
Monthly Roundup

Settembre 2026

Settembre 2026

I principali aggiornamenti in materia di TMT & Data Protection del mese di settembre.

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

GARANTE PRIVACY

- Recupero crediti: online la versione aggiornata del vademecum del Garante; [\[Link\]](#)
- La Cassazione conferma la correttezza dell'operato del Garante privacy; [\[Link\]](#)
- Parere sullo schema di decreto legislativo recante "Attuazione della direttiva (UE) 2024/2831 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali". [\[Link\]](#)

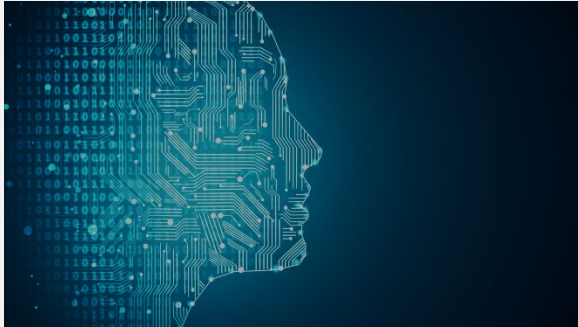
EDPB

- L'EDPB adotta le Linee guida 04/2026 sull'applicazione del potere di imporre sanzioni amministrative in relazione ad altri poteri correttivi previsti dal GDPR; [\[Link\]](#)
- L'EDPB adotta le Linee guida 3/2025 sull'interazione tra il DSA e il GDPR. [\[Link\]](#)

ACN

- Aggiornamento dell'elenco dei soggetti NIS; [\[Link\]](#)
- Vademecum per i soggetti NIS. [\[Link\]](#)

IA e responsabilità d'impresa: cosa cambia con il D.Lgs. 160/2026



Il prossimo 30 settembre entrerà in vigore il **D. Lgs. 160/2026** (il “Decreto”), che completa il quadro nazionale di attuazione della Legge italiana sull'intelligenza artificiale (L. 132/2025).

Sebbene una parte rilevante delle nuove disposizioni riguardi l'impiego dell'intelligenza artificiale (“IA”) per finalità di pubblica sicurezza, il Decreto contiene alcune novità di particolare interesse anche per le imprese, poiché introduce specifici profili di **responsabilità penale**, estende la **responsabilità degli enti** ai sensi del D.Lgs. 231/2001 e rafforza gli strumenti a disposizione dei soggetti che intendano agire per il **risarcimento dei danni** causati dall'utilizzo di sistemi di IA.

Ma cosa prevede il Decreto? E a quali profili devono prestare attenzione le imprese?

Trattamenti di dati biometrici per finalità di pubblica sicurezza

Uno dei profili maggiormente rilevanti disciplinati dal Decreto riguarda l'impiego dell'IA nei trattamenti di dati biometrici per finalità di pubblica sicurezza, distinguendo tra identificazione biometrica remota in tempo reale e utilizzo di tecnologie di riconoscimento facciale a posteriori.

La disciplina consente l'impiego di *dataset* biometrici esclusivamente per specifiche finalità

di polizia, escludendone l'utilizzo per dedurre o inferire caratteristiche vietate dall'AI Act (quali l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche e l'orientamento sessuale) e prevedendo che gli esiti dei sistemi di IA non possano costituire l'unico fondamento di decisioni che producano effetti giuridici nei confronti degli interessati.

L'identificazione biometrica remota in tempo reale è ammessa solo nei casi eccezionali espressamente previsti dalla legge (ad esempio, per la prevenzione di specifiche minacce alla sicurezza pubblica, nonché per la ricerca di persone scomparse o vittime di sequestro di persona, tratta di esseri umani o sfruttamento sessuale), mentre il riconoscimento facciale a posteriori è soggetto a specifiche garanzie e limitazioni (ad esempio, nell'ambito di attività investigative finalizzate all'identificazione di soggetti indiziati della commissione di un reato).

Resta in ogni caso escluso il ricorso a forme di sorveglianza biometrica generalizzata o indiscriminata della popolazione.

L'introduzione del nuovo Articolo 437-bis c.p.

Sul versante penale, il Decreto introduce il **nuovo art. 437-bis c.p.**, rubricato “*Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi*”.

Il reato riguarda chi omette di adottare le misure tecniche di sicurezza necessarie a prevenire malfunzionamenti o alterazioni, o le misure di supervisione umana, nelle fasi di progettazione, addestramento, produzione, immissione sul mercato o uso professionale di sistemi di IA ad alto rischio. Il trattamento sanzionatorio previsto dalla norma è graduato in base alla gravità del rischio generato dalla condotta.

La reclusione va da uno a cinque anni quando il pericolo riguarda la vita o l'incolumità delle

persone e da due a otto anni quando sono coinvolte la sicurezza pubblica o la sicurezza dello Stato.

Il reato ricomprende inoltre le alterazioni illecite del funzionamento dei sistemi di IA realizzate da soggetti estranei al loro ciclo di vita, per le quali sono previste pene da due a sei anni, aumentate nelle ipotesi più gravi.

La pena è invece attenuata nei casi di colpa grave. La previsione attribuisce, pertanto, specifica rilevanza penale agli obblighi di sicurezza e di supervisione dei sistemi di IA ad alto rischio, rafforzando il rilievo degli **adempimenti tecnici e organizzativi** connessi alla loro gestione.

Sotto questo profilo, il Decreto segna un passaggio significativo: obblighi che fino ad oggi erano generalmente percepiti come requisiti di natura tecnico-organizzativa previsti dall'AI Act possono assumere, in determinate circostanze, rilevanza anche sul piano penalistico.

In caso di contestazione del reato, i soggetti che hanno assunto le decisioni o posto in essere le condotte che hanno determinato la violazione possono essere ritenuti personalmente responsabili.

Accanto a tale responsabilità individuale, il Decreto estende però le conseguenze dell'illecito anche all'ente, introducendo specifiche ipotesi di responsabilità da reato ai sensi del D.Lgs. 231/2001.

Le modifiche al D.Lgs. 231/2001: la responsabilità da reato degli enti

Un ulteriore punto fondamentale del Decreto è l'intervento sul **D.Lgs. n. 231/2001**, mediante l'introduzione del **nuovo art. 25-vicies**, rubricato *"Reati commessi con l'uso di sistemi di intelligenza artificiale"*. Le nuove disposizioni ampliano il novero dei reati presupposto, con conseguente

necessità di considerare i rischi connessi all'utilizzo dell'IA nell'ambito delle attività di *risk assessment* e dei presidi previsti dai modelli organizzativi.

Nello specifico, con riferimento alla fattispecie di cui al nuovo art. 437-bis c.p., il Decreto estende altresì il regime della responsabilità amministrativa degli enti, prevedendo l'applicazione di una sanzione pecuniaria compresa tra 600 e 1.000 quote, oltre alle sanzioni interdittive nei casi espressamente previsti dalla disposizione.

Inoltre, l'art. 25-vicies ricomprende tra i reati presupposto anche la fattispecie di cui all'art. 612-quater c.p., relativa alla diffusione illecita di contenuti generati o manipolati mediante sistemi di intelligenza artificiale (c.d. **deepfake**). In tali ipotesi, all'ente possono essere applicate sanzioni pecuniarie comprese tra 200 e 700 quote.

In concreto, l'introduzione delle nuove fattispecie nel sistema dei reati-presupposto impone quindi alle società che sviluppano, distribuiscono o impiegano professionalmente sistemi di IA di procedere a una **valutazione dei relativi rischi** ai fini del D.Lgs. n. 231/2001, verificando l'adeguatezza dei modelli organizzativi, dei presidi di controllo e dei meccanismi interni di attribuzione delle responsabilità.

Con questo intervento legislativo, l'IA entra a pieno titolo nell'ambito dei sistemi di controllo interno e della *governance* aziendale.

Una nuova tutela civilistica

Sul fronte civilistico, il Decreto introduce specifici strumenti processuali destinati ad agevolare le azioni di **risarcimento dei danni, contrattuali ed extracontrattuali**, derivanti dall'utilizzo di sistemi di IA.

L'intervento assume particolare rilievo anche alla luce del ritiro della proposta di AI Liability Directive da parte della Commissione europea, contribuendo a colmare il vuoto normativo che si era venuto a creare in materia.

Il danneggiato potrà agire sia direttamente contro l'impresa che pensa sia responsabile del danno, sia contro l'eventuale impresa assicuratrice (nei limiti della copertura assicurativa).

Infatti, con l'introduzione del Decreto, il giudice potrà emettere un ordine di esibizione, imponendo alla controparte di esibire gli elementi e i documenti funzionali a ricostruire il funzionamento del sistema – tra cui le registrazioni dei *log*, la documentazione concernente la gestione dei rischi, la documentazione tecnica e le informazioni relative alle misure di supervisione umana – quando il ricorrente presenta fatti ed elementi di prova sufficienti a dimostrare *prima facie* la fondatezza della domanda.

Da un punto di vista pratico, ciò significa che la capacità dell'impresa di documentare le modalità di funzionamento del sistema, le attività di gestione del rischio, le misure di supervisione umana e le verifiche effettuate assume un'importanza centrale anche in vista di un eventuale contenzioso.

Inoltre, l'eventuale inottemperanza, senza giustificato motivo, all'ordine di esibizione può assumere rilievo anche ai fini della valutazione degli elementi probatori nel giudizio e può portare all'applicazione di sanzioni pecuniarie.

Assume infine particolare rilievo la previsione relativa alla prova del nesso causale: qualora il danno sia riconducibile alla violazione di uno o più obblighi previsti dall'AI Act, il nesso causale tra la violazione e il danno si presume, salvo prova

contraria. Il Decreto chiarisce altresì che la mera conformità del sistema all'AI Act non è, di per sé, sufficiente ad escludere la responsabilità.

Conclusioni e raccomandazioni operative

Le novità introdotte dal Decreto confermano come l'utilizzo di sistemi di IA può assumere rilievo sotto il profilo penale, civilistico e della responsabilità degli enti, con conseguenze che possono coinvolgere non soltanto i fornitori dei sistemi, ma anche le organizzazioni che li impiegano nell'ambito della propria attività.

Sia la condotta disciplinata dall'art. 437-*bis* c.p. sia le possibili responsabilità sotto il profilo risarcitorio, riguardano la progettazione, l'addestramento, la produzione, l'immissione sul mercato e l'uso professionale dei sistemi di IA.

Tale elenco non è casuale, poiché riproduce la catena del valore delineata dall'AI Act, coinvolgendo i diversi operatori economici, dai *provider* ai *deployer* e ai distributori.

Ne consegue che la responsabilità penale in materia di IA, così come l'esposizione a potenziali richieste di risarcimento del danno e, nei casi previsti, alla responsabilità dell'ente, può interessare qualsiasi impresa che sviluppi, commercializzi o utilizzi professionalmente sistemi di IA ad alto rischio, anche quando tali sistemi siano stati realizzati da soggetti terzi.

In questa prospettiva, il principale effetto del Decreto è quello di rafforzare l'importanza dei presidi organizzativi e documentali già richiesti dall'AI Act.

Gli obblighi relativi alla gestione del rischio, alla supervisione umana, alla sicurezza, alla tracciabilità delle attività svolte e alla conservazione della documentazione tecnica assumono infatti una rilevanza che va oltre la mera conformità normativa, potendo incidere

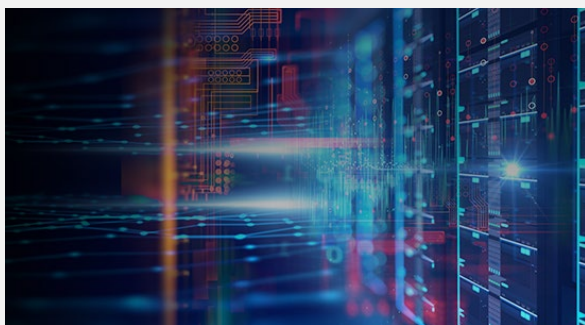
direttamente sulla capacità dell'impresa di dimostrare la correttezza delle proprie scelte e l'adeguatezza delle misure adottate.

Sul piano operativo, le organizzazioni che sviluppano, distribuiscono o utilizzano sistemi di IA dovrebbero pertanto verificare la corretta classificazione dei sistemi impiegati, riesaminare i processi di gestione e documentazione dei rischi, assicurare adeguati meccanismi di tracciabilità e conservazione dei *log* e valutare l'adeguatezza delle procedure interne disciplinanti l'utilizzo dell'IA.

Analoga attenzione dovrebbe essere dedicata ai modelli organizzativi adottati ai sensi del D.Lgs. 231/2001, ai sistemi di controllo interno e, ove opportuno, alle coperture assicurative esistenti.

* * *

Cyber Resilience Act: le nuove Linee Guida della Commissione europea



Il 27 luglio 2026 la Commissione europea ha approvato le [Linee Guida sull'applicazione del Regolamento \(UE\) 2024/2847](#), noto come *Cyber Resilience Act* ("**CRA**" o il "**Regolamento**").

Si tratta del primo quadro orizzontale dell'Unione europea in materia di requisiti di cybersicurezza per i prodotti con elementi digitali, siano essi *hardware*, *software* o combinazioni dei due.

Le Linee Guida non hanno natura vincolante, ma offrono indicazioni operative su diversi aspetti che, nella pratica, possono incidere in modo significativo sulle modalità con cui le imprese dovranno impostare la propria conformità.

I chiarimenti riguardano, tra l'altro, la delimitazione dell'ambito di applicazione del CRA, il trattamento del *software* libero e *open source*, la determinazione del periodo di supporto, la valutazione dei rischi e la gestione delle vulnerabilità.

La pubblicazione assume inoltre particolare rilievo perché, dall'**11 settembre 2026**, trovano applicazione gli obblighi di segnalazione delle vulnerabilità attivamente sfruttate e degli incidenti gravi che incidono sulla sicurezza dei prodotti.

Per le imprese, quindi, il punto è soprattutto capire come tradurre queste regole in processi concreti: quali prodotti rientrano nel perimetro, chi assume le diverse responsabilità, quali informazioni devono essere raccolte e quali procedure devono essere già operative per poter intervenire tempestivamente in caso di vulnerabilità o incidente.

Ambito di applicazione: quali prodotti rientrano nel CRA

Il CRA si applica ai prodotti con elementi digitali, *hardware* o *software*, immessi sul mercato dell'UE la cui destinazione d'uso o utilizzo ragionevolmente prevedibile includa una

connessione dati¹, diretta o indiretta, a un dispositivo o a una rete.

Il perimetro è quindi potenzialmente molto ampio e può comprendere, ad esempio, *software* autonomi, app e programmi informatici, dispositivi IoT, *laptop* e *tablet*, circuiti integrati e schede madri, oltre a prodotti composti da *hardware* e *software* commercializzati separatamente ma destinati a funzionare insieme.

Con riferimento al **software**, le Linee Guida distinguono in modo particolare tra il *software* che costituisce un prodotto immesso sul mercato e i servizi forniti esclusivamente da remoto. Rientra nel CRA il *software* che viene scaricato, installato o comunque messo a disposizione dell'utente per essere eseguito sul suo sistema informatico.

È il caso, ad esempio, di un'estensione del *browser* o di un'app sviluppata mediante tecnologie *web* ma destinata all'esecuzione locale. Non è invece sufficiente che l'utente possa accedere a una funzionalità *software* tramite una connessione *internet*: quando il *software* viene eseguito esclusivamente da remoto, il solo accesso a tale funzionalità non determina, di per sé, la qualificazione come prodotto con elementi digitali.

La distinzione è particolarmente importante per i modelli basati su cloud e SaaS. Una *web* app accessibile attraverso un *browser* può, in linea generale, rimanere fuori dal perimetro del CRA quando costituisce un servizio erogato da remoto; al contrario, il sito o il servizio può rientrare nel Regolamento quando assume i caratteri di un trattamento remoto dei dati che integra il prodotto.

¹ Le Linee Guida chiariscono che per "connessione dati" deve intendersi uno scambio di informazioni codificate in forma digitale: la mera presenza di componenti elettroniche o di segnali elettrici che si limitano ad attivare o alimentare una

Anche per questo motivo, la qualificazione non può essere effettuata sulla base della sola etichetta commerciale utilizzata per descrivere il servizio, ma richiede un esame concreto delle modalità tecniche con cui il *software* viene fornito e utilizzato.

Per l'**hardware**, invece, il canale di distribuzione è irrilevante. Quando il *software* è necessario per il funzionamento, la configurazione, il controllo o l'utilizzo dell'hardware secondo la sua destinazione d'uso, i diversi elementi possono essere considerati come un unico prodotto con elementi digitali.

È il caso, ad esempio, di una stampante di rete accompagnata dai relativi driver o di un dispositivo *wearable* utilizzabile attraverso la relativa *companion app*.

Software libero e open source

Uno dei chiarimenti più rilevanti riguarda il rapporto tra CRA e *software* libero e *open source* (FOSS, *free and open-source software*). Ai fini del Regolamento, un *software* può essere qualificato come FOSS quando è distribuito con una licenza libera o *open source* che ne consente l'accesso, l'utilizzo, la modifica e la redistribuzione e quando il relativo codice sorgente è pubblicamente disponibile.

La questione della responsabilità, tuttavia, non dipende dalla sola possibilità tecnica di modificare il codice, ma dal ruolo effettivamente svolto nell'organizzazione e nella gestione del progetto.

In questo contesto, le Linee Guida attribuiscono rilievo alla figura dei c.d. ***maintainer***, vale a dire i soggetti che esercitano il controllo principale

funzione, senza veicolare informazioni digitalmente codificate, non è di per sé sufficiente a determinare l'applicazione del CRA.

sullo sviluppo, sul rilascio delle versioni e sulle decisioni relative alla distribuzione e alla *governance* del progetto. Il semplice contributo allo sviluppo del codice non è invece, di per sé, sufficiente a far sorgere una responsabilità ai sensi del CRA².

Un altro aspetto importante riguarda la natura commerciale del *software*. Il fatto che un progetto sia disponibile gratuitamente non è sufficiente, da solo, a escludere l'applicazione del CRA.

La valutazione deve tenere conto delle modalità con cui il *software* viene effettivamente fornito e monetizzato. Può assumere rilievo, per esempio, il pagamento richiesto per il *software* o per i file binari compilati, il fatto che il prodotto costituisca uno strumento per monetizzare altri beni o servizi, oppure che l'accesso a determinate versioni, aggiornamenti o funzionalità essenziali sia subordinato a un corrispettivo.

Anche il trattamento di dati personali può rilevare quando non sia necessario per esigenze di sicurezza, compatibilità o interoperabilità.

Al contrario, la semplice offerta di servizi professionali a pagamento non rende automaticamente commerciale il *software*. Un progetto può infatti rimanere al di fuori della nozione di immissione sul mercato quando il *software* è liberamente disponibile e i servizi di consulenza, formazione, installazione o assistenza vengono acquistati separatamente e facoltativamente.

Anche una donazione volontaria, quando non condiziona l'accesso al *software* o alle sue funzionalità, non determina necessariamente la

natura commerciale del progetto. Allo stesso modo, il fatto che lo sviluppo sia finanziato da un'impresa, da un ente pubblico o da uno sponsor non è, di per sé, decisivo: ciò che rileva è il modo in cui il *software* viene successivamente messo a disposizione sul mercato.

Il CRA prevede inoltre una disciplina specifica per gli ***open-source software steward***, cioè le persone giuridiche, diverse dai fabbricanti, che forniscono in modo sistematico e continuativo un supporto allo sviluppo di FOSS destinato ad attività commerciali e ne sostengono la sostenibilità nel tempo. Si tratta di un regime specifico, pensato per tenere conto del particolare ruolo svolto da questi soggetti nell'ecosistema *open source*.

Tra gli obblighi previsti rientrano, in particolare, l'adozione di una politica di cybersicurezza, la cooperazione con le autorità di vigilanza e, nei casi previsti dal Regolamento, la segnalazione delle vulnerabilità attivamente sfruttate e degli incidenti gravi che incidano sulla sicurezza dei prodotti

Le Linee Guida aiutano a distinguere l'incidenza di tali obblighi in funzione del tipo di supporto fornito. Un'attività esclusivamente non tecnica, come quella relativa al *branding*, alla *governance*, all'organizzazione di eventi o alla raccolta di donazioni, non comporta automaticamente gli stessi obblighi di uno *steward* che mette a disposizione infrastrutture tecniche oppure contribuisce direttamente allo sviluppo del *software* e alla gestione delle relative correzioni di sicurezza.

² I *"maintainer"* sono coloro (persone fisiche o giuridiche) che pubblicano il *software* libero e *open source* ed esercitano il controllo principale sul suo sviluppo, sul rilascio delle versioni e sulle decisioni relative alla distribuzione e alla *governance*. I *"contributor"*, invece, sono coloro che contribuiscono allo

sviluppo di tale *software open source*, senza tuttavia esercitare il controllo sul rilascio delle versioni, sulle *roadmap* o sulle decisioni di *governance*.

Valutazione di conformità e valutazione dei rischi cyber

Il CRA distingue tra prodotti con elementi digitali "ordinari", prodotti "importanti" (di classe I e II) e prodotti "critici". Questa classificazione è rilevante soprattutto perché incide sulla procedura con cui il fabbricante deve dimostrare la conformità del prodotto prima della sua immissione sul mercato. Per individuare la categoria di appartenenza non è sufficiente guardare alla descrizione commerciale del prodotto.

Occorre considerare la **funzionalità principale**, individuata sulla base delle caratteristiche tecniche e dell'utilizzo previsto. Le funzioni meramente accessorie non determinano, da sole, la classificazione.

Un prodotto sarà quindi "importante" o "critico" quando la sua funzionalità principale rientra in una delle categorie previste dagli Allegati III e IV del CRA.

La classificazione produce effetti diretti anche sulle modalità con cui il fabbricante è tenuto a comprovare la conformità del prodotto ai requisiti essenziali dell'Allegato I³.

Accanto alla classificazione esiste un secondo elemento, strettamente collegato, che le Linee Guida considerano centrale: la **valutazione dei rischi cyber** (art. 13, par. 2, del CRA). La valutazione del rischio non costituisce, infatti, dovrebbe orientare l'intero percorso di conformità.

³ Per la generalità dei prodotti – quelli che non ricadono nelle categorie degli Allegati III e IV – è ammesso il ricorso al modulo A di controllo interno, con autovalutazione del fabbricante. Per i prodotti importanti di classe I la medesima modalità di autovalutazione è consentita soltanto ove il fabbricante applichi integralmente le norme armonizzate, le specifiche comuni o i sistemi europei di certificazione della cibersecurity pertinenti, coprendo così tutti i rischi associati alla funzionalità principale del prodotto; in caso contrario, il fabbricante deve necessariamente rivolgersi a un organismo

Dall'analisi dei rischi dipendono la scelta delle misure di sicurezza, l'individuazione dei requisiti essenziali applicabili e, in una certa misura, anche la determinazione del periodo di supporto.

In concreto, il fabbricante deve considerare il modo in cui il prodotto è progettato e destinato a essere utilizzato, gli usi ragionevolmente prevedibili, gli utenti e gli ambienti di impiego, le minacce rilevanti, il possibile impatto di un incidente, le interfacce esposte, le componenti *hardware* e *software*, le dipendenze da soggetti o servizi esterni, i servizi remoti e i rischi connessi alla catena di fornitura, tenendo conto anche delle misure tecniche e organizzative già adottate.

La valutazione deve inoltre essere aggiornata durante il periodo di supporto, in modo da riflettere l'evoluzione dei rischi.

Un elemento particolarmente significativo delle Linee Guida è che, quando i rischi individuati non possono essere adeguatamente gestiti con l'architettura esistente, la risposta non può limitarsi alla predisposizione di documentazione o di misure organizzative.

Può rendersi necessario intervenire sul progetto del prodotto, sulla sua architettura o sulle sue funzionalità, fino a rivederne, nei casi più rilevanti, lo stesso scopo previsto.

Le esigenze commerciali o di costo non sono, di per sé, sufficienti a giustificare il mantenimento di

notificato. Per i prodotti importanti di classe II e per i prodotti critici la valutazione da parte di terzi indipendenti è invece sempre obbligatoria; per i critici, in particolare, il fabbricante è chiamato a conseguire un certificato di cibersecurity europeo di livello "sostanziale" o superiore ai sensi del Regolamento (UE) 2019/881. Un regime di favore è infine previsto per i *software* liberi e *open source* qualificati come importanti, che restano soggetti al solo regime ordinario di autovalutazione.

un rischio incompatibile con i requisiti essenziali del CRA. La valutazione del rischio deve inoltre essere accompagnata da un'adeguata **due diligence sulle componenti integrate**.

Il fabbricante è chiamato a prestare attenzione, sia al momento della selezione sia nel corso del ciclo di vita del prodotto, all'affidabilità dei componenti *hardware* e *software* di terze parti, delle soluzioni di elaborazione dati a distanza e dei servizi remoti dai quali il prodotto dipende.

La valutazione cambia, tuttavia, quando si considerano infrastrutture esterne che non siano state progettate dal fabbricante e che non supportino direttamente una funzione del prodotto, come una rete pubblica o un sistema di *back-end* di un terzo estraneo alla sua architettura.

Tali elementi restano esterni al prodotto, ma non possono essere ignorati: il fabbricante deve comunque tenerne conto nella valutazione complessiva dei rischi e adottare, ove necessario, misure di mitigazione attraverso la progettazione del prodotto e le informazioni o istruzioni fornite agli utenti.

Periodo di supporto e gestione delle vulnerabilità

Le Linee Guida intervengono in modo significativo anche sul **periodo di supporto** (art. 13, par. 8, del CRA). I cinque anni previsti dal Regolamento devono essere letti come una soglia minima e non come un periodo automaticamente applicabile a tutti i prodotti.

La durata del supporto deve essere coerente con il periodo durante il quale ci si può ragionevolmente attendere che il prodotto venga utilizzato, tenendo conto della sua natura e delle aspettative degli utenti.

La conseguenza pratica è importante: un prodotto destinato a rimanere in uso per un periodo significativamente più lungo di cinque anni potrà richiedere un supporto più esteso.

La determinazione della durata del supporto dovrebbe quindi essere collegata alla vita utile attesa del prodotto e non essere trattata come una scelta meramente standardizzata.

Per i soli *software*, il CRA (art 13, par. 10) introduce una specifica forma di flessibilità: il fabbricante può concentrare la correzione delle vulnerabilità sull'ultima versione immessa sul mercato, purché l'utente possa effettuare gratuitamente l'aggiornamento. Le Linee Guida precisano che l'assenza di "costi aggiuntivi" non esclude le normali attività operative necessarie per installare l'aggiornamento.

Non sono normalmente considerati costi aggiuntivi, ad esempio, le ordinarie attività di *test*, configurazione o aggiornamento delle dipendenze *software*.

Diverso è il caso in cui l'aggiornamento richieda l'acquisto obbligatorio di nuovo *hardware*, la sostituzione dell'infrastruttura o una modifica sostanziale dell'ambiente operativo.

Resta in ogni caso fermo che la limitazione del supporto all'ultima versione non esonera il fabbricante dagli altri obblighi di gestione delle vulnerabilità (Parte II dell'Allegato I) e di segnalazione degli incidenti (art. 14).

Obblighi di segnalazione: il termine decorre dalla consapevolezza

Il CRA impone al fabbricante di notificare simultaneamente ad ENISA e al CSIRT di riferimento le vulnerabilità contenute nel prodotto che risultano attivamente sfruttate e gli incidenti gravi aventi impatto sulla sicurezza del prodotto.

Le Linee Guida chiariscono un aspetto particolarmente importante per l'organizzazione interna delle imprese: il termine per la segnalazione inizia a decorrere dal momento in cui il fabbricante acquisisce una sufficiente **consapevolezza dell'evento**.

Tale consapevolezza si determina quando, sulla base di una prima valutazione, il fabbricante raggiunge un ragionevole grado di certezza circa il fatto che una vulnerabilità sia attivamente sfruttata o che si sia verificato un incidente grave.

Da quel momento, il sistema interno deve essere in grado di attivare tempestivamente il flusso di segnalazione. In particolare, il CRA prevede un primo *early warning* entro **24 ore**, seguito dalla notifica principale entro **72 ore**.

Per una vulnerabilità attivamente sfruttata, la relazione finale deve essere trasmessa non oltre 14 giorni dalla disponibilità di una misura correttiva o di mitigazione; per un incidente grave, la relazione finale deve essere presentata entro un mese dalla notifica delle 72 ore.

La Commissione chiarisce inoltre che l'obbligo può riguardare anche vulnerabilità presenti in componenti di terze parti, quando tali vulnerabilità risultino effettivamente sfruttabili nel prodotto del fabbricante.

Non è invece prevista una segnalazione retroattiva per vulnerabilità che fossero già note al fabbricante come attivamente sfruttate prima dell'11 settembre 2026.

Anche la comunicazione agli utenti deve essere gestita con attenzione. L'informazione dovrebbe essere adeguata al rischio e alle caratteristiche del prodotto e, nei contesti più sensibili, la divulgazione di dettagli tecnici eccessivamente

specifici potrebbe aumentare il rischio di ulteriori attacchi.

La gestione della comunicazione deve quindi trovare un equilibrio tra l'esigenza di informare tempestivamente gli utenti interessati e quella di non amplificare il rischio per la sicurezza del prodotto.

Le principali scadenze

Il calendario di applicazione del CRA si sviluppa su più date. La prima è l'**11 settembre 2026**, quando diventano applicabili gli obblighi di segnalazione previsti dall'articolo 14. La disciplina generale del CRA troverà invece piena applicazione dall'**11 dicembre 2027**.

I certificati UE di esame del tipo e le relative decisioni di approvazione rilasciati nel quadro della precedente normativa di armonizzazione e relativi ai requisiti di cybersicurezza restano validi, salvo diversa previsione, fino all'**11 giugno 2028**, purché non scadano prima⁴.

Per i prodotti progettati prima della data di applicazione del CRA ma immessi sul mercato successivamente, il fabbricante non è tenuto a una integrale riprogettazione, ma deve svolgere la valutazione dei rischi di cybersicurezza e dimostrare, sulla base di essa, che il prodotto incorpora misure di sicurezza adeguate ai rischi individuati.

Restano, secondo i casi, gli ulteriori adempimenti previsti dal CRA, tra cui la valutazione della conformità, la documentazione tecnica, la dichiarazione UE di conformità, la marcatura CE, i processi di gestione delle vulnerabilità, l'aggiornamento della valutazione del rischio e le informazioni e istruzioni destinate agli utenti.

⁴ I certificati UE di esame del tipo e le relative decisioni di approvazione cui si riferisce l'articolo 69 del CRA restano validi

fino all'11 giugno 2028, salvo scadenza anteriore o diversa previsione della normativa di armonizzazione applicabile.

Conclusioni

Le Linee Guida offrono un quadro interpretativo del CRA più concreto su numerosi aspetti che, per le imprese, saranno decisivi nella fase di attuazione. In particolare, in vista delle prossime scadenze, le imprese dovrebbero partire da una ricognizione dei propri prodotti e delle relative componenti, verificando anzitutto quali rientrino nel perimetro del CRA e quale sia la loro corretta classificazione.

Su questa base sarà possibile collegare la valutazione del rischio alla funzionalità principale del prodotto e definire il percorso di conformità applicabile. Un secondo passaggio riguarda la costruzione (laddove non sia stato già implementato) di un processo strutturato di gestione delle vulnerabilità.

È necessario che le responsabilità siano chiaramente individuate, che esistano canali interni per raccogliere le segnalazioni e che l'organizzazione sia in grado di far decorrere correttamente i termini di 24 e 72 ore, nonché quelli previsti per le relazioni finali.

La questione non riguarda soltanto il *team cybersecurity*: in molti casi coinvolgerà anche le funzioni legale, *compliance*, prodotto, qualità e comunicazione.

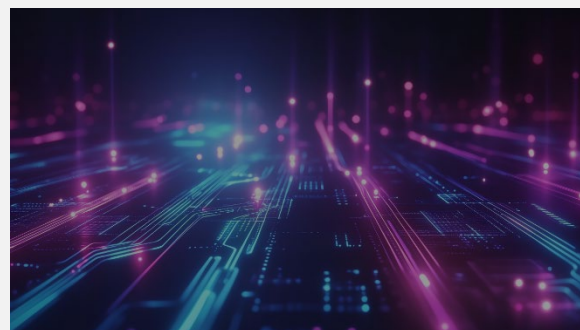
Particolare attenzione dovrà essere dedicata anche alle dipendenze esterne, ai componenti open source e ai servizi cloud o SaaS, verificando non soltanto che tali componenti siano affidabili, ma anche che i rapporti con i relativi fornitori consentano all'impresa di ottenere tempestivamente le informazioni necessarie per gestire vulnerabilità e incidenti.

Infine, sarà utile verificare il coordinamento tra il CRA e gli altri quadri normativi europei che possono incidere sulle medesime organizzazioni, tra cui la NIS2, il GDPR, l'AI Act e, per i soggetti

interessati, il DORA. L'obiettivo dovrebbe essere quello di evitare la creazione di processi paralleli e costruire invece un sistema coerente di gestione del rischio *cyber*, capace di coprire gli obblighi che derivano dalle diverse discipline.

* * *

Data Act: dal 12 settembre 2026 accessibilità per impostazione predefinita dei dati generati da prodotti connessi e servizi correlati



A decorrere dal 12 settembre 2026, diventa applicabile, ai prodotti connessi e ai servizi correlati immessi sul mercato a partire da tale data, l'obbligo di accessibilità dei dati per impostazione predefinita previsto dall'art. 3(1) del [Regolamento \(UE\) 2023/2854](#) (il "**Data Act**" o il "**Regolamento**").

Si tratta di un'evoluzione significativa per i **fabbricanti e fornitori di servizi**, che dal 12 settembre 2026 dovranno garantire – già a livello progettuale – un **accesso agevole, sicuro e strutturato ai dati generati dall'uso del prodotto o del servizio**.

Più in particolare, l'obbligo risultante dall'art. 3(1) si applica ai prodotti connessi e ai servizi correlati **immessi** sul mercato dopo il 12 settembre 2026, mentre le restanti disposizioni del Data Act trovano applicazione, salve le specifiche decorrenze previste dal Regolamento, già dal 12 settembre 2025.

Il quadro normativo del Data Act

Il Data Act introduce regole armonizzate su: (i) la **messa a disposizione dei dati** dei prodotti e dei servizi correlati agli **utenti**; (ii) la **messa a disposizione dei dati** da parte dei *data holder* a **destinatari terzi**; (iii) la **condivisione**, in casi eccezionali, **con enti del settore pubblico**, la Commissione, la BCE e organismi dell'Unione; (iv) la **facilitazione del passaggio** (*switching*) **tra servizi di trattamento dei dati**; (v) la **protezione da accessi illeciti di soggetti terzi ai dati non personali**; e (vi) lo **sviluppo di standard di interoperabilità**.

Il raccordo con la disciplina sulla protezione dei dati personali è esplicito: il Data Act fa salve le norme UE e nazionali in materia di protezione dei dati personali, *privacy* e riservatezza delle comunicazioni, con prevalenza, in caso di conflitto, della disciplina sulla protezione dei dati personali⁵.

In linea generale, il Regolamento mira a promuovere un **mercato dei dati aperto e competitivo**, favorendo la disponibilità, accessibilità e riutilizzabilità delle informazioni generate dall'uso di prodotti connessi e servizi correlati, con particolare riferimento all'ambito industriale.

Il Data Act costruisce una disciplina differenziata in relazione alla funzione svolta da ciascun operatore nella catena del valore dei dati, individuando specifici obblighi a carico di:

- **fabbricanti di prodotti connessi** - tenuti alla progettazione in forma *data-accessible*;
- **fornitori di servizi correlati** - vincolati ai medesimi requisiti di accessibilità;
- **data holder** - soggetti che, in forza del Regolamento o di altre norme,

detengono il diritto o l'obbligo di utilizzare e rendere disponibili i dati;

- **prestatori di servizi di trattamento dei dati** - tenuti a rimuovere ostacoli tecnici e contrattuali allo *switching*.

Il Regolamento riconosce inoltre all'utente la facoltà di indirizzare i dati verso soggetti terzi di propria scelta, imponendo al *data holder* di renderli disponibili per servizi prestati da operatori diversi dal fabbricante originario o dal fornitore del servizio correlato.

La condivisione con enti pubblici o istituzioni UE ha invece carattere eccezionale, essendo ammessa solo in presenza dei presupposti tassativamente previsti (in particolare situazioni di emergenza e specifiche finalità di interesse pubblico).

Sul piano contrattuale, il Data Act introduce meccanismi diretti a prevenire che condizioni squilibrate pregiudichino l'esercizio dei diritti di accesso e utilizzo.

Sul versante dei servizi di trattamento dei dati, l'obiettivo è quello di rendere effettivamente praticabile la sostituzione del fornitore, limitando i vincoli tecnologici e contrattuali al trasferimento di dati, applicazioni e altri elementi digitali e prevedendo la progressiva eliminazione dei relativi costi.

Per le **imprese**, la conformità richiede dunque una **verifica integrata delle caratteristiche di prodotti e servizi**, dei processi di gestione dei dati, delle infrastrutture tecnologiche e degli assetti contrattuali.

⁵ FAQ Data Act, 22 January 2026, Version 1.4, par. 1.

Il nuovo obbligo di accessibilità dei dati *by design* nel Data Act e il rapporto con il GDPR

Come già anticipato, l'art. 3(1) del Data Act pone a carico dei fabbricanti di prodotti connessi e dei fornitori di servizi correlati uno **specifico requisito di progettazione**, richiedendo che i dati generati dal prodotto o dal servizio correlato, compresi i pertinenti metadati necessari a interpretarli e utilizzarli, siano **accessibili all'utente per impostazione predefinita**, in modo facile, sicuro e gratuito e in un formato completo, strutturato, di uso comune e leggibile meccanicamente. Ove pertinente e tecnicamente fattibile, i dati devono inoltre essere direttamente accessibili all'utente.

Pur usando testualmente le parole "per impostazione predefinita", la norma incorpora un vero e proprio obbligo di accessibilità *by design*: le caratteristiche tecniche del prodotto e del servizio devono essere concepite, sin dalla fase progettuale, in modo da rendere concretamente esercitabile il diritto di accesso dell'utente.

La disposizione va letta in coordinamento con il principio di *data protection by design and by default* sancito dall'**art. 25 del Regolamento (UE) 2016/679 ("GDPR")**. Il considerando 8 del Data Act richiama espressamente i principi di minimizzazione e di protezione dei dati fin dalla progettazione e per impostazione predefinita, precisando che tutte le parti coinvolte nella condivisione dei dati dovrebbero adottare misure tecniche e organizzative adeguate al fine di tutelare i diritti fondamentali degli interessati.

In questa prospettiva, assume particolare rilievo il provvedimento adottato dal Garante per la protezione dei dati personali (il "**Garante**" o l'**"Autorità"**) l'11 giugno 2026⁶, nel quale l'Autorità ha accertato che l'erronea

configurazione del protocollo informatico aveva consentito a soggetti non autorizzati l'accesso a documenti contenenti dati personali, con conseguente violazione degli artt. 5(1)(f), 5(2) e 25 del GDPR.

Il Garante ha ricollegato tale configurazione alla mancata predisposizione di sistemi idonei a garantire un accesso selettivo alla documentazione, in coerenza con il principio di protezione dei dati fin dalla progettazione.

Lo stesso approccio rileva nell'attuazione del Data Act: l'accessibilità dei dati richiesta *by design* non equivale, infatti, a un accesso indiscriminato. Quando sono coinvolti dati personali, la configurazione tecnica dei meccanismi di accesso dovrà essere strutturata in modo da conciliare l'esigenza di effettiva disponibilità dei dati con i requisiti di sicurezza, autorizzazione e protezione imposti dal GDPR.

Ne deriva che l'accessibilità *by design* e *privacy by design and by default* devono essere considerate come requisiti **complementari**, destinati a operare congiuntamente nella progettazione dei prodotti connessi e dei servizi correlati.

Conclusioni

Il Data Act segna il passaggio da un modello in cui i dati generati dai prodotti connessi restavano prevalentemente nella disponibilità dei fabbricanti e dei fornitori a un sistema fondato sulla loro effettiva accessibilità, mobilità e condivisione controllata.

Per gli operatori economici, l'adeguamento non può pertanto ridursi a un intervento formale sulla documentazione contrattuale: richiede una **revisione coordinata della progettazione di prodotti e servizi**, delle architetture

⁶ <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10266034>

tecnologiche, dei sistemi di autorizzazione e dei processi di gestione dei dati.

Quando siano coinvolti dati personali, questo percorso dovrà svolgersi nel pieno rispetto del

GDPR: l'accessibilità *by design* prevista dal Data Act dovrà essere **attuata insieme ai principi di minimizzazione, sicurezza e protezione dei dati fin dalla progettazione e per impostazione predefinita.**

Per maggiori informazioni e approfondimenti

Carlo Impalà

Partner e Responsabile Osservatorio TMT&DP

Carlo.Impala@MorriRossetti.it

Morri Rossetti & Franzosi

Osservatorio TMT&DP





OSSERVATORIO TMT·DATA PROTECTION

di Morri Rossetti & Franzosi

Piazza Eleonora Duse, 2
20122 Milano

MorriRossetti.it

Osservatorio-dataprotection.it