

EU Data Act e sicurezza IoT: cosa cambia per le imprese italiane



Il Regolamento (UE) 2023/2854, noto come EU Data Act, è pienamente applicabile dal 12 settembre 2025. Non è un regolamento sulla privacy nel senso in cui lo intendiamo dal 2018: non riguarda principalmente i dati personali degli individui. Riguarda la proprietà e il controllo dei dati generati dall'uso di prodotti connessi, dai macchinari industriali agli elettrodomestici intelligenti, dai veicoli connessi ai dispositivi medici. Il suo impatto sul panorama della sicurezza informatica è strutturale e scarsamente discusso nel dibattito professionale italiano.

Il problema centrale, dal punto di vista della cybersecurity, è questo: il Data Act impone alle aziende di aprire canali tecnici di accesso ai dati dei loro dispositivi IoT verso terze parti designate dagli utenti. Ogni apertura controllata è anche una potenziale superficie di attacco. Ogni API obbligatoria è anche un endpoint da proteggere. Ogni terza parte che riceve dati è anche un rischio di compromissione della supply chain informativa.

Cosa dice il Data Act: la struttura normativa essenziale

Il testo ufficiale del Data Act è organizzato in **dieci capitoli** (da I a X), come si evince dalla struttura completa del regolamento. La Commissione Europea, nella propria scheda di sintesi, descrive sei aree tematiche principali successive alle disposizioni generali del Capitolo I; la numerazione intera del testo legislativo arriva tuttavia a dieci capitoli.

Per le imprese che gestiscono dispositivi connessi, i capitoli più rilevanti sono tre.

Il **Capitolo II** stabilisce il diritto degli utenti di accedere ai dati grezzi e pre-processati generati dai prodotti connessi che posseggono, noleggiano o affittano, e di condividerli con terze parti di loro scelta. Per “prodotto connesso” il regolamento intende qualsiasi dispositivo in grado di raccogliere e trasmettere dati: macchinari industriali, veicoli, elettrodomestici intelligenti, dispositivi medici, attrezzature agricole, edifici intelligenti. Non si tratta di una definizione ristretta: rientra praticamente qualsiasi dispositivo IoT commercializzato nell'UE.

Il **Capitolo III** regola la condivisione obbligatoria tra imprese nei casi in cui un'azienda sia tenuta per legge a mettere dati a disposizione di un'altra. Il principio guida è il FRAND (Fair, Reasonable and Non-Discriminatory): chi detiene i dati può chiedere una remunerazione, ma proporzionale ai costi e non discriminatoria verso le PMI o gli enti di ricerca.

Il **Capitolo V** prevede che le autorità pubbliche possano richiedere accesso a dati privati in casi di necessità eccezionale (*exceptional need*). Come chiarisce la Commissione Europea, tali situazioni comprendono le emergenze pubbliche (disastri naturali, pandemie, grandi incidenti di cybersecurity) e circostanze non emergenziali di interesse pubblico. Le organizzazioni che detengono dati rilevanti, dagli operatori di trasporto alle infrastrutture intelligenti, sono soggette a queste disposizioni.

La timeline di implementazione non è monolitica. Le disposizioni principali sono in vigore dal 12 settembre 2025. I requisiti di progettazione *access by design* per i nuovi prodotti si applicheranno dal **12 settembre 2026**: i dispositivi messi in commercio dopo quella data dovranno essere progettati sin dall'origine per consentire l'accesso ai dati

direttamente, in modo sicuro e gratuito (art. 3, par. 1). Dal **12 gennaio 2027**, i fornitori di servizi cloud non potranno più applicare switching charges per il cambio di provider.

Chi è il “data holder” e perché il manifatturiero italiano è in prima linea

La distinzione centrale del Data Act è tra *data holder* (il soggetto che controlla l'accesso ai dati, tipicamente il produttore o il fornitore del servizio connesso) e utente (chi usa il prodotto). Nella maggior parte degli ecosistemi IoT il produttore del dispositivo è automaticamente il data holder, salvo che abbia contrattualmente delegato tale ruolo a un terzo.

Il manifatturiero italiano è uno dei settori più direttamente coinvolti, per tre ragioni convergenti. Prima: l'Italia ha una delle filiere di automazione industriale più dense d'Europa, con migliaia di produttori di macchinari connessi in Emilia-Romagna, Lombardia e Veneto. Seconda: secondo il Rapporto CLUSIT 2026, l'Italia è stata bersaglio del 9,6% degli attacchi informatici globali nel 2025 con una crescita del 42% rispetto all'anno precedente, collocandosi quarta al mondo e prima in Europa per numero assoluto di attacchi, una sproporzione che rivela vulnerabilità strutturali già esistenti.

Secondo l'IBM X-Force Threat Intelligence Index 2025, il settore manifatturiero è il più colpito a livello globale per il quarto anno consecutivo, con circa il 26% di tutti gli attacchi ransomware documentati. Terza: il settore agricolo, tradizionalmente meno digitalizzato, ha visto un'impennata nell'adozione di macchinari connessi e sensori IoT grazie ai piani nazionali Industria 4.0 e al PNRR, portando migliaia di aziende in scope regolatorio senza adeguata cultura della

sicurezza dei dati.

Come già discusso su ICT Security Magazine nell'approfondimento sulla gestione delle vulnerabilità nei sistemi IoT, la mancanza di crittografia espone i dati trasmessi da dispositivi IoT con conseguenze economiche documentate. Ora il Data Act aggiunge a questa vulnerabilità tecnica un obbligo legale di condivisione che amplifica l'esposizione se non gestito con i controlli appropriati.

Il paradosso della sicurezza: aprire i dati senza aprire la superficie di attacco

Il Data Act pone il team di sicurezza davanti a una tensione fondamentale che non ha precedenti nella normativa europea recente. La NIS2 chiede di proteggere meglio i sistemi. Il Data Act chiede di renderli più accessibili a terze parti. Il Cyber Resilience Act chiede *security by design*. Il Data Act chiede *access by design*. Come si conciliano questi obiettivi?

La risposta della norma si articola attraverso più disposizioni. L'**articolo 4(2)** consente ai data holder di limitare o vietare l'accesso ai dati nei contratti con gli utenti qualora tale accesso pregiudichi gravemente la sicurezza del prodotto connesso o del servizio correlato, a condizione che il requisito di sicurezza violato sia previsto da una norma UE o nazionale. L'**articolo 5(9-11)** disciplina le misure tecnico-organizzative necessarie a preservare la riservatezza dei segreti commerciali nella condivisione con terze parti. L'**articolo 11** autorizza i data holder ad applicare misure tecniche di protezione appropriate, inclusi smart contract e cifratura, per prevenire accessi non autorizzati.

Non si tratta di raccomandazioni: sono parte integrante degli

obblighi di compliance. In pratica, ogni API sviluppata per soddisfare gli obblighi del Data Act deve essere progettata, testata e monitorata con lo stesso rigore di qualsiasi interfaccia critica. I requisiti tecnici minimi includono: cifratura end-to-end per tutti i trasferimenti, autenticazione forte dei destinatari dei dati, log di audit completi di tutti gli accessi e le condivisioni, procedure di incident response specifiche per violazioni legate ai flussi Data Act, verifica dell'identità e dell'autorizzazione delle terze parti prima di ogni condivisione.

I framework di riferimento raccomandati per questa implementazione sono la NIS2, la ISO/IEC 27001 e gli standard ENISA per la sicurezza IoT. La conformità a questi framework costituisce anche la dimostrazione, coerente con le finalità del Data Act, di aver adottato misure di sicurezza adeguate.

Il rischio concreto: la terza parte come nuovo vettore di attacco

Il punto più critico dal punto di vista della sicurezza è la gestione delle terze parti designate dagli utenti. L'articolo 5 del Data Act impone che, su richiesta dell'utente, il data holder trasmetta i dati a una terza parte designata nelle stesse condizioni tecniche previste per l'utente. In pratica, se un'azienda manifatturiera raccoglie dati da un macchinario e li mette a disposizione del cliente tramite un'API, deve essere in grado di trasmettere gli stessi dati a un manutentore terzo, a un'assicurazione, a un fornitore di servizi di ottimizzazione o a qualsiasi altro soggetto che l'utente scelga.

La terza parte ha l'obbligo contrattuale di usare i dati solo per gli scopi concordati e di cancellarli quando non più necessari. I contratti con le terze parti devono essere il più possibile protettivi riguardo ai segreti commerciali e alla sicurezza informatica, ma la norma lascia ampi margini

interpretativi su cosa ciò significhi in pratica. L'assenza di standard obbligatori per la postura di sicurezza delle terze parti è una delle lacune più criticate dagli operatori del settore.

Il rischio operativo è reale. Un data holder che apre i dati di un macchinario industriale a una terza parte di manutenzione non sa con certezza quale sia la postura di sicurezza di quella terza parte. Se la terza parte viene compromessa, i dati del macchinario sono esposti. Se i dati operativi rivelano pattern di produzione, ritmi di utilizzo o parametri di processo, possono essere usati per pianificare attacchi fisici o sabotaggio industriale. Come documentato nell'analisi di ICT Security Magazine sulla convergenza IT/OT e le infrastrutture critiche, la superficie di attacco negli ambienti OT si amplifica esponenzialmente con ogni nuova connessione esterna.

Dati grezzi vs. dati derivati: il confine che protegge il know-how

Una distinzione cruciale, spesso trascurata nella discussione sul Data Act, è quella tra dati obbligatoriamente condivisibili e dati protetti come segreto commerciale. L'obbligo di condivisione riguarda i dati grezzi (*raw data*, output diretto dei sensori) e i dati pre-processati di base. Sono potenzialmente protetti i dati derivati: quelli che il produttore ha elaborato con investimenti significativi, algoritmi proprietari o modelli di apprendimento automatico per ricavarne insight, previsioni o ottimizzazioni. La protezione come segreto commerciale non è automatica: richiede l'attivazione delle procedure previste dall'art. 5(9)-(11) del regolamento, inclusa la proposta di misure tecnico-organizzative alla controparte.

Questo confine ha implicazioni di sicurezza rilevanti. Un produttore di macchinari che elabora i dati grezzi dei sensori

con un algoritmo di *predictive maintenance* proprietario può difendere come segreto commerciale l'output di quell'algoritmo, non i valori grezzi che lo alimentano. L'obbligo riguarda i dati sensoristici elementari, non le previsioni derivate.

In pratica, questo significa che i produttori devono progettare un'architettura tecnica che separi chiaramente il livello di raccolta dati grezzi (accessibile agli utenti e alle terze parti designate) dal livello di elaborazione e valorizzazione (proteggibile come IP). Questa separazione architetturale non è solo una tutela commerciale: è anche una difesa di sicurezza, perché limita la superficie dei dati esposta alle terze parti.

La sfida è che molte aziende italiane, soprattutto PMI, non hanno un'architettura IoT progettata con questa separazione. I dati grezzi e i dati elaborati coesistono nelle stesse piattaforme, negli stessi database, sulle stesse infrastrutture cloud. Il Data Act diventa quindi anche l'occasione per un'architettura review obbligata.

Cloud switching e vendor lock-in: le implicazioni per la sicurezza operativa

Il Capitolo VI del Data Act introduce regole specifiche per i fornitori di servizi di elaborazione dati, con l'obiettivo di ridurre il lock-in tecnologico. Dal 12 settembre 2025, i fornitori devono garantire la portabilità dei dati e delle configurazioni. Dal 12 gennaio 2027, non potranno più applicare switching charges. Come chiarisce la Commissione Europea, durante il periodo transizionale (dal 11 gennaio 2024 al 12 gennaio 2027) i fornitori possono ancora addebitare costi collegati al trasferimento, ma in modo progressivamente decrescente.

Per i team di sicurezza, questo introduce una nuova dimensione nella valutazione dei cloud provider: la capacità di migrazione sicura diventa un requisito normativo, non solo una best practice. Le aziende devono avere processi per rispondere rapidamente alle richieste di portabilità e i contratti con i fornitori cloud devono includere clausole specifiche su tempi e modalità di migrazione.

La sovrapposizione con la NIS2 è significativa per i soggetti in scope: la direttiva richiede che le organizzazioni essenziali e importanti gestiscano il rischio derivante dai fornitori ICT, inclusa la capacità di sostituirli in tempi ragionevoli in caso di incidente. Il Data Act aggiunge a questa previsione l'obbligo per i fornitori di supportare tecnicamente la migrazione. Le due normative si rafforzano a vicenda nel ridurre la dipendenza da singoli fornitori critici.

La convergenza normativa: Data Act, NIS2, Cyber Resilience Act e la mappa degli obblighi

Per una PMI manifatturiera italiana che produce macchinari connessi, il 2025 e 2026 presentano una sovrapposizione normativa di notevole complessità. Di seguito la mappa sintetica degli obblighi rilevanti, con le rispettive basi normative e le date applicative.

Il D.Lgs. 138/2024 che recepisce la Direttiva NIS2 (UE) 2022/2555 impone misure di sicurezza proporzionate al rischio per circa **50.000 organizzazioni italiane** in scope, secondo le stime dell'Agenzia per la Cybersicurezza Nazionale (ACN), incluse quelle nel settore manifatturiero e logistica. È entrato in vigore il 16 ottobre 2024.

Il Regolamento (UE) 2023/2854 (Data Act) impone obblighi di

accesso e condivisione dei dati IoT. Si applica dal 12 settembre 2025 per le disposizioni principali, dal 12 settembre 2026 per i requisiti di progettazione dei nuovi prodotti.

Il Cyber Resilience Act (UE) 2024/2847 impone requisiti orizzontali di cybersecurity su tutti i prodotti con elementi digitali. È entrato in vigore il 10 dicembre 2024 e sarà pienamente applicabile dall'**11 dicembre 2027**. Gli obblighi di notifica di vulnerabilità e incidenti si applicheranno dall'11 settembre 2026. Si segnala che autoveicoli e dispositivi medici sono soggetti a discipline settoriali specifiche che possono prevalere sul CRA.

Il Regolamento Delegato (UE) 2022/30, adottato ai sensi dell'art. 3(3)(d-f) della Direttiva RED 2014/53/UE, ha introdotto requisiti obbligatori di cybersecurity per dispositivi radio connessi a Internet dal **1° agosto 2025**. Le misure richieste riguardano la protezione della rete e delle risorse di rete, la tutela dei dati personali e della privacy, e la protezione dalle frodi finanziarie. I requisiti tecnici di riferimento sono le norme armonizzate EN 18031-1:2024, EN 18031-2:2024 ed EN 18031-3:2024. L'obbligo di predisporre una *Software Bill of Materials* (SBOM) è invece previsto dal Cyber Resilience Act, non da questo regolamento delegato.

L'intersezione non è caotica: chi implementa correttamente il Cyber Resilience Act e la NIS2 ha già la maggior parte degli strumenti per soddisfare i requisiti di sicurezza del Data Act. Il problema è che molte aziende italiane non hanno ancora completato il percorso NIS2. Il Data Act arriva come obbligo aggiuntivo su una base di sicurezza ancora incompleta.

Cosa fare concretamente: priorità

per i produttori IoT italiani

Le azioni prioritarie variano in base al ruolo nella catena del valore, ma la sequenza logica è la stessa per quasi tutti.

Data mapping IoT. Prima ancora di qualsiasi azione tecnica o contrattuale, è necessario un inventario completo: quali prodotti generano dati, quali dati sono “grezzi” vs. “derivati”, dove sono archiviati, chi vi ha attualmente accesso, quali canali API esistono già. Questa mappatura è il prerequisito per qualsiasi valutazione di compliance e per l’attivazione del meccanismo di protezione dei segreti commerciali ai sensi dell’art. 5(9)-(11).

Architettura tecnica di separazione. Progettare o adeguare i sistemi per separare fisicamente lo strato di raccolta dati grezzi (condivisibile) dallo strato di elaborazione e valorizzazione (proteggibile). Questa separazione deve essere documentabile per dimostrare la protezione dei segreti commerciali.

API sicure con autenticazione forte. Ogni interfaccia sviluppata per soddisfare gli obblighi del Data Act deve implementare: autenticazione MFA per le terze parti accreditanti, TLS 1.3 per tutti i trasferimenti, rate limiting per prevenire exfiltrazione massiva, logging completo degli accessi in un SIEM o sistema di audit trail. I requisiti tecnici di protezione trovano la propria base normativa nell’art. 11 del Data Act e si intersecano con gli obblighi di sicurezza della NIS2.

Due diligence sulle terze parti. Prima di autorizzare la condivisione dei dati con una terza parte designata dall’utente, verificare che la terza parte abbia adeguate misure di sicurezza. Includere nei contratti clausole di cybersecurity con requisiti minimi verificabili, obblighi di notifica in caso di violazione e diritto di audit. Come segnalato dall’IAPP nell’analisi operativa del Data Act,

l'assenza di standard obbligatori per la postura di sicurezza delle terze parti è una delle lacune più criticate dalla comunità della sicurezza.

Revisione dei contratti con i cloud provider. Verificare che i contratti esistenti con i fornitori di servizi cloud includano clausole di portabilità conformi al Data Act. Per i prodotti messi in commercio dopo settembre 2026, progettare l'architettura con capacità di migrazione nativa.

Incident response aggiornato. Il piano di risposta agli incidenti deve includere procedure specifiche per violazioni legate ai flussi Data Act: chi notificare (l'autorità nazionale competente, l'utente, le terze parti coinvolte), in quali tempi, con quale documentazione. Le notifiche di incidente previste dal Data Act si sovrappongono alle notifiche NIS2: le organizzazioni in scope di entrambe le normative devono coordinare i due processi.

Il decreto attuativo italiano e il vuoto di enforcement

Un aspetto pratico che le imprese italiane devono tenere presente: il Data Act è un regolamento UE direttamente applicabile, ma il quadro nazionale di enforcement non è ancora completamente definito. Gli Stati Membri erano tenuti ad adottare i propri regimi sanzionatori nazionali entro il 12 settembre 2025, ma Italia e altri Paesi non hanno ancora completato il processo legislativo di designazione delle autorità competenti.

Questo non significa che le imprese non siano già obbligate. L'articolo 40 del Data Act rimette a ciascuno Stato Membro la definizione di sanzioni "effettive, proporzionate e dissuasive". Per le violazioni che coinvolgono dati personali rientranti nel Capitolo II, III e V, le autorità di protezione dei dati possono applicare sanzioni ai sensi dell'art. 83(5)

del GDPR, che prevede fino a **20 milioni di euro o il 4% del fatturato annuo mondiale** (quale dei due valori sia superiore). Per le infrazioni riguardanti esclusivamente dati non personali, le sanzioni saranno determinate dalle legislazioni nazionali di attuazione, ancora in elaborazione in Italia.

Il paradosso dell'enforcement frammentato è che crea incertezza operativa senza ridurre il rischio legale: le imprese non sanno quali comportamenti saranno effettivamente sanzionati, ma non possono escludere di essere trascinate in arbitrati o cause civili per mancata condivisione dei dati, meccanismo previsto direttamente dall'art. 38 del regolamento.

Il Data Act come opportunità di architettura: chi si adegua bene ne esce rafforzato

C'è una narrativa comune che presenta il Data Act come un onere burocratico. Vale la pena leggere anche il lato opposto. Le aziende che costruiranno API sicure, documentate e controllate per soddisfare gli obblighi del Data Act si troveranno con un'architettura IoT più moderna, più manutenibile e più difendibile degli stessi sistemi che hanno oggi.

Il manifatturiero italiano è caratterizzato da un'enorme quantità di dati di processo che non vengono sfruttati perché intrappolati in sistemi proprietari dei produttori delle macchine. Il Data Act rompe questa asimmetria. Le imprese che sapranno accedere ai dati dei propri macchinari e integrarli in sistemi di analisi propri avranno vantaggi competitivi reali: migliore manutenzione predittiva, ottimizzazione dei processi, indipendenza dal vendor per i servizi post-vendita.

Il rischio di sicurezza è reale. Ma è un rischio gestibile con le stesse metodologie che si applicano a qualsiasi

integrazione di sistema: threat modeling, API security testing, monitoraggio continuo, gestione strutturata delle terze parti. Chi lo gestisce bene non solo è compliant: ha un'infrastruttura IoT più matura di chi aspetterà l'ultima notifica di enforcement.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/eu-data-act/>