

Aggiornamento Data protection, AI, IT and IP

n. 19/2026

DATA PROTECTION

13 ottobre 2026 – Comitato europeo per la protezione dei dati personali (EDPB): gli smart glasses richiedono trasparenza effettiva anche verso i passanti.

12 ottobre 2026 – Garante privacy: l'Autorità ricorda la scadenza del 29 ottobre prossimo in merito al tracking pixel nelle e-mail.

11 ottobre 2026 – Garante privacy: recupero crediti, online la versione aggiornata del vademecum. Stop a prassi invasive come sms o telefonate preregistrate.

INTELLIGENZA ARTIFICIALE

12 Ottobre 2026 - AI Act: pubblicato il primo standard armonizzato per i sistemi di IA ad alto rischio, dedicato alla gestione della qualità.

8 ottobre 2026 – AI Act in Italia: il decreto 179/2026 definisce controlli, sanzioni e regole per l'uso dell'IA nelle imprese.

CYBERSICUREZZA

15 Ottobre 2026 – NIS 2: ad ottobre scade il termine di 18 mesi per l'adozione da parte dei soggetti NIS iscritti e registrati nel 2025 delle misure di sicurezza di base.

11 ottobre 2026 – Autorità di Vigilanza europee: Q&A di chiarimento sulla classificazione degli incidenti relativi ad accessi malevoli riusciti.

10 Ottobre 2026 - Cyber Resilience Act: le FAQ ENISA chiariscono come notificare vulnerabilità e incidenti tramite la piattaforma unica europea.

MERCATI DIGITALI

15 ottobre 2026 – Corte di Giustizia UE: nei servizi di pagamento la negligenza grave del cliente non esonera il prestatore di servizi di pagamento dal rimborso immediato dell'importo di un'operazione di pagamento non autorizzata.

PROPRIETÀ INTELLETTUALE E INDUSTRIALE

15 Ottobre 2026 – WIPO - Marchi internazionali: l'Arabia Saudita nel Sistema di Madrid, possibile ora designare il territorio saudita nelle domande di registrazione.

8 ottobre 2026 – Segreti commerciali: il nuovo art. 98 CPI comprende dati e metodi di addestramento IA.

8 Ottobre 2026 - EUIPO e la Federazione Bancaria Europea rafforzano la cooperazione nel settore finanziario garantito dalla proprietà intellettuale.

DATA PROTECTION

13 ottobre 2026 – Comitato europeo per la protezione dei dati personali (EDPB): gli smart glasses richiedono trasparenza effettiva anche verso i passanti.

Il Comitato europeo per la protezione dei dati (EDPB) ha adottato il 13 ottobre 2026 uno **Statement sugli smart glasses**. Si tratta di prime riflessioni interpretative, non di linee guida od orientamenti (lo Statement non introduce un divieto generale degli smart glasses). Telecamere, microfoni, streaming e funzioni di intelligenza artificiale possono acquisire dati di persone che non utilizzano il dispositivo e non percepiscono di essere riprese o ascoltate. L'EDPB segnala rischi accentuati in luoghi di cura, scuole, ambienti di lavoro e spazi riservati, anche per segreti aziendali e proprietà intellettuale.

La ripartizione dei ruoli dipende da chi decide finalità e mezzi: utilizzatore, produttore e fornitore dell'app o della funzione IA possono essere titolari autonomi o contitolari. L'eccezione per attività esclusivamente personali o domestiche è interpretata restrittivamente: non copre l'uso professionale o la pubblicazione su un profilo social aperto a un numero indeterminato di persone. Inoltre, l'eventuale esenzione dell'utilizzatore privato non esonera produttore e provider dai propri obblighi.

Un'informativa tradizionale rivolta al solo acquirente non basta per i terzi ripresi. Il Comitato propone **segnali di registrazione visibili e difficili da disattivare**, eventualmente combinati con indicatori acustici e altre misure contestuali. Il consenso dei passanti raccolto dopo la ripresa non legittima la raccolta già avvenuta; il legittimo interesse richiede un bilanciamento concreto ed è particolarmente difficile da sostenere per riutilizzi commerciali e addestramento dell'IA. Restano da valutare minimizzazione, conservazione, diritti, dati particolari, trasferimenti e, nei casi pertinenti, regole ePrivacy.

Per produttori, app provider e imprese che valutano l'uso del dispositivo occorrerebbe mappare separatamente acquisizione, assistenza in tempo reale e riutilizzo dei dati, oltre a verificare le basi giuridiche e la fattibilità della trasparenza verso terzi e prevedere limitazione della registrazione continua e di accessi alle aree sensibili.

12 ottobre 2026 – Garante privacy: l'Autorità ricorda la scadenza del 29 ottobre prossimo in merito al tracking pixel nelle e-mail.

Il Garante privacy ha ricordato che il 29 ottobre 2026 scade il periodo di sei mesi concesso dalle Linee guida del 17 aprile 2026, pubblicate nella Gazzetta Ufficiale il 29 aprile. Il richiamo di ottobre rende urgente l'adeguamento di aziende, piattaforme di invio massivo e gestori di newsletter che usano immagini remote o tecniche equivalenti per rilevare aperture e comportamenti dei destinatari.

Secondo il Garante, il pixel può rientrare nell'art. 122 del Codice privacy e, per le finalità di tracciamento, richiede un consenso preventivo, libero, specifico e informato, salvo le circoscritte ipotesi tecniche, di sicurezza o di comunicazioni istituzionali e di servizio contemplate dalle Linee guida. L'informativa deve spiegare che cosa si misura, per quali finalità e con quali soggetti; il destinatario deve poter revocare il consenso facilmente e in modo granulare. La disciplina del GDPR continua ad applicarsi a ruoli, accountability, minimizzazione e *privacy by design*.

In pratica occorre censire i pixel incorporati nei template, le impostazioni dei fornitori di *marketing automation* e le aperture registrate anche per conto di terzi; disabilitare il tracciamento fino alla scelta valida; separare la revoca del tracciamento dalla gestione delle comunicazioni, quando appropriato; aggiornare informativa, registro e accordi contrattuali.

È opportuno ricordare, infine, che il Garante ha indicato la verifica delle Linee guida tra gli ambiti di verifica ispettiva nel Piano per il secondo semestre del 2026.

11 ottobre 2026 – Garante privacy: recupero crediti, online la versione aggiornata del vademecum. 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.

INTELLIGENZA ARTIFICIALE

12 Ottobre 2026 - AI Act: pubblicato il primo standard armonizzato per i sistemi di IA ad alto rischio, dedicato alla gestione della qualità.

Con [la decisione di esecuzione \(UE\) 2026/2274](#) del 12 ottobre 2026, pubblicata nella Gazzetta ufficiale dell'Unione europea il 14 ottobre 2026 ed entrata in vigore lo stesso giorno, la Commissione ha pubblicato il riferimento alla norma EN 18286:2026, «*Intelligenza artificiale — Sistema di gestione della qualità ai fini dei requisiti normativi del regolamento dell'UE sull'IA*». L'allegato alla decisione contiene, per ora, un solo standard: non si tratta quindi della pubblicazione dell'intero insieme di norme tecniche attese per i sistemi ad alto rischio.

Lo standard riguarda il sistema di gestione della qualità dei fornitori previsto dall'articolo 17 dell'AI Act. In termini operativi, tale sistema deve essere documentato attraverso politiche, procedure e istruzioni che coprano, fra l'altro, la strategia di conformità, la progettazione e le modifiche dei sistemi, le verifiche e i

test, la gestione dei dati e dei rischi, il monitoraggio dopo l'immissione sul mercato, la segnalazione degli incidenti e l'attribuzione delle responsabilità interne. EN 18286:2026 offre ai fornitori un riferimento tecnico comune per organizzare e rendere verificabili questi processi.

Per le imprese, la prima verifica consiste nello stabilire se, per uno o più sistemi, assumano il ruolo di *fornitore* ai sensi dell'AI Act. In tal caso è opportuno confrontare il sistema di gestione già adottato con EN 18286:2026, individuare procedure e registrazioni mancanti e documentare come siano gestiti controlli, modifiche e monitoraggio.

Chi dispone già di un sistema basato su ISO 9001 o ISO/IEC 42001 può utilizzarlo come base di lavoro: lo standard europeo contiene tabelle di corrispondenza, ma l'esistenza di quelle certificazioni non equivale, da sola, a dimostrare la conformità all'AI Act. L'adozione dello standard resta volontaria e non esaurisce gli altri obblighi applicabili ai sistemi ad alto rischio.

Un punto giuridico da seguire: CEN-CENELEC presenta la citazione in Gazzetta come fonte di una presunzione di conformità per il sistema di qualità dell'articolo 17. Il testo dell'articolo 40, paragrafo 1, dell'AI Act, tuttavia, richiama espressamente i requisiti della *sezione 2* del capo sui sistemi ad alto rischio, mentre l'articolo 17 è collocato nella *sezione 3*. È quindi prudente verificare la portata precisa della presunzione prima di descrivere EN 18286:2026 come una prova automatica di conformità all'intero articolo 17. Resta fermo il suo valore di riferimento tecnico ufficialmente pubblicato.

8 ottobre 2026 – AI Act in Italia: il decreto 179/2026 definisce controlli, sanzioni e regole per l'uso dell'IA nelle imprese.

Il [decreto legislativo 7 ottobre 2026, n. 179](#), pubblicato nella Gazzetta Ufficiale n. 234 dell'8 ottobre ed **applicabile dal prossimo 23 ottobre 2026**, aggiunge – dopo le regole del decreto legislativo 160/2026 – nuove norme all'assetto normativo italiano in materia di AI (L. 132/2025 e decreti delegati).

Chi vigila e come. Il decreto assegna ad **AgID** il compito di valutare, designare e monitorare gli organismi che, nei casi previsti dall'AI Act, verificano la conformità dei sistemi di IA. Ad **ACN** affida invece la vigilanza sul mercato: controllare il rispetto delle regole applicabili ai sistemi di IA e intervenire in caso di violazioni. Per i sistemi ad alto rischio impiegati nei rispettivi ambiti finanziari, la vigilanza spetta a **Banca d'Italia, CONSOB e IVASS**; restano ferme le attribuzioni del Garante privacy su AI e biometria nei sistemi ad alto rischio. Il testo disciplina poteri di controllo, misure correttive e reclami: un'impresa che sviluppa o utilizza IA dovrà quindi identificare l'autorità competente in base al sistema e al settore, predisporre documentazione verificabile e sapere chi gestirà un'eventuale contestazione. I reclami presentati all'autorità sbagliata saranno trasmessi d'ufficio a quella competente. In determinati casi del settore finanziario, le controversie con la clientela relative a violazioni dell'AI Act potranno essere trattate dagli organismi di risoluzione stragiudiziale già esistenti, entro i confini delle loro competenze.

Decisioni sul personale: controllo umano effettivo. L'articolo 41 è fra le disposizioni di maggiore impatto immediato per i datori di lavoro. Se un sistema di IA interviene nei processi relativi alla costituzione, modifica o cessazione del rapporto, comprese valutazioni delle prestazioni e decisioni disciplinari, la decisione finale non può basarsi unicamente su un trattamento automatizzato: deve essere assunta da una persona che eserciti un potere **effettivo e autonomo**. Il consenso del lavoratore non elimina questo vincolo. Il decreto esclude da questa specifica previsione le attività di ricerca e selezione delle candidature, anche quando una persona non accede alla fase successiva; rimangono però applicabili le altre regole pertinenti, fra cui quelle del GDPR. Prima del trattamento il datore deve assolvere gli obblighi informativi richiamati dall'articolo 41. Su richiesta, il lavoratore può ottenere, con l'intervento di una persona, una motivazione comprensibile della decisione, che indichi l'eventuale peso dell'IA e i principali parametri considerati. Le decisioni adottate in violazione del divieto del comma 1 sono **nulle**, incluso il licenziamento. In pratica, una mera approvazione formale dell'output del sistema non offre la garanzia di un giudizio umano autonomo: occorre organizzare e poter ricostruire il processo decisionale.

Salute e sicurezza. L'articolo 42 richiede di valutare, nell'ambito della valutazione dei rischi prevista dal d.lgs. 81/2008, l'uso di IA che incida sull'organizzazione del lavoro, sui ritmi produttivi, sulle modalità di esecuzione della prestazione o su decisioni rilevanti per la sicurezza. I datori devono inoltre informare e formare i lavoratori sui rischi specifici e sulle misure di prevenzione e protezione. Per esempio, prima di introdurre strumenti che assegnano compiti, modificano i ritmi o assistono decisioni operative, sarà opportuno coinvolgere le funzioni HR e sicurezza nella valutazione degli effetti concreti sul lavoro.

Sanzioni e gestione delle contestazioni. L'articolo 23 prevede massimali differenziati: fino a **35 milioni di euro o, se superiore, al 7% del fatturato mondiale annuo** per le pratiche vietate dall'AI Act; fino a **15 milioni o al 3%** per le violazioni degli obblighi europei elencati dalla disposizione; fino a **7,5 milioni o all'1%** per informazioni inesatte, incomplete o fuorvianti rese alle autorità o agli organismi notificati. È prevista una fascia specifica, fino a **1 milione o allo 0,5%**, per le violazioni degli articoli 27 e 86 dell'AI Act. Per PMI, microimprese e start-up innovative si applica il criterio di determinazione richiamato dall'articolo 99, paragrafo 6, del regolamento. Questi importi sono **massimali**, non sanzioni automatiche: la verifica va compiuta sulla disposizione violata, sulla sua data di applicazione e sulle circostanze del caso.

Sperimentazione e tutela del patrimonio tecnologico. Il decreto istituisce uno spazio italiano di sperimentazione regolamentare per l'IA (cosiddetta *sandbox normativa*), gestito congiuntamente da AgID e ACN, con attenzione all'accesso di PMI e start-up. Le modalità operative e i criteri di ammissione richiedono però ulteriori provvedimenti: l'istituzione dello spazio non equivale ancora all'apertura delle candidature. Sul fronte della proprietà industriale, l'articolo 52 chiarisce che dati, algoritmi, architetture dei modelli e metodi di addestramento possono rientrare nella tutela dei segreti commerciali **solo se** soddisfano i requisiti ordinari di segretezza, valore economico derivante dalla segretezza e misure ragionevoli di protezione. Per chi sviluppa IA, ciò rende particolarmente importante documentare accessi, accordi di riservatezza e misure tecniche di protezione.

Le imprese possono partire da una ricognizione dei sistemi di IA usati nei processi HR, nelle attività che incidono sulla sicurezza e nei servizi regolati; per ciascuno, conviene registrare finalità, ruolo dell'impresa, fornitore, autorità potenzialmente competente, intervento umano previsto e documentazione disponibile. È una base concreta per adeguare procedure e contratti senza presumere che tutti i sistemi ricadano negli stessi obblighi o nelle stesse scadenze.

CYBERSICUREZZA

15 Ottobre 2026 – NIS 2: ad ottobre scade il termine di 18 mesi per l'adozione da parte dei soggetti NIS iscritti e registrati nel 2025 delle misure di sicurezza di base.

Per le organizzazioni inserite nell'elenco NIS durante il 2025, **l'adozione delle misure di sicurezza di base scade 18 mesi dopo la ricezione della comunicazione di inserimento**. ACN segnala che le prime scadenze cadono in ottobre 2026, ma il giorno esatto va ricavato dalla notifica ricevuta da ciascun soggetto: non esiste un'unica data di ottobre valida per tutti. Il quadro deriva dalle determinazioni sulle specifiche di base e dai chiarimenti ACN; [il vademecum dell'11 settembre 2026](#) è uno strumento operativo, non un nuovo rinvio del termine.

L'adozione richiede la concreta implementazione dei requisiti applicabili ai soggetti importanti o essenziali, con evidenze documentali, valutazione dei rischi, procedure e coinvolgimento degli organi di amministrazione e direzione. Conviene chiudere le lacune rilevate nelle verifiche tecniche, tracciare decisioni e responsabilità, allineare contratti e presidio dei fornitori, e verificare separatamente le procedure di notifica degli incidenti già operative. La sola approvazione formale di una policy non dimostra l'attuazione dei requisiti tecnici e organizzativi.

Il calendario differisce per chi è entrato **per la prima volta nell'elenco nel 2026**: le misure di base sono dovute entro il **31 luglio 2027** e la notifica degli incidenti significativi di base decorre dal **1° gennaio 2027**, secondo la determina ACN 127434/2026.

11 ottobre 2026 – Autorità di Vigilanza europee: Q&A su DORA di chiarimento sulla classificazione degli incidenti relativi ad accessi malevoli riusciti.

La Q&A 2026_7779, pubblicata come definitiva nel *Single Rulebook* delle autorità di vigilanza europee (EBA, ESMA ed EIOPA), interpreta l'art. 6, lett. c), del regolamento delegato (UE) 2024/1772 relativo al quadro normativo DORA sulla classificazione degli incidenti ICT. Un accesso riuscito, malevolo e non autorizzato ai sistemi di rete e informazione di un'entità finanziaria va valutato autonomamente ai fini della "criticità dei servizi interessati", **anche se i sistemi compromessi non supportano funzioni critiche o importanti** e anche se l'accesso è passato attraverso la rete di un fornitore terzo ICT.

Il chiarimento evita che il *triage* escluda l'incidente soltanto perché è stato colpito un sistema ritenuto non critico o perché il vettore iniziale è presso il fornitore. Non significa, però, che ogni intrusione sia automaticamente un **incidente grave**: la classificazione complessiva richiede l'applicazione delle soglie e degli altri criteri del regolamento delegato.

Per banche, assicurazioni e altri soggetti DORA è utile aggiornare i PlayBook SOC e le procedure di classificazione degli incidenti, prevedendo una verifica documentata dell'accesso riuscito e dei criteri di gravità anche negli scenari di compromissione del fornitore. I contratti e i flussi di *escalation* con i terzi ICT dovrebbero mettere a disposizione in tempo i log e i fatti necessari alla valutazione e alle eventuali notifiche.

10 Ottobre 2026 - Cyber Resilience Act: le FAQ ENISA chiariscono come notificare vulnerabilità e incidenti tramite la piattaforma unica europea.

Nelle [FAQ aggiornate il 3 ottobre 2026](#), ENISA precisa le modalità d'uso della Single Reporting Platform, operativa dall'11 settembre. I fabbricanti di prodotti con elementi digitali devono utilizzarla per segnalare vulnerabilità attivamente sfruttate e incidenti gravi che incidono sulla sicurezza del prodotto: un primo avviso va inviato entro 24 ore dalla conoscenza dell'evento e una notifica più completa entro 72 ore, in entrambi i casi senza ritardo ingiustificato. Una sola notifica è sufficiente anche se il fabbricante ha più società o sedi nell'UE, ma occorre selezionare il CSIRT coordinatore competente.

ENISA avverte che, nella versione attuale, il contatore delle 72 ore della piattaforma può indicare una scadenza inesatta, perché calcola 48 ore dall'invio del primo avviso. L'impresa deve quindi tenere traccia autonoma del momento in cui ha acquisito conoscenza dell'evento. Le notifiche volontarie non sono ancora disponibili sulla piattaforma; gli obblighi corrispondenti per gli *open-source software stewards* si applicheranno dall'11 dicembre 2027

MERCATI DIGITALI

15 ottobre 2026 – Corte di Giustizia UE: nei servizi di pagamento la negligenza grave del cliente non esonera il prestatore di servizi di pagamento dal rimborso immediato dell'importo di un'operazione di pagamento non autorizzata.

Il prestatore di servizi di pagamento può tuttavia richiedere successivamente al cliente il rimborso delle perdite derivanti da una negligenza grave da parte di quest'ultimo. Una cliente di una banca polacca è stata vittima di una frode tramite *phishing*: un terzo si è presentato come interessato all'acquisto di un oggetto che ella stava vendendo su una piattaforma di vendita online e le ha inviato un link fraudolento, presentato come proveniente da tale piattaforma e destinato a confermare la vendita. Ingannata, la medesima ha cliccato su tale link che conduceva a un sito Internet che riproduceva l'aspetto di quello della sua banca e vi ha inserito i propri dati di connessione al servizio di e-banking. Grazie a tali dati, il terzo in questione è riuscito a trasferire dal conto bancario della cliente a un conto a lui intestato un importo pari a circa EUR 700. Il giorno successivo la cliente ha segnalato l'operazione fraudolenta alla propria banca. Quest'ultima ha tuttavia rifiutato di rimborsare l'importo dell'operazione di pagamento non autorizzata ritenendo che la cliente, per negligenza grave, avesse reso possibile tale operazione venendo meno al proprio obbligo di proteggere le credenziali di sicurezza personalizzate. A seguito di tale rifiuto, la cliente ha adito un tribunale polacco, il quale ha richiesto alla Corte di giustizia UE se, alla luce del diritto dell'Unione, la banca, in qualità di prestatore di servizi di pagamento, sia tenuta a rimborsare immediatamente l'importo di un'operazione non autorizzata, anche qualora ritenga che il cliente abbia commesso una negligenza grave.

Nella sua sentenza, la Corte risponde affermativamente. In caso di operazione di pagamento non autorizzata, il prestatore di servizi di pagamento è, in linea di principio, tenuto a rimborsare immediatamente l'importo di tale operazione, al più tardi entro la fine del primo giorno lavorativo successivo a quello in cui ne è venuto a conoscenza o ne è stato informato, a condizione che il cliente ne informi senza indugio tale prestatore di servizi di pagamento.

È prevista un'unica eccezione a tale obbligo di rimborso immediato: nel caso in cui il prestatore di servizi di pagamento abbia ragionevoli motivi per sospettare una frode commessa dal cliente e comunichi tali motivi per iscritto all'autorità nazionale competente. Il fatto che il prestatore di servizi di pagamento ritenga che il cliente abbia reso possibile l'operazione non autorizzata a causa di una negligenza grave – in particolare omettendo di adottare le misure necessarie per proteggere le credenziali di sicurezza personalizzate – non gli consente di rifiutare il rimborso immediato. Il diritto dell'Unione consente infatti di distinguere la questione del rimborso dell'importo dell'operazione di pagamento non autorizzata da quella di chi debba, in definitiva, sostenere le perdite relative a tale operazione. Pertanto, in un primo momento, il prestatore di servizi di pagamento è tenuto a procedere al rimborso immediato. In un secondo momento, esso può, se del caso, richiedere al cliente il rimborso delle perdite subite qualora dimostri che queste derivino dal fatto che il cliente, dolosamente o per negligenza grave, ha violato gli obblighi a lui incombenti, in particolare quello di proteggere le credenziali di sicurezza personalizzate. Spetta al prestatore di servizi di pagamento dimostrare l'esistenza di tale negligenza grave da parte del cliente.

PROPRIETÀ INTELLETTUALE E INDUSTRIALE

15 Ottobre 2026 – WIPO - Marchi internazionali: l'Arabia Saudita nel Sistema di Madrid, possibile ora designare il territorio saudita nelle domande di registrazione.

Il Protocollo di Madrid è entrato in vigore per l'Arabia Saudita l'8 ottobre 2026. Le imprese italiane che utilizzano il Sistema di Madrid possono ora chiedere protezione nel Paese mediante una nuova domanda internazionale o una designazione successiva di una registrazione esistente.

Per chi esporta o intende entrare nel mercato saudita è il momento di verificare portafoglio, classi e strategia di deposito.

L'adesione era stata annunciata da WIPO il **23 luglio**; la novità del periodo considerato è la sua **entrata in vigore**.

L'[avviso ufficiale WIPO](#) precisa, fra l'altro, che il termine ordinario per notificare un rifiuto provvisorio è di **18 mesi** e che si applica una tassa individuale.

8 ottobre 2026 – Segreti commerciali: il nuovo art. 98 CPI comprende dati e metodi di addestramento IA.

L'**art. 52 del d.lgs. 179/2026**, pubblicato l'8 ottobre ed efficace dal 23 ottobre 2026, aggiunge il comma 1-*bis* all'art. 98 del Codice della proprietà industriale. Tra le informazioni aziendali e le esperienze tecnico-industriali tutelabili possono rientrare **dati, algoritmi e metodi matematici per l'addestramento di sistemi IA**, incluse architetture dei modelli, funzioni di ottimizzazione, procedure e configurazioni di addestramento.

La norma non attribuisce una protezione automatica a ogni dataset o algoritmo. Devono comunque sussistere le tre condizioni già previste dall'art. 98, comma 1: informazioni segrete, valore economico proprio della segretezza e misure ragionevolmente adeguate a mantenerla. Il coordinamento con licenze, diritto d'autore, Data Act e GDPR resta necessario: la qualificazione come segreto commerciale non autorizza trattamenti illeciti di dati personali né consente di eludere obblighi legali di accesso.

Per imprese che sviluppano o commissionano modelli IA, è consigliabile inventariare dataset, pipeline, pesi e configurazioni effettivamente riservate, definire accessi per ruolo, marcatura e logging, patti di riservatezza e regole per fornitori e dipendenti. In una controversia, la prova delle misure di protezione adottate sarà centrale quanto la descrizione dell'asset tecnico.

8 Ottobre 2026 - EUIPO e la Federazione Bancaria Europea rafforzano la cooperazione nel settore finanziario garantito dalla proprietà intellettuale.

L'Ufficio per la Proprietà Intellettuale dell'Unione Europea (EUIPO) e la Federazione Bancaria Europea (EBF) hanno firmato un Memorandum d'Intesa per rafforzare la cooperazione all'intersezione tra proprietà intellettuale, finanza e supporto alle imprese. L'accordo combina l'esperienza dell'EUIPO in materia di proprietà intellettuale con l'esperienza pratica e la conoscenza del settore bancario europeo, rappresentato attraverso la rete di associazioni bancarie nazionali dell'EBF. L'EBF riunisce 33 associazioni bancarie nazionali come membri effettivi e 10 membri associati in tutta Europa, rappresentando circa 3.500 banche.

Gli sforzi congiunti si concentreranno sul rafforzamento del riconoscimento finanziario dei diritti di proprietà intellettuale, sull'espansione della capacità di prestito commerciale contro beni intangibili e sull'integrazione della collaborazione a lungo termine tra entrambi gli ecosistemi.

Per molte aziende innovative, alcuni dei loro beni più preziosi sono intangibili, dalla tecnologia e i design ai marchi e ad altre forme di proprietà intellettuale. Tuttavia, valutare il loro valore, la loro applicabilità e il potenziale recupero rimane una sfida per le istituzioni finanziarie. Una cooperazione più stretta tra esperti di proprietà intellettuale e settore bancario può aiutare a colmare queste lacune informative e migliorare la comprensione di come tali asset possano essere presi in considerazione nelle decisioni di finanziamento.

All'inizio di quest'anno, l'EUIPO ha pubblicato [finanza sostenuta da proprietà intellettuale in Europa: State of Play and Future Perspectives](#), identificando ostacoli strutturali all'uso più ampio della proprietà intellettuale nell'accesso ai finanziamenti, incluse sfide relative alla divulgazione, valutazione, dati e valutazione del rischio.

Lo studio è stato seguito dalla [Roadmap Europea per la Finanza Sostenuta dalla PI](#), sviluppata attraverso la cooperazione con istituzioni UE, uffici nazionali di proprietà intellettuale, istituzioni finanziarie, imprese ed esperti. L'accordo con l'EBF rappresenta un altro passo pratico in questo sforzo continuo per avvicinare le comunità di proprietà intellettuale e finanziarie.

L'[accordo](#) fornisce un quadro per la cooperazione continua, con attività specifiche da sviluppare attraverso piani di lavoro congiunti.