



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

NEWSLETTER 30/09/26 - Convegno il 20 ottobre con i consumatori - Sanzione di 39mila euro a società di vigilanza di Bologna - Più tutele per rider e lavoratori gestiti da piattaforme digitali - Recupero crediti: online la versione aggiornata del vademecum - Videosorveglianza, sanzionato l'Istituto Nazionale di Ricerca Metrologica - Il ruolo del RPD al centro del nuovo episodio del podcast



GPDP

newsletter

NOTIZIARIO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

anno
XXVII

NEWSLETTER N. 552 del 30 settembre 2026

- [Vita digitale e dati personali. Convegno il 20 ottobre con le Associazioni consumatori](#)
- [Garante: sanzione di 39mila euro a società di vigilanza di Bologna](#)
- [Più tutele per rider e lavoratori gestiti da piattaforme digitali](#)
- [Recupero crediti: online la versione aggiornata del vademecum del Garante](#)
- [Videosorveglianza, Garante privacy sanziona l'Istituto Nazionale di Ricerca Metrologica](#)
- [Il ruolo del RDP al centro del nuovo episodio del podcast del Garante Privacy](#)
- [Sanzione di 403 milioni a Google, intervento del Garante privacy italiano con la Dpc irlandese](#)
- [L'Autorità Garante per la privacy e il caso Revolut](#)
- [La Cassazione conferma la correttezza dell'operato del Garante privacy](#)

Vita digitale e dati personali. Convegno il 20 ottobre con le Associazioni consumatori

**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

VITA DIGITALE E DATI PERSONALI

Il Garante incontra le Associazioni dei consumatori

*martedì 20 ottobre 2026
ore 9.30 - 13*

Auditorium della Tecnica
Viale Umberto Tupini, 65 - 00144 Roma

Martedì 20 ottobre 2026 l'Autorità Garante per la protezione dei dati personali organizza un evento dal titolo "Vita Digitale & dati personali. Il Garante incontra le Associazioni dei consumatori".

L'incontro si svolgerà dalle ore 9.30 alle 13 presso l'auditorium di Confindustria, viale Umberto Tupini 65, Roma, ed è programmato in collaborazione con il Ministero delle Imprese e del Made in Italy, e con le Associazioni dei consumatori.

Sarà un'occasione importante di dialogo con il mondo dei consumatori sui temi dell'intelligenza artificiale, del telemarketing illecito, del fascicolo sanitario digitale, del futuro dei nostri dati digitali dopo di noi. Le sessioni che scandiranno la mattinata dei lavori toccheranno temi di grande attualità, cercando di conoscere meglio come tutelare i dati personali di ciascuno di noi anche attraverso l'aiuto prezioso e proattivo dell'Autorità Garante Privacy.

Tutti sono invitati. Sul sito dell'Autorità Garante verranno indicate le modalità per l'iscrizione. Dato l'alto livello formativo della giornata, l'incontro rientrerà tra le giornate formative del personale del Garante e del Ministero delle Imprese e del made in Italy.

[CLICCA QUI PER SCARICARE IL PROGRAMMA](#)

**Garante: sanzione di 39mila euro a società di vigilanza di Bologna
Dati Gps auto aziendale per contestazione disciplinare. Licenziato l'addetto**







Il Garante per la protezione dei dati personali ha inflitto una sanzione di 39mila euro a La Patria S.p.A. di Bologna, società di vigilanza e sicurezza tecnologica, per specifiche violazioni del Regolamento europeo (Gdpr) nel trattamento dei dati dei dipendenti ([provvedimento n.585 del 6.8.2026](#)).

L'Autorità si era attivata a seguito del reclamo di un ex lavoratore al quale la società aveva negato l'accesso, tra l'altro, ai dati raccolti tramite il sistema di localizzazione satellitare GPS installato sull'autovettura aziendale a lui assegnata. L'interessato aveva chiesto di visionare e ottenere copia di tale documentazione per difendersi in una contestazione disciplinare con l'azienda che lo aveva licenziato.

Nel provvedimento il Garante – ritenendo illecita la condotta della società, in quanto non aveva fornito idoneo riscontro all'istanza di esercizio del diritto di accesso ai dati – ha ribadito che il titolare del trattamento anche quando reputa di non poter dare seguito a istanze di esercizio dei diritti, deve comunque comunicare al richiedente i motivi del diniego, nonché l'esistenza del diritto di presentare ricorso all'autorità giudiziaria o reclamo al Garante privacy. Circostanza non verificatasi nel caso in specie.

L'Autorità ha inoltre accertato che la società di vigilanza non aveva adempiuto all'obbligo di informativa per quanto riguarda il trattamento dei dati effettuato tramite il GPS aziendale, nonostante gli stessi siano dati personali. Fra l'altro, anche nell'accordo stipulato con le rappresentanze sindacali ai sensi dell'articolo 4 dello Statuto dei Lavoratori era richiamato l'obbligo di informativa previsto dalla disciplina di protezione dei dati. I documenti informativi erano inoltre non corretti in quanto descrivevano operazioni di trattamento di dati particolari che la società in realtà non effettuava.

Nel determinare l'importo della sanzione, il Garante Privacy ha tenuto conto del fatto che La Patria S.p.A. nel corso dell'istruttoria ha adottato le misure correttive necessarie a conformare i trattamenti al Gdpr. In particolare, ha fornito un'idonea informativa in merito al trattamento dei dati di geolocalizzazione ai propri dipendenti e ha rimosso sempre nella stessa i riferimenti ai trattamenti dei dati particolari.

Più tutele per rider e lavoratori gestiti da piattaforme digitali

Le garanzie passano dalla protezione dati





Il Garante Privacy ha espresso parere favorevole, con rilievi, sullo schema di decreto legislativo che recepisce in Italia la direttiva europea 2024/2831 sul lavoro mediante piattaforme digitali, con particolare attenzione alla situazione dei rider. Nel complesso, l'Autorità considera lo schema coerente con la direttiva europea e con la normativa nazionale di delega, chiede tuttavia alcune modifiche e propone diversi correttivi ([parere n. 624 del 17.09.2026](#)). L'obiettivo è rafforzare le tutele dei lavoratori e rendere più trasparente l'utilizzo dell'intelligenza artificiale e dei sistemi automatizzati, evitando sovrapposizioni tra le diverse autorità di controllo.

L'Autorità richiama, in particolare, l'esigenza di coordinare le nuove disposizioni con il Regolamento europeo sulla protezione dei dati e di definire in modo chiaro l'attribuzione delle competenze tra il Garante e l'Ispettorato nazionale del lavoro.

Il rischio, evidenzia il Garante, è che alcune violazioni previste dal decreto - dalla valutazione d'impatto sulla protezione dei dati alla trasparenza degli algoritmi, dalla supervisione umana alle misure di sicurezza - si sovrappongano a obblighi già previsti dal Gdpr e sanzionati dall'Autorità per la privacy. Si potrebbe così creare un doppio binario sanzionatorio per la medesima condotta.

Per evitarlo, il Garante propone di introdurre una clausola di assorbimento, basata sui principi di specialità e proporzionalità, oppure una clausola che coordini i procedimenti sanzionatori tra Ispettorato e Garante. Ulteriori osservazioni riguardano la condivisione delle informazioni con le autorità pubbliche, per la quale viene richiesta una disciplina più puntuale che definisca con maggiore precisione finalità dell'accesso, categorie di dati utilizzabili, ruoli delle amministrazioni e limiti al riutilizzo delle informazioni.

Recupero crediti: online la versione aggiornata del vademecum del Garante Stop a prassi invasive come sms o telefonate preregistrate



Online la nuova edizione del [vademecum](#) "Privacy e recupero crediti", una guida pratica per orientare imprese specializzate nel recupero crediti, banche, finanziarie, società telefoniche o energetiche verso il pieno rispetto dei diritti fondamentali dei cittadini, prevenendo trattamenti illeciti o lesivi della dignità della persona. Il documento del Garante privacy ribadisce – in linea con quanto stabilito dal GDPR – l'esigenza di un bilanciamento tra il legittimo interesse del creditore a recuperare le somme che gli sono dovute e la tutela della riservatezza del debitore.

Ma vediamo più nel dettaglio i principali chiarimenti contenuti nel vademecum.

La base giuridica e i limiti di competenza del Garante

Il trattamento dei dati personali per finalità di recupero crediti è legittimo anche senza il consenso del debitore, poiché si fonda sul legittimo interesse del titolare.

L'Autorità precisa, tuttavia, che il Garante non è competente sulle controversie relative alla sussistenza o all'ammontare del credito, per le quali i cittadini devono rivolgersi alle autorità di riferimento (esempio, Autorità giudiziaria ordinaria, Antitrust, Arera).

Le prassi illecite e lecite

Gli accertamenti del Garante hanno evidenziato il persistere di comportamenti invasivi. A tal riguardo, l'Autorità ricorda che è vietato esercitare indebite pressioni o comunicare lo stato di inadempimento a soggetti terzi. Sono illecite le visite a domicilio o sul lavoro che esponano la condizione del debitore, le telefonate di sollecito preregistrate senza operatore (che rischiano di essere ascoltate da terzi), l'affissione di avvisi di mora sulla porta di casa o nell'androne condominiale, e l'invio di posta con scritte esterne visibili quali "recupero crediti".

È invece consentito cercare il debitore (anche sul posto di lavoro), a patto di non fare alcun riferimento al debito. Le comunicazioni postali devono essere in plichi chiusi e prive di scritte riguardanti il recupero credito.

I dati che i soggetti incaricati possono trattare

I soggetti incaricati possono trattare i dati anagrafici, il codice fiscale, l'ammontare del credito e i recapiti forniti in sede contrattuale. Ma anche i dati acquisiti da database pubblici, registri o fonti terze autorizzate.

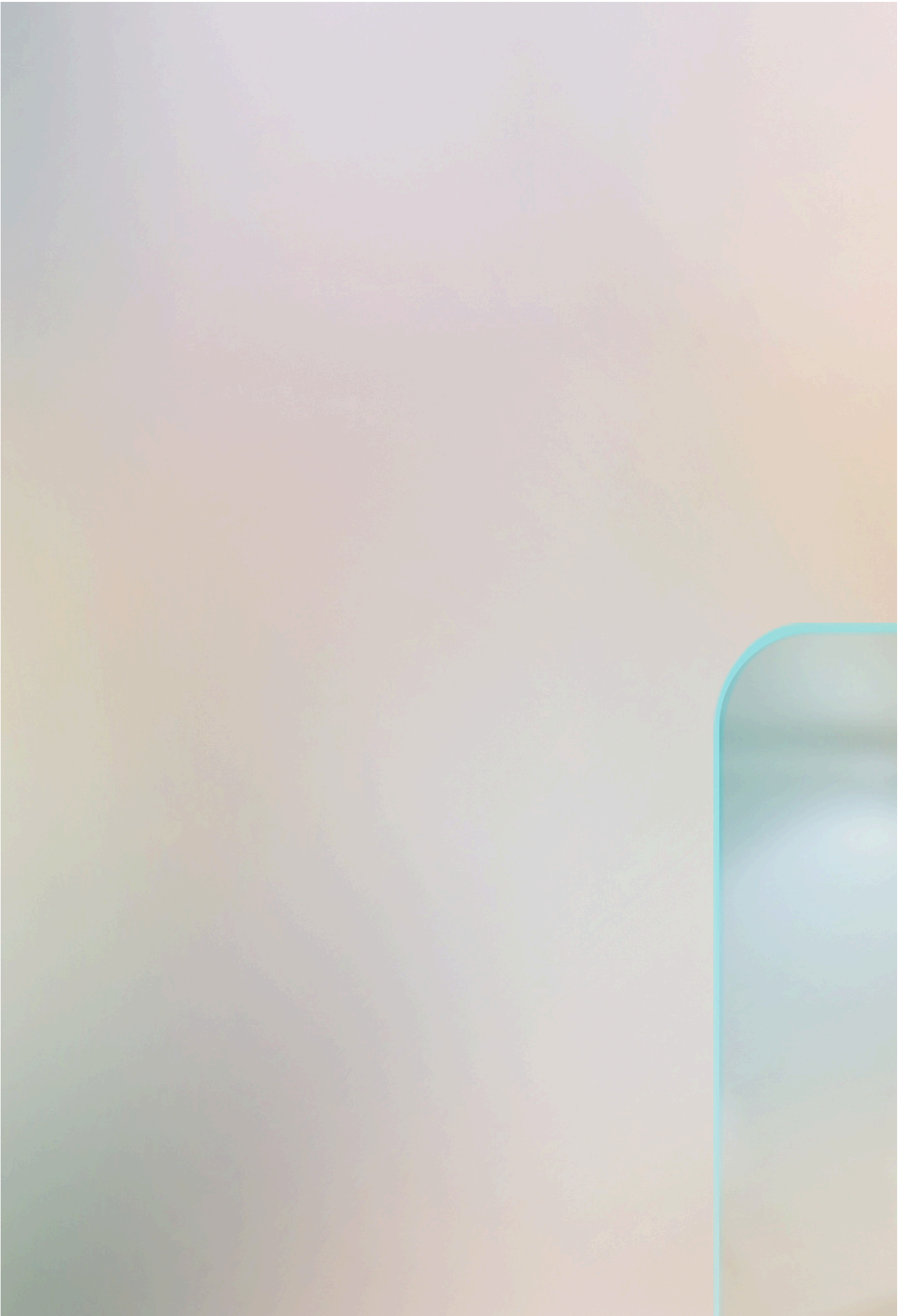
Accountability e obbligo di informativa

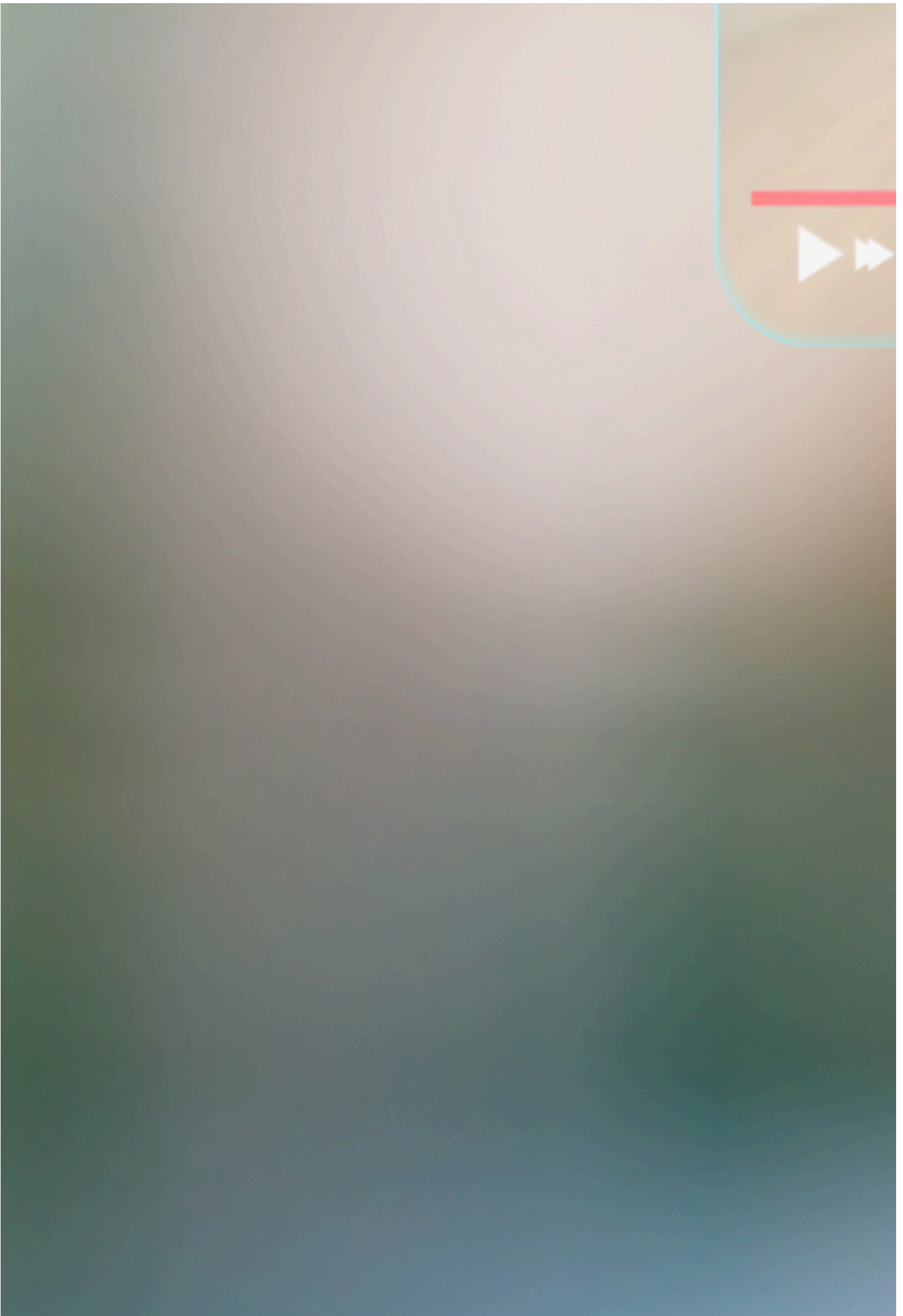
I creditori hanno l'obbligo di effettuare controlli periodici sull'operato delle agenzie esterne e devono fornire al debitore una chiara e dettagliata informativa privacy.

Il vademecum completo è disponibile sul [sito dell'Autorità](#).

Videosorveglianza, Garante privacy sanziona l'Istituto Nazionale di Ricerca Metrologica

L'attivazione delle telecamere deve rispettare gli accordi sindacali







Il Garante per la protezione dei dati personali ha comminato una sanzione di 10mila euro all'Istituto Nazionale di Ricerca Metrologica (INRIM) di Torino a seguito dei reclami di due dipendenti che lamentavano una violazione dei dati personali e dell'articolo 4 dello Statuto dei lavoratori in relazione all'impiego di un impianto di

videosorveglianza ([provvedimento](#) n.620 del 3.9.2026). L'impianto era stato installato per motivi di sicurezza e doveva riprendere solo i muri e le recinzioni.

Nel corso dell'istruttoria è emerso che l'Istituto, dopo aver stipulato un accordo con le organizzazioni sindacali, aveva installato l'impianto in maniera non conforme alla planimetria condivisa. Nello specifico, l'ente aveva aumentato di otto unità il numero di telecamere previste, modificandone la collocazione e le relative aree di

ripresa rispetto a quanto stabilito nell'accordo sindacale. L'INRIM aveva poi attivato – all'insaputa dei dipendenti, seppur per sole finalità di test – i dispositivi in alcune giornate, durante gli orari di apertura degli uffici dando così luogo a un trattamento illecito dei dati personali dei propri lavoratori e di tutti i soggetti che a vario titolo erano presenti in sede.

Contravvenendo al principio di "liceità, correttezza e trasparenza" previsto dal Regolamento europeo, l'Istituto non aveva inoltre fornito agli stessi un'informativa sul trattamento dei dati personali, essendo irrilevante che l'attivazione delle telecamere fosse avvenuta a soli fini di verifica tecnica e non avesse comportato la registrazione delle immagini. L'Istituto, infine, non aveva svolto una valutazione di impatto sulla protezione dei dati, prima di iniziare il trattamento, per tutelare i diritti e le libertà degli interessati.

Il ruolo del RDP al centro del nuovo episodio del podcast del Garante Privacy Disponibile sulle principali piattaforme

Il Garante per la protezione dei dati personali ha comminato una sanzione di 10mila euro all'Istituto Nazionale di Ricerca Metrologica (INRIM) di Torino a seguito dei reclami di due dipendenti che lamentavano una violazione dei dati personali e dell'articolo 4 dello Statuto dei lavoratori in relazione all'impiego di un impianto di videosorveglianza ([provvedimento](#) n.620 del 3.9.2026). L'impianto era stato installato per motivi di sicurezza e doveva riprendere solo i muri e le recinzioni.

Nel corso dell'istruttoria è emerso che l'Istituto, dopo aver stipulato un accordo con le organizzazioni sindacali, aveva installato l'impianto in maniera non conforme alla planimetria condivisa. Nello specifico, l'ente aveva aumentato di otto unità il numero di telecamere previste, modificandone la collocazione e le relative aree di ripresa rispetto a quanto stabilito nell'accordo sindacale. L'INRIM aveva poi attivato – all'insaputa dei dipendenti, seppur per sole finalità di test – i dispositivi in alcune giornate, durante gli orari di apertura degli uffici dando così luogo a un trattamento illecito dei dati personali dei propri lavoratori e di tutti i soggetti che a vario titolo erano presenti in sede.

Contravvenendo al principio di "liceità, correttezza e trasparenza" previsto dal Regolamento europeo, l'Istituto non aveva inoltre fornito agli stessi un'informativa sul trattamento dei dati personali, essendo irrilevante che l'attivazione delle telecamere fosse avvenuta a soli fini di verifica tecnica e non avesse comportato la registrazione delle immagini. L'Istituto, infine, non aveva svolto una valutazione di impatto sulla protezione dei dati, prima di iniziare il trattamento, per tutelare i diritti e le libertà degli interessati.

Sanzione di 403 milioni a Google, intervento del Garante privacy italiano con la Dpc irlandese Violati i dati di geolocalizzazione degli utenti

Google è stato condannato a una multa di 403 milioni di euro comminata dall'Autorità irlandese per la protezione dei dati, per aver violato le norme europee (Gdpr) sull'utilizzo dei dati di geolocalizzazione dei propri utenti.

Il provvedimento è frutto della collaborazione dell'Autorità italiana Garante della Privacy con la Commissione irlandese per la protezione dei dati (DPC), l'ente che vigila su Google a livello europeo poiché la sede della società Google Ireland Ltd. si trova a Dublino.

La Data Protection Commission (DPC) irlandese ha accolto integralmente le osservazioni formulate dal Garante italiano.

Le [osservazioni](#) dell'Autorità italiana, presentate nell'ambito del meccanismo di cooperazione previsto dal Gdpr tra l'autorità capofila irlandese e le altre autorità europee di protezione dei dati interessate, attraverso il sistema europeo IMI (Internal Market Information), hanno riguardato sia la qualificazione delle violazioni sia le misure correttive e i criteri per la determinazione delle sanzioni. In particolare, anche sulla base delle obiezioni del Garante italiano, la DPC ha riconosciuto nella decisione finale la violazione del principio di correttezza nel trattamento dei dati relativi agli spostamenti e alla posizione degli utenti raccolti attraverso le funzionalità Google "Web & App Activity" e "Location History", oltre alle violazioni già individuate in materia di liceità e trasparenza.

Sono state inoltre recepite le osservazioni dell'Autorità italiana relative alla durata e alla gravità delle violazioni, alla natura dei dati trattati e alle misure correttive da adottare. L'esito del procedimento conferma l'efficacia del meccanismo di cooperazione tra le autorità europee previsto dal Gdpr nel garantire un'applicazione coerente della normativa europea sulla protezione dei dati personali.

Intervento del 28.09.2026

L'Autorità Garante per la privacy e il caso Revolut

Sul caso Revolut si è mossa prontamente l'Autorità Garante della Privacy. È partita una [verifica](#) immediata su eventuali falle nella sicurezza degli accessi delle banche italiane. Sia per appurare se vi siano stati altri casi di tentata infiltrazione - come nella vicenda Revolut - sia per richiamare gli istituti bancari a un controllo efficace al proprio interno.

Dagli uffici dell'Autorità è partita una comunicazione alla rete dei responsabili di protezione dati (Dpo) degli istituti bancari invitandoli ad una solerte verifica interna sui propri sistemi e, nel caso di falle accertate, a prendere subito contatto con l'Autorità.

Sul tema degli accessi abusivi ai conti correnti, già da mesi sta lavorando una task force Autorità-banche per rafforzare le misure di sicurezza.

Considerato che le modalità utilizzate per l'acquisizione illecita di dati personali risultano particolarmente insidiose e non si può escludere a priori che siano stati fatti tentativi analoghi anche nei confronti di altri istituti di credito, l'Autorità ha chiesto agli istituti bancari di avviare una verifica all'interno dei sistemi per escludere l'eventuale presenza di comunicazioni "anomale" provenienti dalla stessa casella pec ed effettuare gli opportuni approfondimenti. Se dovessero emergere situazioni simili a quelle del caso Revolut, banche e istituti finanziari sono chiamati ad adottare tempestivamente le misure per attenuare i possibili effetti negativi per gli interessati e informare l'Autorità, ai sensi degli artt. 33 del Regolamento.

L'Autorità Garante si è fatta promotrice di un'azione con l'Autorità omologa lituana (dove si trova la sede legale principale di Revolut), fornendo le informazioni in possesso del Garante italiano, e invitando ad uno scambio reciproco, così da rafforzare l'azione di contrasto.

Inoltre, l'Autorità si è mossa sul fronte del Ministero degli Interni per inquadrare più approfonditamente la vicenda Revolut e appurare se vi siano altre banche o istituti finanziari coinvolti, circoscrivendo il danno avvenuto facendo emergere quanti e quali dati siano stati compromessi.

La vicenda, infatti, ha evidenziato alcuni lati deboli delle Pec ufficiali in uso, e su questo occorrerà lavorare approfonditamente.

Intervento del 18.09.2026

La Cassazione conferma la correttezza dell'operato del Garante privacy

La Suprema Corte dà ragione all'Autorità sia sui tempi del procedimento, sia nel merito

La Corte di Cassazione ha confermato la legittimità dell'azione del Garante per la protezione dei dati personali respingendo, con le sentenze nn. 24861/2026 e 22791/2026, i ricorsi proposti avverso le [sanzioni amministrative pecuniarie](#) irrogate dall'Autorità - rispettivamente di 20.000 euro alla Società Editoriale Il Fatto S.p.A. e di 2.000 euro a Chiarelettere S.r.l. (oggi incorporata in Garzanti S.r.l.) - per la pubblicazione di un articolo, successivamente ripreso in un libro, contenente informazioni idonee a rendere identificabili i figli di una persona coinvolta in una vicenda giudiziaria.

Sul piano procedurale, la Suprema Corte ha chiarito che il procedimento avviato a seguito di un reclamo e quello volto all'eventuale applicazione di una sanzione amministrativa sono autonomi e distinti. Il termine previsto dall'articolo 143, comma 3, del Codice in materia di protezione dei dati personali per la decisione sul reclamo è posto a tutela del diritto del reclamante a ottenere una risposta in tempi ragionevoli: il suo superamento, pertanto, non determina la decadenza del potere sanzionatorio del Garante, che resta soggetto ai soli termini, previsti dalla legge n. 689 del 1981, per la contestazione della violazione e per la prescrizione quinquennale - termini che, nei casi esaminati, risultavano rispettati.

Anche nel merito i ricorsi sono stati respinti.

La Cassazione ha condiviso la valutazione già compiuta dai giudici di primo grado (Tribunale di Roma e Tribunale di Milano), secondo cui la pubblicazione dei nomi dei figli, unitamente al titolo di studio e all'attività professionale svolta, ha ecceduto il limite dell'essenzialità dell'informazione rispetto ai fatti di interesse pubblico narrati, trattandosi di soggetti privi di notorietà pubblica e non protagonisti della vicenda giudiziaria oggetto della narrazione.

Le due pronunce ribadiscono un principio cardine dell'attività di vigilanza dell'Autorità: l'interesse pubblico alla conoscenza di una vicenda giudiziaria non giustifica la diffusione di informazioni ulteriori rispetto a quelle effettivamente essenziali per comprenderla, specialmente quando i dati diffusi riguardano soggetti terzi, estranei ai fatti narrati. Il Garante prosegue nella propria attività di bilanciamento tra il diritto di cronaca e di informazione, da un lato, e la tutela della riservatezza delle persone coinvolte, anche indirettamente, in vicende giudiziarie altrui, dall'altro.

Intervento del 14.09.2026

L'ATTIVITÀ DEL GARANTE - PER CHI VUOLE SAPERNE DI PIÙ

Gli interventi e i provvedimenti più importanti recentemente adottati dall'Autorità

- Dal Garante privacy stop ai deepfake satirici su Enrico Mentana. Ammonita R.T.I. per alcuni video di Striscia la Notizia - [Comunicato del 7.8.2026](#)
- Telemarketing, il Garante privacy sanziona Tim per 9,5 milioni di euro
Consensi acquisiti illecitamente, inadeguati controlli sulla filiera e ostacoli all'esercizio dei diritti degli utenti - [Comunicato del 31.7.2026](#)

NEWSLETTER del Garante per la protezione dei dati personali (Reg. al Trib. di Roma n. 654 del 28 novembre 2002)

Direttore responsabile: Stefano Sabella

Direzione e redazione: Garante per la protezione dei dati personali, Piazza Venezia, n. 11 - 00187 Roma.

Tel: 06.69677.2751 - Fax: 06.69677.3785

Newsletter è consultabile sul sito Internet www.gpdp.it