FIVERS

Aggiornamento
Data protection, AI, IT and IP

n. 18/2026

DATA PROTECTION

21 Settembre 2026 – Comitato europeo per la protezione dei dati personali: adottata la versione definitiva delle Linee Guida 3/2025 sul coordinamento tra DSA e GDPR.

---

19 Settembre 2026 – Comitato europeo per la protezione dei dati personali: in consultazione pubblica le Linee Guida 4/2026 sulla metodologia comune per decidere quando irrogare una multa e quando ricorrere ad altre misure correttive.

INTELLIGENZA ARTIFICIALE

15 Settembre 2026 – Intelligenza artificiale e responsabilità penale, civile e 231: il D.lgs. 160/2026 introduce nuovi obblighi e adempimenti per le imprese.

CYBERSICUREZZA

15 Settembre 2026 – Agenzia Nazionale per la cybersicurezza: online il vademecum per i soggetti NIS.

---

11 Settembre 2026 - Cyber Resilience Act: dall'11 settembre 2026 scattano gli obblighi di notifica delle vulnerabilità attivamente sfruttate e degli incidenti gravi.

INFORMATION TECHNOLOGY

17 Settembre 2026 – Commissione UE: presentata la proposta dello EU Kids Act a tutela dei minori nell'utilizzo dei servizi digitali.

---

12 Settembre 2026 – Data Act: dal 12 settembre 2026 si applicano i nuovi obblighi di "access by design" per i dati generati dai prodotti connessi.

MERCATI DIGITALI

18 Settembre 2026 – Autorità bancaria europea (EBA): EBA: adottate nuove Linee guida sulla gestione dei rischi derivanti dai fornitori terzi non informatici.

PROPRIETA' INTELLETTUALE E INDUSTRIALE

18 Settembre 2026 – Corte di Giustizia dell'Unione europea: anche un breve post sui social media può costituire un'opera protetta ai sensi della normativa sul diritto d'autore.

18 settembre 2026 – EUIPO: dichiarato decaduto il marchio europeo META per non uso quinquennale.

DATA PROTECTION

21 Settembre 2026 – Comitato europeo per la protezione dei dati personali: adottata la versione definitiva delle Linee Guida 3/2025 sul coordinamento tra DSA e GDPR.

L'EDPB ha adottato la versione definitiva delle ***Guidelines 3/2025 on the interplay between the Digital Services Act and the GDPR***, chiarendo come devono coordinarsi i due regolamenti quando l'adempimento degli obblighi previsti dal **Digital Services Act (DSA)** comporta trattamenti di dati personali.

Il principio di fondo è che **il DSA non sostituisce il GDPR e non costituisce, di per sé, una base giuridica generalizzata per il trattamento dei dati personali**. Ogni trattamento effettuato nell'ambito della compliance DSA deve quindi essere autonomamente valutato alla luce del GDPR, verificando base giuridica, necessità, proporzionalità, minimizzazione, trasparenza, privacy by design, eventuale applicabilità dell'art. 22 sulle decisioni automatizzate e necessità di una DPIA.

Le Linee guida affrontano in particolare alcuni ambiti ad alto impatto operativo.

Per la **moderazione dei contenuti**, l'EDPB distingue tra attività volontarie e trattamenti necessari per adempiere a specifici obblighi di legge. Le attività volontarie di individuazione dei contenuti illeciti possono, ricorrendone i presupposti, essere fondate sul legittimo interesse; quando invece il trattamento è imposto da uno specifico obbligo normativo può trovare applicazione l'art. 6, par. 1, lett. c), GDPR. L'EDPB esclude però che il DSA possa giustificare forme generalizzate di monitoraggio o profilazione degli utenti. Se la moderazione automatizzata conduce alla rimozione di contenuti o alla sospensione di account, deve inoltre essere verificata l'eventuale applicabilità dell'art. 22 GDPR e l'intervento umano deve essere effettivo, non meramente formale.

In materia di **pubblicità online**, l'EDPB chiarisce che gli obblighi di trasparenza previsti dal DSA si aggiungono a quelli del GDPR e non li sostituiscono. L'obbligo DSA di informare l'utente sui parametri utilizzati per la pubblicità non costituisce una base giuridica autonoma per il targeting. Particolarmente rilevante è inoltre il divieto di utilizzare, per pubblicità basata sulla profilazione, **categorie particolari di dati personali**, comprese quelle inferite mediante profilazione: il divieto opera anche quando il trattamento potrebbe astrattamente essere consentito ai sensi dell'art. 9 GDPR.

Sul fronte dei **sistemi di raccomandazione**, l'EDPB sottolinea che, quando il DSA impone la disponibilità di un'opzione non basata sulla profilazione, tale scelta deve essere effettiva anche sul piano tecnico. Non è sufficiente mostrare all'utente un feed diverso: se l'utente seleziona l'opzione non profilata, il provider non dovrebbe continuare a raccogliere o utilizzare dati personali per profilarlo ai fini delle future raccomandazioni. In alcuni casi, inoltre, la raccomandazione automatizzata può integrare una decisione rilevante ai sensi dell'art. 22 GDPR, ad esempio nei servizi che raccomandano offerte di lavoro o immobili.

Le Linee guida dedicano poi particolare attenzione ai **dark patterns**, chiarendo che quando il design manipolativo incide sulle scelte relative al trattamento dei dati personali entra direttamente in gioco il principio di correttezza del GDPR. Interfacce che inducano l'utente a fornire più dati, accettare opzioni privacy meno protettive o mantenere comportamenti compulsivi possono quindi assumere rilevanza simultaneamente ai sensi del DSA e del GDPR.

Ulteriori indicazioni riguardano la **protezione dei minori**. L'EDPB ammette che gli obblighi DSA possano giustificare trattamenti di verifica dell'età, ma insiste sulla necessità di soluzioni. Le piattaforme dovrebbero evitare raccolte generalizzate di documenti di identità o altri strumenti che determinino l'identificazione univoca dell'utente quando non strettamente necessari e, ove possibile, limitarsi a verificare il superamento o meno della soglia di età richiesta.

DSA e GDPR non possono dunque più essere gestiti attraverso programmi di *compliance* separati. Moderazione dei contenuti, advertising, sistemi di raccomandazione, gestione dei reclami, tutela dei minori e valutazione dei rischi sistemici devono essere analizzati congiuntamente, associando a ciascun obbligo DSA i trattamenti di dati necessari per attuarlo e verificandone la conformità al GDPR.

Diventa quindi opportuno predisporre una **matrice integrata DSA-GDPR**, capace di mappare, per ciascun processo, finalità, base giuridica, categorie di dati, tempi di conservazione, eventuali decisioni automatizzate, misure di sicurezza e necessità di una DPIA. È su questa integrazione tra obbligo digitale e trattamento sottostante che l'EDPB concentra ora il baricentro della *compliance.*

---

19 Settembre 2026 – Comitato europeo per la protezione dei dati personali: in consultazione pubblica le Linee Guida 4/2026 sulla metodologia comune per decidere quando irrogare una multa e quando ricorrere ad altre misure correttive.

Il Comitato europeo per la protezione dei dati personali (EDPB) ha adottato le nuove **Linee guida 04/2026 sull'esercizio del potere di irrogare sanzioni amministrative pecuniarie in relazione agli altri poteri correttivi previsti dal GDPR**, successivamente pubblicate per consultazione pubblica dal **21 settembre al 13 novembre 2026**.

Il documento affronta un profilo diverso da quello della mera quantificazione delle sanzioni: chiarisce **quando un'Autorità di protezione dei dati dovrebbe irrogare una sanzione amministrativa pecuniaria e quando, invece, possa ricorrere ad altri poteri correttivi** previsti dall'art. 58, par. 2, GDPR, quali ammonimenti, reprimende, ordini di adeguamento, limitazioni o divieti del trattamento e revoca delle certificazioni. Le nuove Linee guida sostituiscono sul punto i precedenti orientamenti del Gruppo Articolo 29 e si pongono in rapporto di complementarità con le **Guidelines 04/2022**, dedicate al metodo di calcolo dell'importo delle sanzioni.

L'obiettivo è rendere maggiormente uniforme l'attività di enforcement nell'Unione europea, attraverso una **metodologia articolata in cinque passaggi**.

In primo luogo, l'Autorità deve verificare che la violazione accertata sia effettivamente suscettibile di essere sanzionata con una multa ai sensi del GDPR o, nei casi consentiti, del diritto nazionale. Deve poi stabilire **quale soggetto possa essere chiamato a risponderne** – ad esempio titolare, responsabile del trattamento, organismo di certificazione o organismo di monitoraggio – e accertare che la violazione sia stata commessa **intenzionalmente o per negligenza**. Soltanto dopo queste verifiche preliminari l'Autorità valuta, sulla base dei criteri dell'art. 83, par. 2, GDPR, se la violazione possa essere qualificata come "minore" e, infine, se l'irrogazione di una sanzione pecuniaria sia **effettiva, proporzionata e dissuasiva** nel caso concreto.

Particolarmente rilevante per le imprese è il chiarimento sulla **responsabilità dell'organizzazione**. L'EDPB, richiamando la giurisprudenza della Corte di giustizia, precisa che titolari e responsabili possono rispondere direttamente delle violazioni commesse da amministratori, dipendenti o altri soggetti che operano nell'ambito dell'attività dell'organizzazione e per suo conto: **non è necessario dimostrare che l'organo di gestione fosse a conoscenza della condotta né identificare necessariamente la persona fisica cui materialmente imputare l'infrazione**.

Le Linee guida dedicano inoltre particolare attenzione al requisito della **colpa**. Perché possa essere irrogata una sanzione pecuniaria deve sussistere almeno una condotta negligente, ma la soglia prospettata dall'EDPB è relativamente bassa: ciò che conta è se il soggetto **fosse in condizione di conoscere l'illiceità della propria condotta e avrebbe dovuto conoscerla adottando l'ordinaria diligenza richiesta**. La semplice ignoranza della normativa non è quindi sufficiente ad escludere la negligenza.

Nemmeno l'esistenza di un **parere legale interno o esterno** produce automaticamente un effetto esimente. Tra gli esempi contenuti nelle Linee guida, l'EDPB considera possibile la sussistenza della negligenza anche quando l'impresa abbia seguito un parere legale che si discosti da orientamenti consolidati o noti dell'Autorità di controllo o della dottrina; analogamente, un parere esterno non documentato o fondato su informazioni incomplete non è, di per sé, sufficiente ad escludere la responsabilità.

Un passaggio centrale riguarda poi la distinzione tra **violazioni minori e non minori**. L'Autorità deve effettuare una valutazione complessiva dei fattori aggravanti e attenuanti dell'art. 83, par. 2, considerando, tra l'altro, natura, gravità e durata della violazione, numero di interessati, danni prodotti, grado di colpa,

misure adottate per limitare le conseguenze, precedenti violazioni, grado di cooperazione con l'Autorità, categorie di dati coinvolte e eventuali vantaggi economici ottenuti.
Se la violazione è qualificata come **minore**, la regola generale indicata dall'EDPB è che non venga irrogata una sanzione pecuniaria e possa essere utilizzata, ad esempio, una reprimenda. Ciò non costituisce tuttavia un automatismo: in presenza di specifiche circostanze una multa può essere irrogata anche per una violazione minore. Per converso, quando la violazione **non è minore**, le Linee guida individuano una forte presunzione – e, in termini generali, la regola – a favore dell'applicazione di una sanzione pecuniaria, ferma restando la possibilità dell'Autorità di scegliere diversamente quando ciò sia imposto dai principi di effettività, proporzionalità e dissuasività. In circostanze eccezionali può persino risultare non necessario esercitare alcun potere correttivo

L'EDPB sottolinea inoltre che le **misure di compliance già obbligatorie ai sensi del GDPR non diventano automaticamente circostanze attenuanti**. Nell'esaminare il grado di responsabilità, l'Autorità valuterà piuttosto se il titolare o il responsabile abbia fatto quanto ragionevolmente ci si poteva attendere in relazione alla natura, alle finalità e alle dimensioni del trattamento e se le misure adottate ai sensi degli artt. 24, 25 e 32 GDPR abbiano effettivamente ridotto i rischi residui per gli interessati.

Anche la **condotta successiva alla violazione** assume rilievo. La tempestiva mitigazione del danno, la cooperazione effettiva con l'Autorità e l'adozione spontanea di misure capaci di evitare la reiterazione possono incidere sulla valutazione complessiva. Al contrario, la presenza di violazioni precedenti – soprattutto se dello stesso tipo – o la ripetizione di condotte inizialmente qualificabili come minori possono evidenziare un problema organizzativo sistemico e rendere più probabile l'applicazione di una multa.

Da un punto di vista operativo, le Linee Guida 04/2026 rafforzano quindi l'importanza di una **compliance GDPR effettiva e documentabile**. Per le imprese diventa particolarmente importante poter dimostrare non soltanto l'esistenza formale di policy e procedure, ma anche la concreta attuazione delle misure di accountability; conservare evidenza delle valutazioni giuridiche e delle decisioni adottate; documentare l'esame e l'attuazione delle indicazioni del DPO; disporre di procedure per una rapida remediation delle violazioni; e monitorare eventuali precedenti o criticità ricorrenti che potrebbero trasformare episodi isolati in un indice di carenze organizzative strutturali.

Le nuove Linee guida completano quindi il quadro sanzionatorio elaborato dall'EDPB: **le Linee Guida 04/2022 spiegano come determinare l'importo di una multa; le Linee Guida 04/2026 indicano, invece, quando quella multa dovrebbe essere applicata rispetto agli altri strumenti correttivi disponibili alle Autorità**.

INTELLIGENZA ARTIFICIALE

15 Settembre 2026 – Intelligenza artificiale e responsabilità penale, civile e 231: il D.lgs. 160/2026 introduce nuovi obblighi e adempimenti per le imprese.

Il **15 settembre 2026** è stato pubblicato nella Gazzetta Ufficiale, Serie Generale n. 214, il **Decreto Legislativo 9 settembre 2026, n. 160**, recante l'"*Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 […] in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità civile e penale*". Il decreto entra in vigore il **30 settembre 2026**.

Il provvedimento costituisce uno dei principali interventi di attuazione interna del quadro normativo europeo sull'intelligenza artificiale e dà seguito alla delega contenuta nella **Legge 23 settembre 2025, n. 132**. La sua rilevanza, tuttavia, non riguarda soltanto le amministrazioni di pubblica sicurezza: accanto alla disciplina dell'utilizzo dell'IA da parte delle Forze di polizia, il decreto introduce infatti disposizioni di carattere generale in materia di **responsabilità penale, responsabilità amministrativa degli enti ai sensi del D.lgs. 231/2001 e risarcimento dei danni cagionati dall'utilizzo di sistemi di intelligenza artificiale**.

Il decreto si articola in **22 articoli e tre Titoli**. Il **Titolo I (artt. 1-10)** disciplina l'utilizzo dei sistemi di IA nell'attività di polizia, compresi ricerca e sperimentazione, formazione, sorveglianza umana, trattamento dei dati biometrici, identificazione biometrica remota in tempo reale e riconoscimento facciale a posteriori.

Il **Titolo II (artt. 11-20)** interviene sulla responsabilità penale e civile: introduce l'art. 437-bis c.p., disciplina l'impiego processuale dell'identificazione biometrica, modifica le regole sul sequestro dei contenuti online generati anche con IA, introduce il nuovo art. 25-vicies nel D.lgs. 231/2001 e stabilisce specifiche regole per le azioni risarcitorie relative ai sistemi di IA. Il **Titolo III (artt. 21-22)** contiene le disposizioni transitorie e finanziarie; per i sistemi di IA già oggetto di contratti, sviluppo, sperimentazione o utilizzo nelle attività di polizia è previsto un periodo di adeguamento di un anno alle disposizioni del Capo II del Titolo I.

CYBERSICUREZZA

15 Settembre 2026 – Agenzia Nazionale per la cybersicurezza: online il vademecum per i soggetti NIS.

La riunione plenaria del Tavolo di attuazione della NIS dell'Agenzia per la cybersicurezza nazionale, con le Autorità di settore e i rappresentanti regionali, ha approfondito le determinazioni del Direttore generale di ACN. È stato disposto **l'aggiornamento dell'elenco dei soggetti NIS**, che riguarda oltre 2000 registrazioni tardive e circa 2000 istruttorie di revisione, analizzate da ACN da maggio a luglio. L'attività fa parte del percorso collaborativo di attuazione dell'Autorità nazionale NIS portato avanti da ACN per assicurare il presidio efficace del tessuto produttivo del Paese.

È stata avviata anche la **consultazione delle misure di sicurezza rafforzate**, elaborate in accordo con i principi di proporzionalità e gradualità della disciplina NIS. Il percorso consultivo **con i tavoli settoriali** ha l'obiettivo di integrare e sostituire le misure di sicurezza di base adottate nella fase di prima applicazione del decreto NIS.

È la terza consultazione con cui l'Agenzia, con le Autorità di settore, invita il confronto costruttivo con i settori interessati sui provvedimenti attuativi del decreto NIS. I contributi saranno valorizzati in fase di revisione da parte dell'Autorità secondo il principio di regolamentazione partecipata che contraddistingue ACN.

Il Tavolo ha ricordato che il 1° gennaio 2027 si apre la **nuova finestra di registrazione** o aggiornamento per i soggetti pubblici e privati a cui si applica la NIS. La registrazione termina il 28 febbraio 2027.

da metà settembre è inoltre disponibile il Vademecum NIS con le indicazioni di carattere generale sui principali adempimenti le relative scadenze e alcuni focus su temi specifici.

La prima scadenza, nel prossimo ottobre, riguarda il termine per l'attuazione delle misure di sicurezza di base per i soggetti inseriti nell'elenco NIS nel 2025.

La prossima scadenza riguarda la registrazione per il 2027. Come ogni anno, dal 1 ° gennaio al 28 febbraio tutti i soggetti NIS sono tenuti a fare o aggiornare la registrazione online attraverso l'accesso al portale dei servizi di ACN.

I focus riguardano anche l'aggiornamento delle informazioni e la categorizzazione di attività e i servizi.
La registrazione, oltre a essere un adempimento obbligatorio, è il primo passo per entrare a far parte della costituency dei soggetti NIS e avere accesso all'attività di supporto di ACN e dello CSIRT Italia in un contesto di regolazione partecipata e compliance cooperativa.
Con l'aggiornamento delle informazioni il soggetto NIS condivide con l'Autorità nazionale competente NIS (ACN) le informazioni previste dal decreto NIS per rendere più efficace la protezione delle reti e dei sistemi informativi dei soggetti e del Paese, grazie anche al potenziamento delle analisi a tutela della rilevanza sistemica della catena di approvvigionamento.

Attraverso la categorizzazione delle attività e dei servizi, inoltre, il soggetto NIS svolge un'analisi di impatto semplificata in base a un modello armonizzato e condivide gli esiti con ACN per stabilire obblighi in materia di misure di sicurezza proporzionati.

---

11 Settembre 2026 - Cyber Resilience Act: dall'11 settembre 2026 scattano gli obblighi di notifica delle vulnerabilità attivamente sfruttate e degli incidenti gravi.

Dall'**11 settembre 2026** è divenuto applicabile uno dei primi blocchi di obblighi sostanziali previsti dal **Regolamento (UE) 2024/2847 – Cyber Resilience Act (CRA)**: i fabbricanti di prodotti con elementi digitali devono ora notificare le **vulnerabilità attivamente sfruttate** e gli **incidenti gravi che incidono sulla sicurezza dei prodotti** secondo le tempistiche e le modalità previste dall'art. 14 del Regolamento. Contestualmente, ENISA ha reso operativa la **CRA Single Reporting Platform (SRP)**, il punto unico europeo attraverso il quale devono essere effettuate le notifiche.

Si tratta di una tappa particolarmente rilevante nell'attuazione progressiva del CRA. Il Regolamento è entrato in vigore il 10 dicembre 2024 e sarà pienamente applicabile dall'**11 dicembre 2027**, ma il legislatore europeo ha anticipato l'applicazione di alcune disposizioni: dopo le norme relative agli organismi di valutazione della conformità, applicabili dall'11 giugno 2026, dall'11 settembre 2026 sono operative le disposizioni dell'**art. 14 sugli obblighi di reporting**.

La novità riguarda direttamente i **fabbricanti di prodotti con elementi digitali**, vale a dire, in termini generali, i soggetti che immettono sul mercato dell'Unione con il proprio nome o marchio prodotti hardware o software dotati di una connessione logica o fisica, diretta o indiretta, a un dispositivo o a una rete. Il campo di applicazione comprende quindi un panorama estremamente ampio: dispositivi IoT, apparecchiature connesse, software, applicazioni, sistemi operativi, componenti hardware e software, dispositivi industriali e numerose altre categorie di prodotti digitali.

Un elemento di particolare rilievo è che **gli obblighi di notifica si applicano anche ai prodotti con elementi digitali già messi a disposizione sul mercato dell'Unione prima dell'11 dicembre 2027**. Non è quindi corretto ritenere che le imprese possano attendere la piena applicabilità del CRA prima di adeguare le proprie procedure di vulnerability e incident management: per il reporting previsto dall'art. 14, l'obbligo è già operativo.

Quali eventi devono essere notificati

Il CRA distingue due categorie di eventi soggetti a notifica obbligatoria.

La prima è costituita dalle **"vulnerabilità attivamente sfruttate"** (*actively exploited vulnerabilities*). Non è sufficiente, pertanto, la mera esistenza di una vulnerabilità o la sua astratta possibilità di sfruttamento. Ai sensi del Regolamento, è attivamente sfruttata la vulnerabilità rispetto alla quale esistano **evidenze affidabili che un soggetto malevolo l'abbia effettivamente sfruttata in un sistema senza l'autorizzazione del titolare del sistema**.

La seconda categoria riguarda gli **incidenti gravi che incidono sulla sicurezza di un prodotto con elementi digitali**. L'incidente è considerato grave quando incide negativamente, o è in grado di incidere negativamente, sulla capacità del prodotto di proteggere la disponibilità, autenticità, integrità o riservatezza di dati o funzioni sensibili o importanti; oppure quando ha comportato, o può comportare, l'introduzione o l'esecuzione di codice malevolo nel prodotto o nei sistemi informativi e di rete di un suo utilizzatore. La distinzione è importante anche sotto il profilo operativo: **non ogni vulnerabilità deve essere notificata obbligatoriamente ai sensi dell'art. 14**, ma occorre che ricorrano i requisiti dell'"active exploitation"; analogamente, non ogni anomalia o evento di sicurezza integra automaticamente un "severe incident". Le imprese devono quindi essere in grado di qualificare rapidamente l'evento alla luce delle definizioni regolamentari.

Le notifiche seguono una tempistica particolarmente stringente. Il sistema delineato dal CRA prevede una sequenza di comunicazioni successive. Per una **vulnerabilità attivamente sfruttata**, il fabbricante deve trasmettere:

- un **early warning entro 24 ore** dal momento in cui ne viene a conoscenza;
- una **notifica della vulnerabilità entro 72 ore**, contenente, ove disponibili, informazioni generali sul prodotto interessato, sulla natura dell'exploit e della vulnerabilità, nonché sulle misure correttive o di mitigazione già adottate e su quelle che possono essere adottate dagli utenti;
- una **relazione finale entro 14 giorni dalla disponibilità di una misura correttiva o di mitigazione**, contenente almeno la descrizione della vulnerabilità, la sua gravità e il relativo impatto, le eventuali informazioni disponibili sull'attore malevolo e i dettagli dell'aggiornamento di sicurezza o delle altre misure correttive predisposte.

Per gli **incidenti gravi**, il fabbricante deve invece inviare:

- un **early warning entro 24 ore** dalla conoscenza dell'incidente, indicando almeno se vi sia il sospetto che esso derivi da condotte illecite o malevole;
- una **notifica entro 72 ore**, comprendente, ove disponibili, informazioni sulla natura dell'incidente, una prima valutazione e le misure correttive o di mitigazione;
- una **relazione finale entro un mese dalla notifica delle 72 ore**, con una descrizione dettagliata dell'incidente, della sua gravità e del suo impatto, la probabile tipologia di minaccia o *root cause* e le misure di mitigazione adottate o ancora in corso.

INFORMATION TECHNOLOGY

17 Settembre 2026 – Commissione UE: presentata la proposta dello EU Kids Act a tutela dei minori nell'utilizzo dei servizi digitali.

Il 17 settembre 2026 la Commissione europea ha presentato la proposta di regolamento **EU KIDS Act – "EU Keeping Internet Digital Spaces Accountable and Trustworthy" (COM(2026) 681 final)**, destinata a rafforzare e armonizzare nell'Unione la protezione dei minori nell'utilizzo dei servizi digitali. Si tratta, allo stato, di una proposta legislativa, che dovrà essere esaminata dal Parlamento europeo e dal Consiglio e il cui contenuto potrà quindi essere modificato nel corso dell'iter legislativo.

L'intervento va ben oltre il tema, maggiormente visibile, dell'età minima per accedere ai social network. La proposta introduce infatti un sistema progressivo di accesso: **al di sotto dei 13 anni non sarebbe consentita la titolarità di account sui social media; tra 13 e 14 anni sarebbe possibile utilizzare account limitati e sottoposti al controllo di un genitore o tutore; dai 15 anni il minore potrebbe invece aprire e gestire autonomamente il proprio account**. Per gli account dei 13-14enni sono previsti, tra l'altro, strumenti permanenti di controllo parentale e un limite giornaliero di utilizzo non superiore a un'ora. Entro sei mesi dall'applicazione delle nuove regole, le piattaforme interessate dovrebbero inoltre verificare gli account già esistenti e disabilitare quelli riferibili a utenti di età inferiore a 15 anni o per i quali l'età non possa essere accertata secondo le modalità previste.

Particolarmente significativo per gli operatori è il principio di **"safety by design"**. I fornitori non potranno limitarsi a introdurre strumenti di controllo successivi, ma dovranno progettare servizi e funzionalità tenendo preventivamente conto dei rischi per i minori. La disciplina proposta interessa, con obblighi differenziati, non soltanto social network e piattaforme di condivisione video, ma anche **videogiochi online, app store, AI companions e chatbot conversazionali**. Tra le misure indicate dalla Commissione rientrano il contrasto alle tecniche di progettazione suscettibili di favorire un uso compulsivo – quali infinite scrolling, autoplay continuo, determinate notifiche e meccanismi di "streak" – nonché impostazioni maggiormente protettive per default, limitazioni ai contatti da parte di sconosciuti e una diversa configurazione dei sistemi di raccomandazione destinati ai minori.

Un altro profilo centrale riguarda la **verifica dell'età**. La semplice autodichiarazione della data di nascita non sarebbe più sufficiente nei casi disciplinati dal regolamento. La proposta punta invece sull'utilizzo di sistemi certificati di age assurance, compresa la soluzione europea di verifica dell'età e, successivamente, lo European Digital Identity Wallet. L'architettura delineata dalla Commissione mira, tuttavia, a coniugare

la verifica dell'età con il principio di minimizzazione dei dati: attraverso tecniche di "*zero-knowledge proof*", il servizio dovrebbe poter conoscere soltanto se l'utente abbia o meno superato una determinata soglia di età, senza riceverne l'identità o ulteriori informazioni personali. Il nuovo quadro dovrà pertanto essere letto anche in coordinamento con il **GDPR**, oltre che con gli obblighi già derivanti dal Digital Services Act.

Specifiche disposizioni sono previste anche per i sistemi di **intelligenza artificiale destinati o accessibili ai minori**. AI companions e chatbot non dovrebbero utilizzare modalità di interazione idonee a creare forme di dipendenza emotiva attraverso la simulazione di relazioni umane; inoltre, determinate funzionalità dovranno essere disattivate per impostazione predefinita e i fornitori saranno chiamati a valutare i rischi per i minori prima della messa a disposizione del sistema e a monitorarli successivamente. Il KIDS Act costruisce, sotto questo profilo, un raccordo diretto con il sistema di governance e vigilanza previsto dall'**AI Act**.

Anche il sistema di enforcement è particolarmente incisivo. Per le piattaforme di maggiori dimensioni il modello delineato dalla Commissione comporta una sostanziale **inversione dell'onere della conformità**: prima di consentire l'interazione con minori, le VLOP dovrebbero predisporre un piano dettagliato di compliance e sottoporlo a verifica indipendente. Le sanzioni previste dalla proposta possono arrivare fino al **6% del fatturato annuo mondiale complessivo**, facendo leva, per le piattaforme e per i sistemi di IA, sulle strutture di vigilanza già istituite rispettivamente dal DSA e dall'AI Act.

Sul piano operativo, la proposta merita quindi attenzione sin d'ora da parte delle imprese che progettano o forniscono servizi digitali potenzialmente utilizzabili da minori. In particolare, sarà opportuno verificare se i servizi offerti rientrino nel futuro ambito di applicazione, mappare le funzionalità che presuppongono la conoscenza o la stima dell'età dell'utente, riesaminare sistemi di raccomandazione, notifiche, meccanismi di engagement e acquisti in-app, nonché valutare l'integrazione futura di strumenti di *age assurance* e *parental control*. Per i fornitori di sistemi di IA, l'analisi dovrà inoltre essere coordinata con la classificazione e gli adempimenti già richiesti dall'AI Act; per tutti gli operatori, la progettazione dei meccanismi di verifica dell'età dovrà essere accompagnata da una specifica valutazione dei relativi impatti privacy.

Il testo non introduce dunque soltanto una "soglia di età europea" per i social media, ma anticipa un modello più ampio nel quale **la protezione del minore diventa un requisito strutturale di progettazione del prodotto e del servizio digitale**. Per le imprese interessate, l'evoluzione dell'iter legislativo dovrà quindi essere monitorata soprattutto sotto il profilo della progettazione dei servizi, della governance dei dati e dell'integrazione tra gli adempimenti derivanti da KIDS Act, DSA, GDPR e AI Act.

---

12 Settembre 2026 – Data Act: dal 12 settembre 2026 si applicano i nuovi obblighi di "access by design" per i dati generati dai prodotti connessi.

Entra in una nuova fase applicativa il **Regolamento (UE) 2023/2854 – Data Act**: dal **12 settembre 2026** trova infatti applicazione l'obbligo previsto dall'art. 3, par. 1, in base al quale i prodotti connessi e i relativi servizi immessi sul mercato dopo tale data devono essere progettati in modo da consentire agli utenti un accesso agevole ai dati generati dal loro utilizzo. La previsione ha portata unionale e interessa quindi anche produttori e fornitori che commercializzano prodotti o servizi nel mercato italiano.

Il Data Act è applicabile, nel suo complesso, già dal **12 settembre 2025**. Fino ad oggi, tuttavia, il diritto dell'utente di ottenere i dati generati dall'utilizzo di un prodotto connesso può richiedere, in determinate circostanze, una specifica richiesta al titolare dei dati. Con la nuova fase applicativa, il legislatore europeo compie un ulteriore passaggio verso un modello di **"access by design"**: l'accessibilità dei dati deve essere incorporata nella progettazione stessa del prodotto o del servizio, anziché essere gestita esclusivamente attraverso procedure successive di richiesta.

In particolare, l'art. 3, par. 1, del Data Act dispone che i **prodotti connessi siano progettati e fabbricati e i servizi correlati siano progettati e forniti** in modo tale che i dati del prodotto e del servizio correlato, compresi i metadati necessari alla loro interpretazione e utilizzazione, siano per impostazione predefinita accessibili all'utente **facilmente, in modo sicuro e gratuito, in un formato completo, strutturato, di**

uso comune e leggibile da dispositivo automatico. Ove pertinente e tecnicamente possibile, l'accesso deve inoltre essere **diretto**.

La disciplina riguarda un numero molto ampio di dispositivi dell'**Internet of Things (IoT)**. Rientrano nella nozione di prodotto connesso, ad esempio, **smartwatch e dispositivi per il monitoraggio della salute, apparecchiature smart home, automobili e altri veicoli connessi, macchinari industriali, agricoli e altri dispositivi capaci di raccogliere o generare dati relativi al proprio utilizzo o all'ambiente circostante e di comunicarli elettronicamente**. Sono interessati anche i "servizi correlati", quali applicazioni, software o servizi di monitoraggio remoto connessi al prodotto e funzionali al suo funzionamento o alla modifica delle sue funzionalità.

I dati interessati comprendono, in linea generale, i **dati grezzi e pretrattati generati dall'utilizzo del prodotto connesso o del servizio correlato che siano prontamente disponibili al titolare dei dati**, nonché i relativi metadati. Possono quindi rientrare nel perimetro, a seconda del prodotto, dati relativi a temperatura, pressione, posizione, velocità, accelerazione, utilizzo o prestazioni dell'apparecchiatura. Restano invece fuori dall'ambito del Capo II, in linea di principio, i dati desunti o derivati mediante elaborazioni ulteriori e i contenuti protetti, ferme restando le specifiche disposizioni del Regolamento e la normativa in materia di proprietà intellettuale.

L'"access by design" non significa, tuttavia, che ogni dato debba necessariamente essere fisicamente memorizzato sul dispositivo o che sia sempre richiesto un accesso diretto. Quest'ultimo è imposto dall'art. 3 nella misura in cui sia **pertinente e tecnicamente possibile**. Quando l'utente non possa accedere direttamente ai dati dal prodotto o dal servizio correlato, continua ad operare il meccanismo previsto dall'art. 4 del Data Act, in base al quale il titolare deve mettere a disposizione dell'utente, su semplice richiesta e senza indebito ritardo, i dati interessati e i relativi metadati, gratuitamente e, ove pertinente e tecnicamente possibile, anche in maniera continua e in tempo reale.

Il diritto non è riservato ai consumatori. Ai fini del Data Act, possono essere utenti anche le **imprese che possiedono, prendono in locazione o utilizzano in leasing un prodotto connesso** o che ricevono un servizio correlato. Il nuovo regime assume quindi particolare importanza nei rapporti **B2B**, ad esempio per macchinari industriali, flotte di veicoli, dispositivi professionali e apparecchiature IoT, consentendo all'impresa utilizzatrice di sfruttare i dati generati per attività di manutenzione, ottimizzazione dei processi, analisi delle prestazioni o ricorso a fornitori di servizi post-vendita diversi dal produttore.

La possibilità di rendere i dati accessibili all'utente è infatti strettamente collegata all'altro obiettivo centrale del Data Act: consentire all'utente di **utilizzare i dati e metterli a disposizione di terzi scelti dallo stesso**, favorendo così lo sviluppo di servizi di manutenzione, riparazione e altri servizi data-driven e riducendo fenomeni di lock-in rispetto al produttore originario.

Sul piano operativo, per produttori e fornitori la nuova fase applicativa richiede un controllo che non può essere limitato alla documentazione contrattuale. Le imprese dovrebbero verificare se i prodotti e i servizi immessi sul mercato dopo il 12 settembre 2026 rientrino nelle definizioni di "prodotto connesso" e "servizio correlato"; identificare quali dati e metadati ricadano nel perimetro del Data Act; verificare se l'architettura tecnica consenta l'accesso diretto dell'utente; predisporre interfacce, dashboard, applicazioni, API o altri strumenti tecnici idonei; e documentare adeguatamente le ragioni per cui, in determinati casi, l'accesso diretto non sia tecnicamente possibile. La stessa CCPC raccomanda ai data holder di effettuare tale verifica e di poter dimostrare e documentare le ragioni dell'eventuale mancata disponibilità di un accesso diretto.

L'adeguamento deve inoltre essere coordinato con gli obblighi di **sicurezza, tutela dei segreti commerciali, proprietà intellettuale e protezione dei dati personali**. Il Data Act si applica infatti sia a dati personali sia a dati non personali, ma non modifica le condizioni di liceità previste dal GDPR: quando i dati richiesti comprendono dati personali riferiti a soggetti diversi dall'utente, la loro comunicazione presuppone comunque l'esistenza di una valida base giuridica ai sensi della normativa sulla protezione dei dati.

La scadenza del 12 settembre 2026 segna quindi un passaggio significativo nell'attuazione del Data Act: **l'accesso ai dati generati dai prodotti connessi non deve più essere considerato soltanto come un diritto da gestire ex post, ma come un requisito da incorporare nell'architettura del prodotto e del**

servizio sin dalla fase di progettazione. Per produttori, fornitori IoT e provider di servizi digitali collegati, la compliance al Data Act diventa pertanto anche una questione di *product design, data architecture* e governance tecnica, oltre che di disciplina contrattuale.

MERCATI DIGITALI

18 Settembre 2026 – Autorità bancaria europea (EBA): EBA: adottate nuove Linee guida sulla gestione dei rischi derivanti dai fornitori terzi non informatici.

L'Autorità bancaria europea (EBA) ha pubblicato le nuove **Linee guida sulla gestione dei rischi derivanti da fornitori terzi di servizi non informatici (EBA/GL/2026/09)**. Le Linee guida sono definitive, ma non ancora applicabili: la relativa data di applicazione sarà individuata successivamente.

L'intervento segna il passaggio da una disciplina incentrata sull'**esternalizzazione** a un modello più ampio di **gestione del rischio da terze parti**. Una volta applicabili, le nuove Linee guida sostituiranno quelle EBA del 2019 sugli accordi di esternalizzazione e completeranno il quadro introdotto dal **DORA**, che disciplina invece i rischi connessi ai fornitori di servizi informatici.
Il nuovo sistema si fonda sul principio di **proporzionalità** e concentra i requisiti più rigorosi sui rapporti con terzi che supportano **funzioni critiche o importanti**, ossia funzioni la cui interruzione può incidere in modo significativo sull'operatività o sul rispetto degli obblighi regolamentari dell'entità finanziaria.

Le Linee guida adottano un approccio riferito all'intero ciclo di vita del rapporto con il fornitore: **valutazione preventiva del rischio, verifica del fornitore, disciplina contrattuale, gestione della subfornitura, monitoraggio continuativo, documentazione ed exit strategy**.
Resta fermo un principio centrale: **il ricorso a un soggetto terzo non trasferisce al fornitore la responsabilità dell'entità regolamentata per il rispetto dei propri obblighi**. Per questo motivo, particolare attenzione dovrà essere riservata alla qualità della due diligence, ai diritti di controllo, alla gestione della catena di subfornitura e alla possibilità di uscire dal rapporto senza compromettere la continuità operativa.

Le entità interessate dovranno inoltre disporre di una **mappatura strutturata dei rapporti con i fornitori terzi**, individuando quelli che supportano funzioni critiche o importanti e coordinando tale presidio con quello già previsto dal DORA per i fornitori informatici.
È previsto un **periodo transitorio di due anni** per l'adeguamento dei rapporti esistenti, che decorrerà dalla futura data di applicazione delle Linee guida.
Sul piano operativo, le imprese del settore finanziario dovrebbero quindi iniziare a riesaminare la propria governance dei fornitori non informatici, verificando censimento dei rapporti, criteri di valutazione del rischio, clausole contrattuali, subfornitura, diritti di controllo, continuità operativa e strategie di uscita.

La novità più rilevante è il progressivo superamento di una gestione frammentata dell'esternalizzazione: **il rischio derivante da terze parti diventa un autonomo ambito di governance, da presidiare in modo integrato lungo l'intero ciclo di vita del rapporto**.

PROPRIETA' INTELLETTUALE E INDUSTRIALE

18 Settembre 2026 – Corte di Giustizia dell'Unione europea: anche un breve post sui social media può costituire un'opera protetta ai sensi della normativa sul diritto d'autore.

La Corte di giustizia dell'Unione europea - **nella causa C-598/24, Gândul Media Network** ,- ha fornito principi decisori e importanti indicazioni sulla tutela mediante diritto d'autore dei contenuti pubblicati sui social network.

La controversia riguardava un testo di appena **22 righe pubblicato su Facebook** da un'insegnante rumena e successivamente riprodotto integralmente, senza preventiva autorizzazione, sul sito di un quotidiano online.

La Corte ha chiarito che **la brevità del testo, il carattere informale della pubblicazione e il fatto che il contenuto sia stato diffuso attraverso un social network non escludono, di per sé, la protezione autoriale**. Ciò che rileva è verificare se il testo costituisca una creazione intellettuale propria dell'autore, espressione di scelte libere e creative, ad esempio nella selezione, disposizione e combinazione delle parole. La verifica concreta spetta al giudice nazionale.

La Corte si è pronunciata anche sull'**eccezione relativa alla cronaca di avvenimenti attuali** prevista dall'art. 5, par. 3, lett. c), della Direttiva 2001/29. Gli Stati membri possono limitare tale eccezione alla riproduzione di brevi estratti, purché la restrizione sia proporzionata e non ne comprometta la finalità. La riproduzione integrale di un'opera può quindi risultare eccedente rispetto allo scopo informativo, salvo, ad esempio, che la sua brevità renda irragionevole una riproduzione soltanto parziale.

La Corte ha invece escluso che l'eccezione possa essere negata in via generale per il solo fatto che la riproduzione produca un **vantaggio economico o commerciale**: anche l'attività giornalistica è normalmente svolta professionalmente e nell'ambito di un'attività economica. Resta comunque necessario che l'utilizzazione sia giustificata dalla finalità informativa e rispetti le altre condizioni previste dalla disciplina sul diritto d'autore.

Per imprese, editori, agenzie di comunicazione e funzioni marketing, la conseguenza pratica è rilevante: **la disponibilità pubblica di un contenuto sui social media non equivale alla sua libera riutilizzabilità**. Prima di riprodurre integralmente post, testi o altri contenuti pubblicati online occorre verificare sia la possibile sussistenza della tutela autoriale sia l'effettiva applicabilità di una specifica eccezione o limitazione al diritto d'autore.

---

18 settembre 2026 – EUIPO: dichiarato decaduto il marchio europeo META per non uso quinquennale.

La Divisione di annullamento dell'EUIPO ha accolto una domanda proposta da Heymeta GmbH e dichiarato la **decadenza integrale del marchio dell'Unione europea n. 18 178 061 "META"**, di titolarità di Meta Platforms, Inc., registrato per una serie di prodotti della classe 9, tra cui altoparlanti, apparecchiature audio e relativo software. La decadenza produce effetti dal **4 febbraio 2026**, data della relativa domanda.

La decisione si fonda sull'art. 58, par. 1, lett. a), del Regolamento sul marchio dell'Unione europea, secondo cui il titolare può decadere dai propri diritti quando, per un periodo ininterrotto di cinque anni, il marchio non sia stato oggetto di **uso effettivo nell'Unione** per i prodotti o servizi registrati e non sussistano motivi legittimi per il mancato uso.

Il profilo più significativo del caso è di natura probatoria. L'EUIPO aveva invitato Meta a produrre le prove dell'uso del marchio, concedendo anche una proroga del termine iniziale. Secondo la decisione, la società **non ha presentato osservazioni né prove dell'uso entro il termine concesso**. In un procedimento di decadenza per non uso, l'onere di provare l'uso effettivo grava sul titolare del marchio, poiché non può essere imposto al richiedente di dimostrare un fatto negativo, ossia l'assenza di utilizzo del segno.

Il provvedimento costituisce un promemoria particolarmente utile per le imprese titolari di portafogli marchi articolati: **la registrazione e il rinnovo del marchio non sono sufficienti a garantirne indefinitamente la tutela**. Decorso il periodo quinquennale, la conservazione del diritto può dipendere dalla capacità di documentare in modo adeguato un uso effettivo del segno in relazione ai prodotti e servizi per i quali è registrato. L'EUIPO conferma infatti che l'assenza di uso effettivo per cinque anni costituisce uno dei presupposti per la decadenza.

Sul piano operativo, le imprese dovrebbero quindi affiancare alla gestione amministrativa del portafoglio marchi una vera **governance delle prove d'uso**, conservando in modo strutturato fatture, cataloghi, materiale pubblicitario, schermate di siti e piattaforme di vendita, dati commerciali e altre evidenze idonee a dimostrare luogo, periodo, natura ed estensione dell'utilizzo. È inoltre opportuno verificare periodicamente che l'elenco dei prodotti e servizi coperto dalle registrazioni continui a corrispondere all'effettivo utilizzo commerciale dei segni.