INSIGHT | 18 settembre 2025

Data Act: le nuove regole europee sull'accesso e l'uso dei dati generati dai prodotti connessi

Dal 12 settembre 2025, è diventato applicabile il **Data Act**, il Regolamento UE 2023/2854 ("**Data Act**" o "**Regolamento**") che introduce un nuovo quadro giuridico sull'**accesso, l'uso e la condivisione dei dati generati da prodotti connessi e servizi digitali.**

L'obiettivo della norma è chiaro: garantire che gli utenti che generano dati attraverso l'uso di un prodotto o servizio di terzi abbiano **il diritto di accedervi e di utilizzarli,** anche condividendoli con un soggetto terzo di loro fiducia, ad esempio un fornitore di servizi alternativo o un partner tecnologico.

D'altra parte, il Data Act definisce quali sono le condizioni alle quali le imprese sono tenute a mettere a disposizione tali dati.

Quali dati?

Il Data Act trova applicazione con riferimento ai **dati generati durante l'uso effettivo di un prodotto connesso o servizio correlato.** In particolare, rientrano nell'ambito di applicazione:

- i **dati grezzi** (*raw data*), raccolti da sensori o altri componenti del prodotto;
- i **dati pretrattati** (*pre-processed data*), che abbiano subito operazioni minime come filtraggio, normalizzazione o conversione, purché non si tratti di dati elaborati in modo complesso.

Il Data Act prende in considerazione non solo i dati personali (regolati dal GDPR), ma anche quelli non personali, a condizione che siano prontamente disponibili ("*readily available*"): ossia già raccolti, disponibili al detentore, e accessibili senza sforzi sproporzionati. Non rientrano nell'ambito di applicazione, invece:

- i **dati derivati,** ossia quei dati generati tramite elaborazioni analitiche, intelligenza artificiale o modelli predittivi;
- i **dati aggregati** riferiti a più utenti o dispositivi;
- i dati la cui divulgazione comporterebbe la **rivelazione significativa e non controllabile di segreti commerciali.**

Con riferimento a quest'ultimo aspetto, è evidente che il Data Act riconosce che la condivisione dei dati può entrare in **tensione con la tutela di segreti commerciali, know-how e altre informazioni riservate.** Per questo motivo, il Regolamento consente ai detentori di adottare misure tecniche, contrattuali o organizzative – come, ad esempio, accordi di riservatezza (NDA), clausole limitative o soluzioni di pseudonimizzazione – volte a prevenire la compromissione di tali asset.

L'impatto per le imprese è duplice. Da un lato, esse possono legittimamente proteggere i propri interessi economici, garantendo che informazioni strategiche o sensibili non vengano diffuse senza controllo. Dall'altro, sono chiamate a **strutturare processi interni trasparenti e proporzionati**, in grado di distinguere tra misure di tutela realmente necessarie e ostacoli ingiustificati alla condivisione. Il successo del Regolamento dipenderà proprio da questo equilibrio: solo se la riservatezza

sarà gestita come garanzia e non come barriera, il Data Act potrà esprimere appieno la sua portata innovativa.

Infine, a partire dal **12 settembre 2026**, tutti i **nuovi prodotti e servizi** immessi sul mercato dovranno essere progettati in modo da garantire **l'accessibilità ai dati "*by design*"**. Essi dovranno essere progettati e forniti in modo tale che i dati dei prodotti e dei servizi correlati siano, per impostazione predefinita, accessibili all'utente in modo facile, sicuro, gratuito, in un formato completo, strutturato, di uso comune e leggibile da un dispositivo automatico.

A chi si applica il Regolamento (e chi sono i soggetti coinvolti)

Il **Data Act** trova applicazione nei confronti di tutti i soggetti che immettono sul mercato europeo prodotti e servizi in grado di generare o trattare dati.

Rientrano in questo ambito, da un lato, i **prodotti connessi**, come macchinari industriali, veicoli, dispositivi medici e oggetti smart; dall'altro, i **servizi digitali correlati**, quali applicazioni di diagnostica integrata, soluzioni di manutenzione da remoto o *app companion* che dialogano con i prodotti stessi. Il Regolamento si applica, inoltre, ai **servizi di trattamento dei dati**, ivi incluse le piattaforme di cloud computing, le soluzioni di *edge computing* e i modelli "*as a service*" (SaaS, IaaS, etc.).

Quanto all'ambito di applicazione territoriale, il Regolamento si applica anche a fornitori **stabiliti fuori dall'Unione Europea**, nella misura in cui offrano tali prodotti o servizi nel mercato UE. In tal caso, sono tenuti a **designare un rappresentante legale nell'UE**.

Le categorie di soggetti individuate dal Data Act sono (i) l'**Utente**, ossia chi utilizza il prodotto o il servizio, generando i dati. L'Utente diritto all'accesso gratuito e può indicare un soggetto terzo a cui trasmettere i dati, (ii) il **Data holder**, ossia chi detiene il controllo sui dati generati e ne consente (o meno) l'accesso. Tipicamente, il produttore del prodotto o il fornitore del servizio, (iii) il **Terzo designato** (***Data Recipient***), ossia il soggetto individuato dall'utente per ricevere i dati, per esempio un fornitore di servizi di manutenzione o fornitore alternativo. L'accesso ai dati da parte del Terzo designato può essere soggetto a condizioni, (iv) il **Fornitore di servizi di trattamento dati** (***Data Processing Service Provider***), ossia chi fornisce infrastrutture e servizi per elaborazione, archiviazione e accesso ai dati.

Interferenze tra Data Act e GDPR

Il Data Act si applica senza pregiudicare la disciplina del GDPR: ciò significa che, ogniqualvolta una richiesta di accesso o di trasmissione riguardi un set di informazioni che includano anche dati personali, essa deve essere valutata alla luce dei principi di liceità, correttezza, trasparenza e proporzionalità propri del Regolamento generale sulla protezione dei dati. In altri termini, il Data Act non costituisce una base giuridica autonoma per il trattamento, ma amplia il diritto di accesso e il diritto alla portabilità che possono essere esercitati solo nel rispetto del quadro di protezione dei dati personali già esistente.

La trasmissione dei dati personali può considerarsi lecita, a titolo esemplificativo, quando è l'utente stesso – anche nella propria veste di interessato – a richiederla direttamente, oppure quando il terzo designato dispone di una valida base giuridica ai sensi del GDPR, come il consenso o l'esecuzione di un contratto. In questi casi la condivisione è compatibile con la normativa, purché avvenga nel rispetto dei principi di minimizzazione e di limitazione delle finalità e sia accompagnata da misure tecniche e organizzative idonee a garantire la sicurezza dei dati.

Al contrario, la trasmissione potrebbe non risultare legittima in assenza di una valida base giuridica, quando i dati riguardino soggetti diversi dall'utente senza che sia stato prestato il necessario consenso, o quando l'uso previsto da parte del terzo risulti incompatibile con la finalità originaria della raccolta. Inoltre, la condivisione è vietata se non vengono approntate adeguate garanzie a tutela dei segreti commerciali, delle informazioni riservate o, più in generale, dei diritti e delle libertà fondamentali degli interessati.

In definitiva, il Data Act non modifica l'impianto sostanziale del GDPR: la trasmissione di dati personali rimane legittima solo se sorretta da una base giuridica idonea e conforme ai principi di protezione già previsti dalla normativa europea.

Terzi designati: accesso condizionato ma garantito

Il Data Act riconosce all'utente non solo il diritto di accedere direttamente ai dati generati dall'utilizzo di un prodotto o di un servizio, ma anche la possibilità di richiederne la trasmissione a favore di un soggetto terzo da lui espressamente designato. Tale facoltà amplia le opportunità di utilizzo dei dati e ne favorisce la circolazione all'interno dell'ecosistema digitale.
Il detentore dei dati è tenuto a consentire questa trasmissione, salvo che ricorrano eccezioni specifiche e motivate, connesse – ad esempio – alla tutela della sicurezza, della riservatezza o di diritti altrui. In ogni caso, l'eventuale rifiuto deve essere fondato su ragioni oggettive e proporzionate.

La normativa ammette inoltre che, in caso di trasmissione verso terzi, il detentore possa richiedere un corrispettivo economico. Tale compenso, tuttavia, deve rispettare criteri stringenti: deve essere **ragionevole**, non **discriminatorio** e **proporzionato** ai costi effettivamente sostenuti per mettere a disposizione i dati. In questo modo si bilanciano, da un lato, i diritti degli utenti e dei terzi da essi designati e, dall'altro, la legittima esigenza del detentore di vedere riconosciuti i propri investimenti e i costi operativi.

Portabilità e *switching*

Il **Data Act** introduce un quadro di regole volte a rafforzare la concorrenza e a tutelare gli utenti dei servizi *cloud* e di *data processing services*. I fornitori saranno tenuti a garantire la piena portabilità dei dati e a rimuovere ogni ostacolo, di natura tecnica o contrattuale, che possa limitare la possibilità di migrare verso un diverso prestatore di servizi. Essi dovranno inoltre predisporre strumenti e formati di esportazione interoperabili, in grado di assicurare una transizione agevole e priva di interruzioni.

A partire dal **12 settembre 2025**, eventuali oneri economici connessi al cambio di fornitore potranno essere richiesti soltanto nei limiti dei costi effettivamente sostenuti dal provider. Trascorsa tale fase transitoria, dal **12 gennaio 2027**, l'applicazione di qualsivoglia "***switching charge***" sarà definitivamente preclusa.

Accesso pubblico ai dati in casi eccezionali

Il Regolamento stabilisce che, in situazioni di necessità straordinaria – come emergenze sanitarie, calamità naturali o gravi minacce alla sicurezza pubblica – le autorità pubbliche, le istituzioni dell'Unione europea e altri organismi competenti possano richiedere l'accesso a dati detenuti da privati. Tale facoltà è circoscritta a casi in cui i dati siano indispensabili per fronteggiare l'emergenza e non possano essere ottenuti con strumenti alternativi.

L'accesso deve sempre rispettare i principi di **necessità** e **proporzionalità**, essere limitato nel tempo e riferirsi a finalità specifiche e chiaramente determinate. A tutela degli operatori economici, il Regolamento prevede, inoltre, misure di protezione per i **segreti commerciali** e per altre informazioni riservate, imponendo che i dati raccolti vengano utilizzati esclusivamente per lo scopo per cui sono stati richiesti e cancellati non appena cessata la situazione emergenziale, salvo diversa previsione normativa.

Il regime sanzionatorio

Il Data Act non introduce un sistema sanzionatorio uniforme a livello europeo. La definizione delle misure applicabili è demandata ai singoli Stati membri, i quali sono tenuti a designare le **autorità competenti** responsabili della vigilanza sull'applicazione del Regolamento e a stabilire un regime di **sanzioni efficaci e proporzionate**.

In Italia, il decreto attuativo che disciplinerà la materia non è ancora stato adottato. Tuttavia, il Data Act è già **pienamente applicabile** a partire dal 12 settembre 2025 e le imprese sono pertanto tenute a conformarsi agli obblighi da esso introdotti, indipendentemente dal completamento del quadro nazionale di *enforcement*.

Possibili aree di intervento

Il Data Act rappresenta un **cambio di paradigma**: sposta il baricentro della *governance* dei dati, stabilendo che chi genera dati attraverso l'uso di un prodotto o servizio ha il diritto di accedervi e, in certi casi, di condividerli con soggetti terzi. In tal modo, il dato non resta più confinato nel perimetro esclusivo del produttore o del fornitore,

ma diventa un asset che può essere condiviso, pur sempre soggetto a regole precise e a garanzie per la tutela degli interessi economici e della riservatezza.

Per le imprese, le nuove regole richiedono più di un mero adempimento normativo. In particolare, implicano **un'analisi approfondita e una revisione dei modelli operativi**. In particolare, appare indispensabile **riconsiderare i contratti B2B che disciplinano l'accesso e l'uso dei dati, mappare i flussi informativi** individuando quali dati vengono generati, in quali formati e da chi siano detenuti o gestiti. Occorre, inoltre, **adeguare le procedure interne per gestire in maniera corretta, sicura e trasparente le richieste di accesso o di condivisione dei dati, provenienti tanto dagli utenti quanto da terzi da essi designati.**

L'obiettivo è garantire tracciabilità, sicurezza, trasparenza e coerenza con la normativa, salvaguardando al contempo informazioni riservate e know-how aziendale.

Per molte imprese, l'adeguamento rappresenta una priorità immediata.

Contatti

Giulio Vecchi
giulio.vecchi@lcalex.it

Micol Sabatini
micol.sabatini@lcalex.it