DVR;
- formalizzare la classificazione come segreto commerciale di dataset e modelli proprietari, con le misure di protezione che l'art. 98 richiede;
- definire una procedura per le richieste istruttorie, con revisione legale delle risposte tecniche prima dell'invio.



Allinea
Avvera Compliance Review
Ottobre 2026

Avvera al Convegno sulla Responsabilità Penale per la Violazione delle Misure Restrittive UE



Il 19 novembre 2026, Avvera parteciperà al convegno "La Responsabilità Penale per la Violazione di Misure Restrittive dell'Unione Europea", organizzato dal Dipartimento di Scienze Giuridiche Cesare Beccaria dell'Università degli Studi di Milano. L'Avv.Giancarlo Besia e Luca Franzetti, PhD, di Avvera interverranno alla tavola rotonda "La gestione dei rischi e gli adempimenti di compliance", dedicata alle implicazioni operative delle novità introdotte dal D.Lgs. 211/2025. La partecipazione conferma l'impegno di Avvera nell'approfondimento delle evoluzioni normative e nella promozione di un confronto tra mondo accademico e imprese sui temi della compliance e della gestione dei rischi.

Allinea
Avvera Compliance Review
Ottobre 2026

Avvera al Convegno "e-privacy XXXIX" dedicato alla tutela dei diritti fondamentali e della privacy in Rete

Pavia 13-14 novembre 2026

L'intelligenza artificiale sta trasformando non solo il modo in cui scriviamo e studiamo, ma anche il nostro modo di ragionare e formarci un'opinione. Nel suo intervento, la nostra esperta Avv. Lucia Ruggiero, affronterà il tema della progressiva omologazione del pensiero, favorita dall'uso sempre più diffuso dei chatbot. La proposta è di riconoscere un "diritto all'autonomia cognitiva", capace di tutelare non soltanto la libertà di pensiero, ma anche il processo attraverso cui maturiamo idee, dubbi e giudizi personali. Una sfida particolarmente importante per le nuove generazioni, in un mondo in cui il rischio non è più che qualcuno ci impedisca di pensare, ma che smettiamo di farlo da soli.



Allinea

Avvera Compliance Review

Newsletter Informativa
riservata a clienti e partner
di Avvera

Ottobre

Tutti i diritti riservati
© AVVERA srl S.B.

AVVERA | SB Società Benefit

Largo Umberto Boccioni 1
21040 Origgio VA
T. +39 02 96515401

Altre sedi
Milano - Pesaro - Udine

avvera.it - info@avvera.it

Immagini: © Adobe Stock, © Deposit Photos, © Esalta