FIVERS

# Aggiornamento
# Data protection, AI, IT and IP

**n. 20/2026**

## DATA PROTECTION

**9 novembre 2026 - Garante privacy: cancellare i dati non rimedia al silenzio verso l'interessato**

---

**5 Novembre 2026 - Corte di giustizia UE: il fascicolo di un reclamo privacy non è «inaccessibile» ai dati del reclamante.**

---

**3 Novembre 2026 - Garante privacy: scaduto il termine di adeguamento per i tracking pixel nelle e-mail.**

---

**1° Novembre 2026 – Comitato europeo per la protezione dei dati personali: chiuse le consultazioni pubbliche sull'anonimizzazione e sul web scraping nell'IA generativa.**

---

## INTELLIGENZA ARTIFICIALE

**11 Novembre 2026 – Commissione europea: Digital Fairness Act, nuove regole per agenti di IA, chatbot, contratti digitali e pratiche commerciali manipolative.**

---

**9 Novembre 2026 – AgID: pubblicate le Linee Guida definitive sull'intelligenza artificiale nella PA. Obblighi di governance, gestione dei rischi, protezione dei dati e controlli sui sistemi adottati.**

---

**3 Novembre 2026 - Avvocato generale della Corte di giustizia UE: quando un chatbot usa articoli di stampa per rispondere agli utenti può incidere sui diritti degli editori.**

---

## CYBERSICUREZZA

**6 novembre 2026 – Dipartimento per la trasformazione digitale: adottate le specifiche tecniche per sperimentare l'IT-Wallet.**

---

**25 Ottobre 2026 – Agenzia Nazionale per la Cybersicurezza - ACN: registrazione NIS 2027 semplificata per i soggetti già iscritti, ma solo se i dati non sono cambiati.**

---

## INFORMATION TECHNOLOGY

**10 novembre 2026 - TAR Campania, Salerno: nelle gare telematiche il caricamento dei documenti non basta a presentare l'offerta.**

## MERCATI DIGITALI

**5 Novembre 2026 - Corte di giustizia UE: lo smart meter non è facoltativo per il solo fatto che il cliente preferisce un contatore tradizionale.**

## PROPRIETA' INTELLETTUALE E INDUSTRIALE

**4 novembre 2026 – Tribunale UE: nei marchi brevi non basta una parola comune per dimostrare il rischio di confusione.**

## DATA PROTECTION

### 9 novembre 2026 - Garante privacy: cancellare i dati non rimedia al silenzio verso l'interessato

Un'università ha rimosso dal proprio sito i dati di un ex studente contenuti in un elenco elettorale, ma non aveva risposto alla sua richiesta di cancellazione. Aveva inoltre lasciato senza riscontro due successivi inviti del Garante, comunicando l'avvenuta rimozione soltanto dopo l'avvio del procedimento sanzionatorio. L'Autorità ha accertato la violazione degli artt. 5, 12 e 17 GDPR e irrogato all'Università una sanzione di 4.000 euro.

La decisione mette in evidenza due adempimenti distinti. Il titolare deve valutare e, quando ne ricorrono i presupposti, eseguire la richiesta di cancellazione; deve anche comunicare all'interessato che cosa ha fatto, senza ingiustificato ritardo e comunque entro un mese dalla ricezione dell'istanza. Se non può accoglierla, deve spiegare il motivo e indicare la possibilità di rivolgersi al Garante o al giudice. Nei casi previsti dal GDPR, il termine può essere prorogato, ma l'interessato deve esserne informato entro il primo mese. La rimozione successiva dei dati non elimina la violazione già maturata per il mancato riscontro.

Per imprese e PA, il caso suggerisce di trattare ogni istanza privacy come un procedimento tracciabile: registrare la data di ricezione, assegnare un responsabile della risposta, verificare l'esito dell'intervento tecnico e conservare prova sia dell'azione compiuta sia della comunicazione inviata all'interessato. Occorre inoltre presidiare separatamente le richieste dell'Autorità: nel caso esaminato, la mancata collaborazione è stata considerata dal Garante nella determinazione della sanzione**.**

---

### 5 Novembre 2026 - Corte di giustizia UE: il fascicolo di un reclamo privacy non è «inaccessibile» ai dati del reclamante.

Una persona presenta un reclamo all'autorità privacy e chiede successivamente di conoscere i propri dati personali contenuti nel relativo fascicolo. L'autorità può respingere la richiesta invocando una norma che esclude, in blocco, l'accesso ai suoi fascicoli? Nella causa *Bayerisches Landesamt für Datenschutzaufsicht* (C-205/25), la Corte di giustizia ha risposto di no. Quando tratta i dati raccolti e prodotti nell'ambito del reclamo, l'autorità di controllo è essa stessa titolare del trattamento: il reclamante può quindi esercitare nei suoi confronti, in linea di principio, il diritto di accesso dell'articolo 15 GDPR.

La sentenza distingue però con precisione accesso ai dati personali e accesso indistinto all'intero fascicolo amministrativo. Il primo è tutelato dal GDPR; il secondo non discende automaticamente dall'articolo 15. L'autorità deve valutare quali informazioni riguardino effettivamente il richiedente e contemperare la richiesta con i diritti e le libertà di altre persone. Ove possibile, l'oscuramento o l'anonimizzazione dei dati di terzi consentono di fornire le informazioni dovute senza divulgare quelle da proteggere. L'articolo 23 GDPR permette limitazioni legislative al diritto di accesso solo entro i suoi rigorosi presupposti: non giustifica un'esclusione generalizzata di tutti i dati personali presenti nei fascicoli dell'autorità.

Sul piano operativo, la pronuncia interessa anzitutto le autorità di controllo, che devono poter esaminare queste istanze individualmente e motivare le eventuali limitazioni. È rilevante anche per le imprese coinvolte nelle istruttorie: documenti, risposte e allegati inviati all'autorità possono contenere dati del reclamante insieme a informazioni di terzi o riservate. Conviene identificarli con accuratezza fin dalla trasmissione, così che le esigenze di tutela possano essere valutate concretamente, senza presumere che la collocazione nel fascicolo renda tutto automaticamente ostensibile o, all'opposto, tutto segreto.

Corte di giustizia UE, sentenza 5 Novembre 2026, C-205/25, ECLI:EU:C:2026:933.

---

**3 Novembre 2026 - Garante privacy: scaduto il termine di adeguamento per i tracking pixel nelle e-mail.**

Il 29 ottobre è scaduto il termine di sei mesi, decorrente dalla pubblicazione in Gazzetta Ufficiale del 29 aprile 2026, che il Garante aveva concesso per adeguarsi alle linee guida sui tracking pixel nelle comunicazioni di posta elettronica. Le linee guida erano state adottate con provvedimento n. 284 del 17 aprile 2026: non sono un nuovo atto emanato a ottobre, ma la scadenza rende attuale la verifica delle campagne già operative.

I pixel possono rivelare l'apertura di un messaggio e, a seconda della configurazione, raccogliere ulteriori informazioni sul destinatario. Le indicazioni del Garante riguardano anche newsletter, messaggi automatici e comunicazioni di servizio, non soltanto le e-mail pubblicitarie. Il destinatario deve essere informato preventivamente della presenza del tracciamento e delle sue finalità. Per la misurazione *individuale* delle aperture utilizzata, ad esempio, per valutare campagne promozionali, adattare la frequenza dei messaggi o costruire profili commerciali, le linee guida richiedono in via generale il consenso preventivo. Il Garante contempla però deroghe da valutare concretamente, fra cui statistiche solo aggregate e anonime, determinate esigenze di sicurezza e specifiche comunicazioni istituzionali o di servizio.

La verifica per imprese e PA dovrebbe partire dalla piattaforma effettivamente usata: quali pixel sono attivi per impostazione predefinita, quali dati producono, se misurano il singolo destinatario e chi vi accede. Occorre poi allineare informativa, raccolta e prova del consenso, istruzioni al fornitore e sistemi di revoca. Il Garante ammette, a certe condizioni, un unico consenso informato per messaggi promozionali e relativo tracciamento, ma richiede che l'utente possa successivamente revocare anche il solo tracciamento, continuando a ricevere e-mail prive di pixel. Per i trattamenti preesistenti le linee guida prevedono specifiche modalità transitorie, da non confondere con una dispensa permanente dagli adempimenti.

Garante privacy, linee guida del 17 aprile 2026, pubblicate nella GU del 29 aprile 2026.

---

**1° Novembre 2026 – Comitato europeo per la protezione dei dati personali: chiuse le consultazioni pubbliche sull'anonimizzazione e sul web scraping nell'IA generativa.**

Si è chiusa la consultazione pubblica sugli orientamenti EDPB 02/2026 in materia di anonimizzazione, adottati in luglio in versione sottoposta a consultazione. Il tema è rilevante per chi condivide dataset, pubblica statistiche, alimenta ambienti di ricerca o riutilizza dati per sviluppare sistemi di IA: qualificare un insieme di informazioni come "anonimo" significa sostenere che le persone non siano identificabili secondo il criterio giuridico applicabile, non semplicemente che nomi e codici fiscali siano stati rimossi.

Nella bozza, l'EDPB propone di esaminare la possibilità di identificazione anche dal punto di vista dei soggetti che potrebbero disporre dei dati e dei mezzi ragionevolmente utilizzabili per combinarli con altre informazioni. Il quadro di valutazione considera tre rischi: isolare la registrazione relativa a una persona, collegarla ad altri dati e ricavare informazioni su di lei mediante inferenza. Se uno di questi profili resta aperto, serve un'analisi ulteriore prima di dichiarare riuscita l'anonimizzazione.

Sul piano operativo, imprese e PA dovrebbero documentare quale dataset è stato valutato, in quale contesto sarà messo a disposizione e quali soggetti potrebbero accedervi, riesaminando la conclusione se cambiano dati, destinatari o tecniche disponibili. La chiusura della consultazione, tuttavia, non rende definitiva la bozza e non introduce il 30 ottobre una nuova soglia normativa: occorre attendere l'eventuale versione finale dell'EDPB.

E' terminata anche la consultazione sugli orientamenti EDPB 03/2026 dedicati alla raccolta automatizzata di dati dal web per lo sviluppo dell'IA generativa. La bozza, pubblicata in luglio, affronta una questione pratica per sviluppatori, committenti e fornitori di modelli: la disponibilità di dati su pagine accessibili al pubblico non elimina l'applicazione del GDPR quando la raccolta, la conservazione o l'utilizzo riguardano dati personali.

L'EDPB richiama in particolare la necessità di definire le finalità della raccolta, individuare una base giuridica, rispettare trasparenza e minimizzazione e verificare l'accuratezza dei dati destinati all'addestramento. La bozza discute le condizioni per valutare l'interesse legittimo, senza considerarlo una base automaticamente disponibile per qualsiasi scraping. Se la raccolta coinvolge categorie particolari di dati, occorre inoltre esaminare separatamente una condizione dell'articolo 9 GDPR: non esiste un'esenzione generale per i dati sensibili che compaiono incidentalmente sul web.

Per le organizzazioni che sviluppano o acquistano soluzioni di IA, la conseguenza operativa è chiedere una ricostruzione verificabile delle fonti dei dati, dei criteri di selezione, dei filtri applicati, dei controlli di qualità e delle misure per gestire dati eccedenti o sensibili. La chiusura della consultazione non equivale all'adozione finale degli orientamenti; la bozza resta un riferimento per anticipare le questioni che l'EDPB sta esaminando, non una nuova disciplina entrata in vigore il 30 ottobre.

consultazione EDPB sugli orientamenti 02/2026 e comunicazione EDPB dell'8 luglio 2026. European Data Protection Board

consultazione EDPB sugli orientamenti 03/2026 e comunicazione EDPB dell'8 luglio 2026.

---

## INTELLIGENZA ARTIFICIALE

**11 Novembre 2026 – Commissione europea: Digital Fairness Act, nuove regole per agenti di IA, chatbot, contratti digitali e pratiche commerciali manipolative.**

L'11 Novembre 2026 la Commissione europea ha presentato la proposta di Regolamento *Digital Fairness Act* (COM(2026) 1100 final), destinata a rafforzare la tutela dei consumatori nei mercati digitali e a contrastare le pratiche commerciali che ne condizionano indebitamente le decisioni. L'intervento propone di sostituire la Direttiva 2005/29/CE sulle pratiche commerciali sleali con un Regolamento direttamente applicabile negli Stati membri, conservandone i principi fondamentali e introducendo nuove disposizioni per affrontare i rischi derivanti dalla personalizzazione algoritmica, dalle interfacce digitali e dall'impiego dell'intelligenza artificiale nei rapporti con i consumatori.

Una delle principali novità riguarda il divieto dei cosiddetti *dark patterns*, vale a dire le tecniche di progettazione delle interfacce che inducono gli utenti ad assumere decisioni commerciali non pienamente libere e consapevoli. La proposta vieta, tra l'altro, i messaggi ingannevoli sulla disponibilità dei prodotti, le pressioni artificiali all'acquisto e altre forme di manipolazione delle scelte. Introduce inoltre un principio di *fairness by design*, che comprende la possibilità di disattivare funzionalità progettate per incentivare un utilizzo eccessivo o compulsivo dei servizi digitali. Tale previsione interessa anche i chatbot e gli assistenti di IA che simulano relazioni interpersonali per prolungare le interazioni con gli utenti.

Particolarmente innovative sono le disposizioni dedicate agli agenti di IA in grado di selezionare prodotti, negoziare condizioni e concludere autonomamente contratti per conto dei consumatori. La proposta prevede che gli utenti possano stabilire preventivamente se confermare tutte le operazioni, soltanto determinate categorie di acquisti oppure autorizzare l'agente a operare senza conferme preventive. Dovranno poter essere definiti e modificati parametri quali importi massimi e limiti temporali. Sono inoltre previsti obblighi di trasparenza su remunerazioni e conflitti d'interesse, con necessità di conferma del consumatore nei casi indicati dalla proposta. La disciplina introduce così specifiche garanzie per il commercio automatizzato, pur prevedendo un'esclusione per i servizi finanziari.

Nuove tutele riguardano anche i servizi di assistenza automatizzata e i contratti digitali. Quando l'assistenza postcontrattuale viene fornita online, il consumatore potrà richiedere di comunicare con un operatore umano qualora gli altri strumenti non risultino efficaci, secondo le condizioni e le eccezioni previste dalla proposta. Vengono inoltre introdotte misure contro gli abbonamenti difficili da disdire, i rinnovi automatici poco trasparenti e la trasformazione delle prove gratuite in servizi a pagamento senza un consenso espresso. Ulteriori disposizioni interessano il marketing degli influencer, la pubblicità personalizzata rivolta ai minori, lo sfruttamento delle vulnerabilità dei consumatori e la trasparenza dei prezzi, anche quando determinati da sistemi algoritmici.

Rilevanti sono anche i nuovi strumenti di controllo e accertamento delle violazioni. L'articolo 34 della proposta consentirebbe alle autorità competenti e ai giudici, in presenza delle condizioni previste, di richiedere alle imprese evidenze sulla progettazione, sul funzionamento e sugli effetti delle pratiche commerciali digitali sui comportamenti dei consumatori, nel rispetto dei principi di necessità e proporzionalità e della tutela dei segreti commerciali. La parallela revisione del Regolamento sulla cooperazione per la tutela dei consumatori attribuirebbe inoltre alla Commissione europea poteri diretti di indagine e sanzione per determinate violazioni transfrontaliere, con sanzioni fino al 6% del fatturato mondiale annuo.

Per le imprese che operano nell'e-commerce, nei servizi digitali e nello sviluppo di soluzioni di IA, la proposta rende opportuno avviare una verifica dei processi commerciali automatizzati, delle modalità di utilizzo dei chatbot, dei sistemi di raccomandazione e personalizzazione, dei meccanismi di acquisto e rinnovo contrattuale e della documentazione disponibile per dimostrarne la correttezza. Il Digital Fairness Act non modifica direttamente l'AI Act, ma ne completa il quadro di tutela sul versante delle pratiche commerciali, affiancandosi anche al GDPR e al Digital Services Act. Le disposizioni sono ancora oggetto di proposta legislativa e diventeranno applicabili soltanto dopo l'eventuale approvazione definitiva da parte del Parlamento europeo e del Consiglio, secondo il calendario che sarà stabilito dal testo adottato.

Commissione europea – Digital Fairness Act, proposta COM(2026) 1100 final dell'11 Novembre 2026.

---

**9 Novembre 2026 – AgID: pubblicate le Linee Guida definitive sull'intelligenza artificiale nella PA. Obblighi di governance, gestione dei rischi, protezione dei dati e controlli sui sistemi adottati.**

Con la Determinazione n. 169 del 9 Novembre 2026, l'Agenzia per l'Italia Digitale (AgID) ha adottato le Linee Guida definitive per l'adozione dell'intelligenza artificiale nella Pubblica Amministrazione, emanate secondo la procedura prevista dall'articolo 71 del Codice dell'Amministrazione Digitale e nell'ambito del Piano Triennale per l'Informatica nella PA 2024-2026.

Il documento introduce un quadro organico di prescrizioni organizzative, tecniche e di conformità normativa che le amministrazioni devono considerare nell'introduzione e nell'utilizzo dei sistemi di IA, anche quando acquisiti da fornitori esterni.

Le Linee Guida richiedono innanzitutto alle amministrazioni di definire una strategia per l'IA, coerente con le proprie funzioni istituzionali, con il Piano integrato di attività e organizzazione (PIAO) e con la strategia di governo dei dati. La strategia deve individuare obiettivi, ambiti di applicazione, risorse e misure di trasparenza. Ogni progetto deve inoltre essere accompagnato dall'identificazione dei requisiti, dalla valutazione dei rischi e dalla definizione di indicatori per misurare efficacia, affidabilità e impatto organizzativo dei sistemi. L'impostazione segue un modello di miglioramento continuo, ispirato al ciclo *Plan-Do-Check-Act* e allo standard ISO/IEC 42001, da applicare in modo proporzionato alle caratteristiche e alla complessità delle soluzioni adottate.

Sul piano delle responsabilità, il coordinamento della governance dell'IA è affidato al Responsabile per la Transizione Digitale (RTD) e al relativo Ufficio, con il coinvolgimento del Responsabile della protezione dei dati (RPD) e dei referenti per la cybersicurezza. Le amministrazioni caratterizzate da un utilizzo particolarmente intenso dell'IA possono inoltre individuare un Responsabile dell'Intelligenza Artificiale dedicato. È richiesta l'adozione di procedure per disciplinare lo sviluppo, l'impiego e il monitoraggio dei sistemi, mentre la predisposizione di uno specifico codice etico e di condotta costituisce una misura facoltativa, sebbene raccomandata.

Particolare rilievo assumono gli adempimenti in materia di protezione dei dati personali, sicurezza informatica e tutela dei diritti fondamentali. Le amministrazioni devono verificare la liceità dei trattamenti, la qualità e la provenienza dei dati, le modalità di utilizzo delle informazioni personali e gli eventuali trasferimenti verso Paesi terzi. Devono inoltre effettuare le valutazioni d'impatto richieste dal GDPR e, nei casi previsti dall'AI Act, quelle sui diritti fondamentali, assicurando adeguati meccanismi di sorveglianza umana. La sicurezza deve comprendere anche i rischi specifici dell'IA, quali la manipolazione dei dati di addestramento, gli attacchi ai modelli e l'estrazione non autorizzata di informazioni.

Le implicazioni operative riguardano direttamente anche le imprese che sviluppano o forniscono sistemi di IA alle pubbliche amministrazioni. Gli enti dovranno poter acquisire e verificare la documentazione tecnica, le caratteristiche di sicurezza, le modalità di funzionamento e le evidenze necessarie a dimostrare la conformità delle soluzioni, anche attraverso controlli successivi alla loro introduzione. Per amministrazioni e fornitori diventa quindi essenziale definire con chiarezza responsabilità, requisiti di sicurezza, modalità di sorveglianza, obblighi informativi e strumenti di verifica lungo l'intero ciclo di vita dei sistemi.

Le Linee Guida distinguono espressamente tra requisiti obbligatori, divieti e raccomandazioni. La loro adozione rappresenta pertanto un passaggio rilevante verso una governance dell'IA nella PA strutturata, documentabile e sottoposta a verifiche continuative, destinata a incidere tanto sull'organizzazione interna quanto sulle modalità di acquisizione e gestione delle tecnologie.

AgID – Determinazione n. 169/2026 e Linee Guida definitive per l'adozione di IA nella Pubblica Amministrazione.

---

**3 Novembre 2026 - Avvocato generale della Corte di giustizia UE: quando un chatbot usa articoli di stampa per rispondere agli utenti può incidere sui diritti degli editori.**

Nelle conclusioni presentate nella causa *Like Company contro Google Ireland* (C-250/25), l'avvocato generale Maciej Szpunar affronta l'uso di articoli giornalistici da parte di chatbot come Gemini. Il punto centrale è la generazione di risposte mediante *retrieval-augmented generation* (RAG): il sistema recupera una pubblicazione online in tempo reale e la utilizza per rispondere alla domanda dell'utente. Questa attività va distinta dall'addestramento precedente del modello. Sulle due questioni relative all'addestramento, l'avvocato generale propone infatti alla Corte di non pronunciarsi, ritenendole ipotetiche nel caso concreto perché non risulta provato che gli articoli dell'editore siano stati utilizzati a tale scopo. Le osservazioni che dedica comunque all'eccezione per il *text and data mining* non costituiscono, quindi, la soluzione proposta per la controversia.

Quanto alle risposte del chatbot, Szpunar richiama il diritto connesso riconosciuto agli editori dall'articolo 15 della direttiva (UE) 2019/790. Propone di valutare, tra l'altro, come il sistema abbia avuto accesso all'articolo — in particolare se abbia aggirato un paywall o altre misure tecniche efficaci — e che cosa compaia nella risposta. Il diritto dell'editore non attribuisce un monopolio sui fatti di cronaca: una risposta che riferisca gli stessi fatti con una formulazione autonoma non equivale, per ciò solo, alla riproduzione dell'articolo. Diversa è l'ipotesi in cui la forma espressiva della pubblicazione sia riconoscibile nella risposta al punto da rendere superflua, per l'utente, la lettura della fonte. L'avvocato generale esamina inoltre la possibile responsabilità del fornitore quando tali utilizzi siano inerenti alla sua strategia commerciale o non siano contrastati con misure adeguate ed efficaci. Non conclude, però, che l'esempio prodotto da Like Company dimostri già una violazione: rimette gli accertamenti sul caso al giudice nazionale.

Per gli editori, la questione rende importante documentare le misure di controllo dell'accesso ai contenuti e conservare esempi verificabili delle risposte generate dai servizi di IA, confrontandole con gli articoli originali. Per i fornitori di chatbot, richiama l'attenzione sulle regole impartite ai sistemi di recupero delle fonti, sui filtri delle risposte e, dove necessario, sugli accordi di licenza. Non basta però constatare che una risposta riduca il traffico verso un giornale per dedurne automaticamente una violazione del diritto connesso: secondo l'impostazione proposta, occorre verificare le concrete modalità di accesso e di riutilizzo della pubblicazione.

Stato: conclusioni dell'avvocato generale, presentate il 3 novembre 2026 e non vincolanti. La Corte di giustizia deve ancora pronunciarsi.

testo delle conclusioni, C-250/25, ECLI:EU:C:2026:919 e comunicato della Corte n. 155/26 del 3 novembre 2026.

---

## CYBERSICUREZZA

**6 novembre 2026 – Dipartimento per la trasformazione digitale: adottate le specifiche tecniche per sperimentare l'IT-Wallet.**

La Presidenza del Consiglio ha reso pubblico il decreto del Capo del Dipartimento per la trasformazione digitale che adotta le specifiche tecniche del Sistema IT-Wallet per la fase di sperimentazione. Il provvedimento dà attuazione al quadro fissato dal decreto del 17 giugno 2026: le linee guida definiscono l'impianto del sistema, mentre le specifiche costituiscono il riferimento di dettaglio per sviluppare e verificare le soluzioni dei partecipanti.

Per imprese e pubbliche amministrazioni interessate a emettere attestati elettronici, offrire portafogli digitali o verificarne il contenuto, il passaggio è operativo. Occorre individuare il ruolo che si intende assumere e confrontare architettura, interoperabilità, sicurezza e trattamento dei dati con le specifiche applicabili prima di avviare l'integrazione e i test. La documentazione tecnica è pubblicata dal Dipartimento in un repository aperto, destinato a evolvere anche alla luce dei risultati della sperimentazione: chi sviluppa soluzioni dovrà quindi controllarne gli aggiornamenti e distinguere la versione formalmente adottata dai successivi lavori in corso.

L'adozione delle specifiche non equivale all'apertura indiscriminata di tutti i servizi IT-Wallet al pubblico. Regola, in questa fase, il percorso tecnico dei soggetti che partecipano alla sperimentazione.

Parallelamente AgID ha definito le regole per registrarsi all'IT-Wallet e proporre nuovi casi d'uso. Con la determinazione n. 164 del 23 ottobre 2026, pubblicata lo stesso giorno, AgID ha adottato la versione 1.0 del regolamento sulla registrazione al Sistema IT-Wallet e sulla partecipazione allo Spazio di Sperimentazione. Il testo distingue i ruoli dei partecipanti — tra cui fornitori di portafogli privati e di attestati, soggetti che verificano gli attestati, aggregatori e titolari di fonti autentiche — e stabilisce documenti e requisiti da presentare in funzione dell'attività prevista.

In attesa che il portale di *onboarding* sia pienamente operativo, la domanda si presenta con il modulo allegato al regolamento, firmato digitalmente o con firma elettronica qualificata dal legale rappresentante e inviato via PEC ad AgID. L'istruttoria valuta i requisiti amministrativi, organizzativi e tecnici; se entro 90 giorni non viene comunicato un diniego, la domanda si considera accolta con riserva. Questo passaggio non va confuso con l'iscrizione effettiva nel Registro IT-Wallet, che richiede il superamento delle verifiche e dei test tecnici.

Lo Spazio di Sperimentazione consente ai soggetti registrati di validare e integrare le proprie soluzioni. Un progetto di sperimentazione distinto, da sottoporre ad AgID, è necessario quando si vogliono provare funzionalità, servizi o casi d'uso non ancora contemplati dalle regole o dalle specifiche. Per le imprese e le PA interessate, la prima attività è dunque scegliere il ruolo, predisporre la documentazione corrispondente e valutare se il proprio caso d'uso richieda anche l'ammissione di un progetto. La partecipazione è volontaria e non attribuisce, di per sé, un diritto a finanziamenti o alla prosecuzione del servizio nell'esercizio ordinario.

determinazione AgID e regolamento allegato; comunicato AgID.

pubblicazione della Presidenza del Consiglio; pagina del progetto e documentazione tecnica del Dipartimento; decreto 17 giugno 2026 nella Gazzetta Ufficiale.

---

**25 Ottobre 2026 – Agenzia Nazionale per la Cybersicurezza - ACN: registrazione NIS 2027 semplificata per i soggetti già iscritti, ma solo se i dati non sono cambiati.**

Dal 25 ottobre si applica la determinazione ACN n. 314287/2026, adottata il 20 ottobre per aggiornare le procedure di utilizzo della piattaforma NIS. La novità più immediata riguarda la campagna di registrazione 2027: secondo la comunicazione dell'Agenzia, i soggetti già presenti nell'elenco NIS non devono presentare una nuova dichiarazione se non hanno modifiche da comunicare rispetto alle informazioni già trasmesse. L'ACN ha inoltre aggiornato le FAQ sulla registrazione e ha annunciato che, dal 31 ottobre 2026,

non sarebbe più stato possibile inviare dichiarazioni tardive relative alla precedente campagna, per consentire l'adeguamento della piattaforma.

La semplificazione non equivale a un esonero dai controlli interni. Prima di avvalersene, imprese e PA interessate dovrebbero confrontare la dichiarazione precedente con la situazione attuale: perimetro delle attività e dei servizi, dati organizzativi, referenti e altre informazioni comunicate all'Agenzia. Se nel frattempo sono intervenute variazioni, occorre valutare gli adempimenti di aggiornamento previsti dalla disciplina NIS. È utile assegnare questa verifica a un responsabile interno e conservarne l'esito: l'assenza di una nuova dichiarazione deve dipendere dall'assenza effettiva di modifiche, non da una mancata ricognizione.
La determinazione aggiorna le procedure della piattaforma; non va confusa con gli atti ACN che disciplinano le misure di sicurezza richieste ai soggetti NIS. Prima dell'invio della newsletter suggerisco una verifica finale del PDF dell'atto: il sito ACN non ne ha consentito l'apertura integrale durante questo controllo, e questa notizia è quindi circoscritta ai punti confermati dalla comunicazione pubblica dell'Agenzia.

comunicazione ACN sulla registrazione NIS 2027 e determinazione n. 314287/2026.

---

## INFORMATION TECHNOLOGY

**10 novembre 2026 - TAR Campania, Salerno: nelle gare telematiche il caricamento dei documenti non basta a presentare l'offerta.**

La riapertura dei termini di una gara telematica è un rimedio eccezionale: non è sufficiente che il concorrente segnali di non essere riuscito a inviare l'offerta. Occorre un malfunzionamento comprovato della piattaforma oppure un'assoluta incertezza tecnica sulla causa del mancato invio. È il principio applicato dal TAR Campania, Salerno, nella sentenza n. 1839, pubblicata il 27 ottobre 2026.

Nel caso esaminato, relativo a una gara dell'ASL di Salerno per cure domiciliari e telemedicina, l'impresa aveva caricato i contenuti dell'offerta entro la scadenza, senza però completarne la finalizzazione e la protocollazione. L'istruttoria tecnica ha ricondotto il mancato perfezionamento all'importazione di un file P7M anziché ZIP nella specifica fase in cui la piattaforma richiedeva quest'ultimo formato. Il sistema aveva segnalato l'errore prima della scadenza; le verifiche del gestore non avevano rilevato interruzioni o anomalie del servizio. Il TAR ha quindi respinto la richiesta di valutare l'offerta o di riaprire i termini. La questione, precisa la sentenza, non è l'ammissibilità in generale della firma digitale P7M, ma il rispetto della sequenza tecnica prevista per quella operazione.

Per imprese e stazioni appaltanti, la distinzione decisiva è tra *documenti caricati* e *offerta effettivamente trasmessa e acquisita*. Gli operatori dovrebbero completare l'invio con anticipo, verificare i formati richiesti in ogni passaggio e conservare la ricevuta di acquisizione; in caso di impedimento, segnalarlo subito con elementi tecnici circostanziati. Le amministrazioni, prima di decidere su una proroga, devono svolgere e documentare verifiche sul funzionamento della piattaforma: una rimessione individuale in termini, senza i presupposti accertati, rischia di violare la parità di trattamento tra concorrenti.

---

## MERCATI DIGITALI

**5 Novembre 2026 - Corte di giustizia UE: lo smart meter non è facoltativo per il solo fatto che il cliente preferisce un contatore tradizionale.**

Nella sentenza *Netz Niederösterreich* (C-468/24), relativa a una controversia austriaca, la Corte di giustizia ha chiarito la portata delle norme europee sull'introduzione dei contatori intelligenti. Gli articoli 19, 21 e 22 della direttiva (UE) 2019/944 non obbligano il gestore di rete ad assecondare la richiesta del cliente finale di non ricevere uno smart meter e di installare, al suo posto, un contatore convenzionale. La direttiva, dunque, non riconosce al cliente un diritto generale di opposizione all'installazione. Restano da verificare le disposizioni nazionali applicabili al singolo rapporto.

La Corte si è pronunciata anche sulla sicurezza dei dati: non è necessario che tutti i requisiti siano riprodotti nella norma nazionale che *definisce* il contatore intelligente, purché trovino attuazione nelle disposizioni pertinenti dell'ordinamento. Quanto alla direttiva ePrivacy, la mera trasmissione di dati attraverso una rete elettrica non rende tale rete una rete pubblica di comunicazione elettronica alla quale applicare, per questa ragione, l'articolo 5, paragrafo 3, sull'accesso alle informazioni presenti nelle apparecchiature terminali. Ciò non sottrae i dati di consumo alle regole del GDPR.

In pratica, gestori e fornitori non dovrebbero trattare la sentenza né come un obbligo di offrire sempre un contatore alternativo, né come un'esenzione dagli adempimenti privacy. Rimangono da presidiare le finalità e le basi giuridiche dei trattamenti, la granularità dei dati raccolti, i soggetti autorizzati ad accedervi, la sicurezza delle trasmissioni e le informazioni rese ai clienti. La Corte non ha invece risolto la specifica questione della visibilità sul contatore degli accessi anticipati ai dati di consumo, giudicandola ipotetica nel procedimento esaminato.

Corte di giustizia UE, sentenza 5 Novembre 2026, C-468/24, ECLI:EU:C:2026:936.

---

## PROPRIETA' INTELLETTUALE E INDUSTRIALE

**4 novembre 2026 – Tribunale UE: nei marchi brevi non basta una parola comune per dimostrare il rischio di confusione.**

Nella causa T-696/25, SUNS/SUN68, relativa a prodotti di abbigliamento, il Tribunale dell'Unione europea ha annullato parzialmente una decisione della commissione di ricorso EUIPO. Quest'ultima aveva attribuito al termine comune «sun» un peso distintivo eccessivo per una parte dei prodotti, sottovalutando le differenze tra i segni: la particolare rappresentazione grafica di SUNS, la «s» finale e il numero «68» del marchio anteriore. Secondo il Tribunale, anche quando i prodotti sono identici, il confronto deve considerare l'impressione complessiva dei marchi e il peso effettivo degli elementi che li compongono.

La pronuncia è utile nella scelta di nuovi nomi commerciali e nella gestione delle opposizioni, soprattutto nei settori in cui ricorrono parole evocative o diffuse. Non chiude però definitivamente la controversia: resta da esaminare, tra l'altro, se il marchio anteriore abbia acquisito attraverso l'uso una maggiore capacità distintiva. Per le imprese, la lezione pratica è duplice: una coincidenza lessicale non decide da sola il caso; chi invoca la forza acquisita del proprio marchio deve essere pronto a documentarla.

sentenza del Tribunale UE del 4 novembre 2026, ECLI:EU:T:2026:723.

---