CEDPO
CONFEDERATION OF EUROPEAN
DATA PROTECTION ORGANISATIONS

Bonn, Bucharest, Dublino, Lisbona, Madrid, Milan, Parigi, L'Aia, Vienna, Varsavia

Data Act
FAQ per DPO

EU Digital Strategy Working Group
Ottobre 2025

Contatti:
https://cedpo.eu
info@cedpo.eu

CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Sommario

Introduzione 3

Domanda n. 1: cosa è il Data Act e quale è il suo scopo? 4

Domanda n. 2: a chi si applica il Data Act? 4

Domanda n. 3: a quali dati si applica il Data Act? 5

Domanda n. 4: Chi sono i principali attori previsti dal Data Act? 5

Domanda n. 5: Cosa si intende per dati non personali? 6

Domanda n. 6: Come si deve trattare un file che contiene sia dati personali che dati non personali? 7

Domanda n. 7: Quando la mia organizzazione dovrebbe ricorrere a misure tecniche e organizzative per proteggere i dati? 8

Domanda n. 8: Cosa occorre considerare per ridurre al minimo i rischi associati al Data Act? 9

Domanda n. 9: Qual è un metodo comunemente utilizzato per la condivisione dei dati ai sensi del Data Act e quali sono i modi per ridurre i rischi legati alla protezione dei dati? 11

Domanda n. 10: Quali sono gli obblighi per il Titolare dei dati? 12

Domanda n. 11: Come posso formalizzare la condivisione dei dati in un contesto Business-to-Business? 13

Domanda n. 12: La mia organizzazione è un titolare del trattamento dei dati. Posso rifiutarmi di rendere disponibili i dati? 14

Domanda n. 13: Qual è l'impatto del Data Act sulla gestione dei diritti degli interessati nei casi in cui i dati siano dati personali? 14

Domanda n. 14: Quali sono le basi giuridiche che possono essere utilizzate per il trattamento dei dati personali, a cui si applica il Data Act? 14

Domanda n. 15: La mia organizzazione è un Utente e vorrebbe elaborare i dati messi a disposizione dal Titolare dei dati sulla base del Legittimo Interesse. È possibile? 15

Domanda n. 16: La mia organizzazione è un ente pubblico. In quali situazioni la mia organizzazione può richiedere dati sulla base di una “necessità eccezionale”? 17

Domanda n. 17: Come viene definita la profilazione ai sensi della legge sui dati? 19

Domanda n. 18: La profilazione è vietata ai sensi della legge sui dati? 19

Domanda n. 19: Perché la trasparenza è fondamentale ai sensi del Data Act? 21

Link Utili 23

Disclaimer 23

Introduzione

Sono passata già sette anni da quando il GDPR è entrato in vigore, che ha gettato solide basi solida per la protezione dei dati in Europa. Successivamente, il panorama normativo ha continuato ad evolvere al fine di guidare l'Europa con responsabilità verso il futuro digitale.

L'UE Data Act rappresenta un'altra pietra miliare in questo viaggio. La bozza trapelata del Digital Omnibus mostra che il Data Act avrà un ruolo sempre più importante nella regolamentazione dello spazio digitale in futuro.

Ad oggi il Data Act, insieme alle altre leggi in materia di dati, quali il Data Governance Act (DGA), il Digital Services Act (DSA), il Digital Markets Act (DMA) introduce nuovi obblighi e opportunità. Il risultato è che i Data Protection Officers (DPOs) sono sempre più chiamati ad ampliare le loro competenze oltre il GDPR, fornendo consulenza su una gamma più ampia di questioni relative alla governance dei dati e alla conformità.

Per aiutare la comunità dei DPO ad affrontare queste sfide imminenti, attraverso il CEDPO il Gruppo di lavoro nell'ambito del comitato europeo per i servizi digitali ha collaborato con i suoi membri esperti provenienti da tutta Europa per elaborare risposte pratiche e approfondite alle domande frequenti (FAQ) relative alla legge dell'UE sui dati. Queste FAQ sono specificamente incentrate su argomenti rilevanti per la protezione dei dati.

Un sincero ringraziamento al Gruppo di lavoro nell'ambito del comitato europeo per i servizi digitali e al personale del CEDPO per il loro inestimabile contributo.

Membri del Gruppo che hanno contribuito alla redazione delle FAQ: **Thomas Ajoodha, Filippo Bianchini, Lionel Capel, Julie Crawford, Paul Jordan, Paul Lambert, Dr Maria Maloney, Samira Marquaille, Massimo Pappalardo, Jeremiah Russel, Henry Simwinga.**

Dr. Sachiko Scheuing (GDD) & Filippo Bianchini (ASSO DPO)

Co-Chairs di CEDPO Gruppo di lavoro nell'ambito del comitato europeo per i servizi digitali

Domanda n. 1: cosa è il Data Act e quale è il suo scopo?

Il Data Act è una parte integrante dell'agenda legislativa dell'UE con l'obiettivo di promuovere la strategia europea sui dati, volta a conferire all'UE un ruolo di leader in una società guidata dai dati. Il Data Act promuove il flusso libero dei dati all'interno di un mercato unico, attraverso vari settori come il business, la ricerca e l'amministrazione pubblica. Il Data Act mira a rendere i dati più accessibili e utilizzabili per tutti, attraverso meccanismi di condivisione dei dati. La legge obbliga i titolari dei dati a renderli disponibili nelle circostanze rilevanti. Allo stesso tempo, conferisce agli utenti il diritto di beneficiare dei dati che generano, ad esempio, dai loro dispositivi IoT. Concretamente, il Data Act richiede che i prodotti connessi siano progettati in modo che gli utenti possano accedere direttamente ai dati che generano (Art. 3 Data Act). A prima vista, ciò sembra simile alla portabilità dei dati e ai diritti di accesso sotto il GDPR. Può essere visto come una specificazione ulteriore di tali diritti. Nei casi in cui l'accesso diretto non sia possibile, i dati devono essere forniti rapidamente agli utenti quando richiesti (Art. 4 Data Act). L'obiettivo del Data Act è garantire un accesso equo ai dati e proteggere i diritti degli utenti, bilanciando questi obiettivi con la protezione dei dati personali.

Il Data Act è coerente con le normative esistenti sul trattamento dei dati personali, incluso il GDPR. Può essere utile talvolta fare riferimento incrociato alle definizioni con altre normative UE pertinenti. Ad esempio, il Regolamento sul libero flusso dei dati non personali costituisce un elemento fondamentale dell'economia digitale europea, garantendo che i dati non personali possano essere archiviati, trattati e trasferiti ovunque nell'UE.

Domanda n. 2: a chi si applica il Data Act?

Il Data Act si applica alle organizzazioni e alle persone responsabili della produzione, elaborazione, utilizzo, gestione e condivisione dei dati derivanti dalle tecnologie intelligenti nell'UE. In particolare, il Data Act regolamenta i Titolari dei Dati, solitamente progettisti, produttori o fornitori di servizi che generano o possono recuperare i dati grezzi da queste tecnologie intelligenti. Il Data Act pone un forte focus sulle relazioni Business-to-Business (B2B) e Business-to-Consumer (B2C), ma disciplina anche la condivisione dei dati Business-to-Government (B2G).

Le piccole e micro imprese, insieme alle organizzazioni di medie dimensioni che esistono da meno di un anno, sono esenti dall'obbligo di condivisione previsto dall'Articolo 5 del Data Act.

Domanda n. 3: a quali dati si applica il Data Act?

Il Data Act si applica a tutti i dati grezzi e pre-elaborati generati dall'uso di un prodotto connesso o di un servizio correlato che sia facilmente disponibile per il Titolare dei Dati, come i dati del prodotto (generati tramite l'uso di prodotti connessi), i dati del servizio correlato (dati relativi alle azioni degli utenti) o i metadati (dati necessari per interpretare i dati del prodotto e i dati del servizio correlato). I dati grezzi e pre-elaborati possono essere sia dati personali che non personali. I dati che sono stati fortemente elaborati, come i dati derivati e inferiti (ad esempio, dati altamente arricchiti, materiale audiovisivo) generati tramite algoritmi complessi, non sono soggetti al Data Act.
Il Data Act distingue anche tra dati grezzi e dati derivati o inferiti. Nel caso in cui i dati grezzi siano dati personali, si applica il GDPR oltre al Data Act.
Il Registro delle Attività di Trattamento (RoPA) sarà un buon punto di partenza per determinare se il Data Act è applicabile alla tua organizzazione.

Domanda n. 4: Chi sono i principali attori previsti dal Data Act?

Il Data Act definisce i seguenti tre principali attori: il Titolare dei Dati, il Destinatario dei Dati e l'Utente.

Un **Titolare dei Dati** si riferisce a una persona fisica o giuridica che ha accesso legittimo ai dati grezzi provenienti da prodotti connessi o servizi correlati, e ha l'autorità per concedere l'accesso a tali dati. In sostanza, il Titolare dei Dati è una persona o entità legale con il diritto o l'obbligo di utilizzare o condividere i dati generati o raccolti durante la fornitura di un servizio correlato. Nella pratica, i Titolari dei Dati sono solitamente impresi, come i produttori di prodotti connessi o i fornitori di servizi correlati, che gestiscono dispositivi intelligenti e detengono i dati dei clienti raccolti tramite questi dispositivi. Questo ruolo è probabilmente il più critico sotto il Data Act. Qualsiasi organizzazione, sia pubblica che privata, che controlla i dati generati da prodotti e servizi connessi, è considerata un Titolare dei Dati.

Le responsabilità di un Titolare dei Dati includono facilitare l'accesso ai dati e garantire la possibilità di trasferire i dati ad altri fornitori di servizi in un formato facile da usare, come specificato dalla legge. Inoltre, è vietato imporre condizioni contrattuali ingiuste agli utenti riguardo l'accesso ai loro dati e i loro diritti alla portabilità dei dati.

Un **Destinatario dei Dati** si riferisce a una persona fisica o giuridica che riceve i dati grezzi da un Titolare dei Dati su richiesta dell'Utente. In sostanza, un Destinatario dei Dati è una persona fisica

o giuridica, diversa dall'Utente, a cui il Titolare dei Dati fornisce i dati, inclusi i terzi che agisce su richiesta di un utente o in ottemperanza a un obbligo legale.

Nella pratica, i Destinatari dei Dati sono tipicamente entità legali come aziende, autorità pubbliche, organizzazioni di ricerca o organizzazioni non profit. Esistono specifici limiti per impedire che grandi fornitori, o "guardiani" sotto il Digital Markets Act, agiscano come terzi in determinati accordi di condivisione dei dati.

In sostanza, un Destinatario dei Dati è un'entità che riceve i dati da un Titolare dei Dati con l'intenzione di utilizzarli per scopi commerciali o professionali. Ciò potrebbe comportare che aziende che analizzano i dati relativi al comportamento degli utenti, forniscono servizi di archiviazione cloud per i dati generati dai dispositivi connessi o offrono servizi basati sui dati. La principale distinzione è che un Destinatario dei Dati utilizza i dati per scopi commerciali o organizzativi, piuttosto che per uso personale, come potrebbe fare un Utente.

Un **Utente** si riferisce a una persona fisica o giuridica che possiede o ha il diritto di utilizzare un prodotto connesso o ricevere servizi correlati. In sostanza, un Utente è la persona fisica o giuridica che possiede, noleggia o affitta un dispositivo intelligente.

Nella pratica, l'Utente è tipicamente il cliente di un dispositivo intelligente. È importante notare che le persone che utilizzano il dispositivo ma non sono parte dell'accordo, come i membri della famiglia, probabilmente non sono considerate Utenti.

Domanda n. 5: Cosa si intende per dati non personali?

Il Data Act definisce i dati non personali come qualsiasi dato che non rientra nella categoria dei dati personali, come specificato nell'Articolo 2(4) del Data Act. Mentre il GDPR si riferisce ai dati anonimi come informazioni che non possono essere collegate a una persona fisica identificata o identificabile nel Considerando 26, non definisce esplicitamente i dati non personali.
Il Regolamento sul Quadro per il Libero Flusso dei Dati Non Personali all'interno dell'Unione Europea introduce i dati non personali nell'Articolo 1 come "dati diversi dai dati personali". Rispetto alla definizione di dati personali nell'Articolo 1, i dati non personali possono essere intesi come qualsiasi informazione che non riguarda una persona fisica identificata o identificabile (l"interessato'). Le linee guida della Commissione UE del 2019 sul Regolamento per il libero flusso dei dati non personali supportano questa interpretazione.
Inoltre, la Commissione classifica i dati non personali in due categorie:
(1) dati che originariamente non riguardavano una persona fisica identificata o identificabile, e (2) dati che erano inizialmente personali ma successivamente anonimizzati.

(3) Le letture della temperatura di un edificio sono un esempio di (1), e la media dell'età degli studenti in una classe è un esempio di (2). È importante notare che l'anonimizzazione dei dati personali è diversa dalla pseudonimizzazione. Mentre l'anonimizzazione comporta l'elaborazione dei dati in modo che non possano essere attribuiti a un individuo, la pseudonimizzazione si riferisce a dati che possono ancora essere attribuiti a una persona attraverso informazioni aggiuntive. È anche importante notare che i dati pseudonimizzati diventano dati anonimi quando sono in possesso di organizzazioni che non hanno i mezzi per reidentificare l'interessato[1].

Esempi di dati non personali includono set di dati aggregati o anonimizzati utilizzati nell'analisi dei big data, dati sull'agricoltura di precisione che aiutano a ottimizzare l'uso di pesticidi e acqua, e dati sui bisogni di manutenzione per macchinari industriali. Tuttavia, se i progressi tecnologici consentono la reidentificazione dei dati anonimizzati, tali dati sarebbero considerati dati personali e il GDPR si applicherebbe.

Domanda n. 6: Come si deve trattare un file che contiene sia dati personali che dati non personali?

La maggior parte dei dati coperti dal Data Act è classificata come "non personale", in quanto riguarda prodotti e servizi industriali piuttosto che individui. Tuttavia, non è raro che questi dati vengano mescolati con dati personali. Quando un file contiene sia dati personali che non personali, si parla di un dataset misto.

Per quanto riguarda i dataset misti, il Considerando 7 del Data Act osserva che il GDPR[2] e la Direttiva ePrivacy (ove applicabile) forniscono la base per un'elaborazione dei dati sostenibile e responsabile.

Una sfumatura leggermente diversa si trova in un altro regolamento dell'UE che menziona i dataset misti: il Regolamento sul Quadro per il Libero Flusso dei Dati Non Personali nell'Unione Europea. Secondo questa legge e le linee guida della Commissione sul Regolamento per il libero flusso dei dati non personali, si applicano le seguenti disposizioni:

1. il "Regolamento sul Libero Flusso dei Dati Non Personali" si applica alla parte di dati non personali del set;
2. il GDPR si applica alla parte di dati personali del set;
3. se i dati non personali e i dati personali sono "indissolubilmente legati", il GDPR si applicherà all'intero dataset, anche se i dati personali rappresentano solo una piccola parte

[1] Sentenza dalla Corte del 4 settembre 2025 EDPS vs SRB, C-413/23 P, ECLI:EU:C:2025:645
[2] E il regolamento del 2018 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e alla libera circolazione di tali dati.

del set.

Le linee guida della Commissione spiegano che i dati non personali e i dati personali sono "indissolubilmente legati" quando è impossibile, o tecnologicamente o economicamente non fattibile, separare i due tipi di dati.

La raccomandazione per gestire i dataset misti è quella di garantire una protezione adeguata e di adempiere agli obblighi previsti dal GDPR. Tuttavia, quando non è possibile identificare l'interessato, il Titolare del trattamento è esentato dagli obblighi degli Articoli 15-20 del GDPR. Questi obblighi comprendono i diritti di rettifica, cancellazione, limitazione del trattamento, l'obbligo di notificare la rettifica, la cancellazione o la limitazione del trattamento, e la portabilità dei dati, come descritto nell'Articolo 11 del GDPR.

Domanda n. 7: Quando la mia organizzazione dovrebbe ricorrere a misure tecniche e organizzative per proteggere i dati?

Nel trattamento dei dati personali devono essere attuate misure tecniche e organizzative adeguate per proteggere i dati. Una misura di protezione sottolineata sia nel GDPR sia dal Data Act è la psudonimizzazione. Si raccomanda di applicare lo stesso standard di pseudonimizzazione previsto dal Data Act e richiesto dal GDPR.

Il Data Act affronta anche le misure di protezione nei casi in cui i dati personali debbano essere condivisi con un ente del settore pubblico, la Commissione, la Banca Centrale Europea o un'istituzione dell'UE a causa di una "necessità eccezionale". In tali casi, l'organizzazione richiedente è tenuta a specificare le misure tecniche e organizzative necessarie per proteggere i dati. Inoltre, l'organizzazione richiedente dovrebbe valutare se i dati personali possano essere anonimizzati.

D'altra parte, il Titolare dei Dati deve anonimizzare i dati personali, a meno che la richiesta di rendere i dati disponibili a un ente del settore pubblico, alla Commissione, alla Banca Centrale Europea o a un'istituzione dell'UE non comporti la divulgazione dei dati personali. In tali casi, il Titolare dei Dati è tenuto a pseudonimizzare i dati.

Le leggi nazionali potrebbero eventualmente essere istituite per disciplinare la divulgazione di altri tipi di dati in situazioni specifiche, come i dati medici o statistici. Quando tali dati non possono essere aggregati e devono essere condivisi come dati personali, dovrebbe essere implementato un livello adeguato di misure tecniche e organizzative per proteggerli.

Domanda n. 8: Cosa occorre considerare per ridurre al minimo i rischi associati al Data Act?

Il Data Act dell'UE stabilisce un quadro unico e coerente per la condivisione di dati personali e non personali all'interno del mercato unico europeo. Gli obiettivi sono garantire l'equità nelle catene di valore basate sui dati, migliorare l'accesso degli utenti ai dati generati da prodotti connessi e servizi correlati, e stimolare l'innovazione in vari settori.

Al contempo, rendere più disponibili i dati comporta inevitabilmente un maggiore rischio di abuso, violazioni della privacy, perdita di segreti commerciali, incidenti legati alla cybersecurity e accesso discriminatorio o disuguale. Pertanto, il Data Act associa ai nuovi diritti di accesso una serie di garanzie stratificate che variano a seconda della relazione in cui i dati sono condivisi: business-to-consumer (B2C), business-to-business (B2B) e business-to-government (B2G).

Mitigazione dei rischi nelle relazioni B2C e B2B

Nei contesti B2C (Articoli 3 e 4), i prodotti connessi e i servizi correlati devono essere progettati in modo tale che i dati siano, di default, accessibili direttamente dagli utenti in un formato strutturato, sicuro e leggibile da macchina. I consumatori devono ricevere l'accesso gratuitamente ed essere protetti da termini contrattuali ingiusti o poco trasparenti. Devono mantenere un controllo significativo sui propri dati, comprese le opzioni per concedere o revocare l'accesso e gestire le condizioni di riutilizzo.

Nelle relazioni B2B, dove possono esistere squilibri, il Data Act consente alle parti di definire restrizioni contrattuali sull'uso o sulla condivisione ulteriori dei dati quando tale uso potrebbe minacciare la sicurezza, la salute o i segreti commerciali (Articoli 4(2) e 4(6)). Gli accordi devono includere clausole di riservatezza e le imprese possono sospendere la condivisione dei dati se le misure concordate non vengono attuate o se i segreti commerciali vengono compromessi (Articolo 4(7)). Il Data Act richiede che tali termini siano equi e che evitino di sfruttare asimmetrie nel potere contrattuale, in particolare per le PMI (Articolo 5(3)).

Protezioni tecniche e organizzative

Il Data Act consente ai titolari dei dati di implementare misure di protezione tecniche come la crittografia, i controlli di accesso e i contratti intelligenti per prevenire accessi o usi non autorizzati (Articolo 11(1)). Queste misure non devono impedire l'accesso legittimo degli utenti, ma sono cruciali per garantire la conformità e proteggere le informazioni sensibili. I titolari dei dati possono

anche fare affidamento sulla pseudonimizzazione e sui protocolli di trasferimento sicuro dei dati, soprattutto quando i dati coinvolgono informazioni sensibili o accesso di terzi.

La condivisione dei dati è anche soggetta alla limitazione degli scopi. I terzi devono trattare i dati solo per gli scopi concordati con l'utente e devono eliminarli quando non sono più necessari (Articolo 6(1)). Per i dati personali, è obbligatoria la piena conformità al GDPR. Se queste obbligazioni vengono violate, i titolari dei dati possono richiedere l'eliminazione dei dati e la cessazione dei servizi o prodotti derivati (Articoli 11(2) - 11(4)). Nei contesti B2B, le misure tecniche possono includere anche tracciabilità per monitorare la conformità.

Gestire i segreti commerciali nelle scenarizzazioni di condivisione

Che i dati siano condivisi con utenti o terzi, il Data Act fornisce forti protezioni per i segreti commerciali. Questi possono essere divulgati solo se strettamente necessario e se sono in atto opportune garanzie tecniche e contrattuali (Articoli 4(6) e 5(9)). Se tali protezioni non sono rispettate, i titolari dei dati possono sospendere la condivisione e devono informare l'autorità competente (Articolo 5(10)). I contratti devono definire come i segreti commerciali sono protetti e specificare gli obblighi di riservatezza.

Accesso del settore pubblico e dimensione B2G

In casi eccezionali, le autorità pubbliche possono richiedere dati quando esiste un chiaro interesse pubblico (Articolo 17). Queste richieste devono essere specifiche, proporzionate e giustificate. L'autorità deve utilizzare i dati solo per lo scopo dichiarato, applicare misure di sicurezza rigorose ed eliminare i dati quando non sono più necessari (Articoli 18 e 19). Dove possibile, deve essere applicata l'anonimizzazione o la pseudonimizzazione dei dati personali. Gli enti pubblici devono anche implementare misure tecniche e organizzative simili a quelle degli attori privati e rispettare i requisiti di riservatezza quando trattano dati sensibili.

Il contesto è fondamentale

Gli obblighi e le protezioni previsti dal Data Act sono sensibili al contesto. La condivisione B2C si concentra sull'empowerment degli utenti e sulla protezione dei consumatori. Le relazioni B2B enfatizzano la contrattazione equa e la riservatezza. L'accesso B2G è limitato a necessità eccezionali ed è strettamente regolamentato. Questo approccio stratificato consente una mitigazione dei rischi efficace senza imporre un modello unico per tutti.

In conclusione, definendo regole su misura per diversi contesti di condivisione dei dati e

promuovendo l'uso di garanzie contrattuali, tecniche e organizzative, il Data Act fornisce una solida base giuridica per ridurre i rischi. Tuttavia, rendere operativi questi strumenti richiede più della semplice conformità legale. Soluzioni tecniche, tra cui API e meccanismi di accesso standardizzati, svolgono un ruolo cruciale nel garantire una condivisione dei dati sicura, auditabile e affidabile tra tutti gli attori.

Domanda n. 9: Qual è un metodo comunemente utilizzato per la condivisione dei dati ai sensi del Data Act e quali sono i modi per ridurre i rischi legati alla protezione dei dati?

Esistono diversi modi per ridurre i rischi associati al Data Act; l'implementazione di politiche di governance della condivisione dei dati è il primo passo. Come per la conformità al GDPR, una gestione robusta della condivisione dei dati può essere formalizzata tramite contratti e documenti che definiscono i ruoli e le responsabilità di ciascuna parte; questo è particolarmente utile tra i titolari dei dati e i terzi. I contratti potrebbero includere procedure per la gestione dell'accesso e, se necessario, l'assegnazione dei diritti di controllo degli accessi, la definizione dei requisiti di sicurezza, nonché garantire la responsabilità e la tracciabilità.

Il destinatario dei dati è generalmente un responsabile del trattamento all'interno del processo di condivisione. Tuttavia, il contratto con il terzo potrebbe prevedere una responsabilità congiunta nel trattamento se il terzo, per legge o prassi, esercita un'influenza determinante sugli obiettivi e le condizioni del trattamento. Questo potrebbe applicarsi, ad esempio, quando il terzo fornisce una API di condivisione alla quale il titolare dei dati si collega per la condivisione dei dati.

Misure per prevenire l'accesso non autorizzato, raccomandate da vari regolatori nazionali: Come per il GDPR, dovrebbe essere adottato un approccio basato sul rischio, in cui il livello di protezione richiesto sia proporzionato alla gravità delle possibili conseguenze per il soggetto dei dati o l'utente. Ad esempio, la raccomandazione dell'autorità francese per la protezione dei dati, CNIL, include quanto segue:

- Partizionare i dati da condividere tramite segmentazione fisica o logica dei dati, o entrambi. La disponibilità dei dati può diventare importante in determinate situazioni, in cui l'utente potrebbe essere seriamente danneggiato senza di essi. In tali situazioni, mantenere i dati in "compartimenti" separati può ridurre il rischio di violazione dei dati.
- Utilizzare misure tecniche aggiuntive, come una cassaforte digitale, per proteggere le password e i protocolli di autenticazione.
- Mantenere un registro completo degli accessi e delle azioni effettuate sul database per identificare eventuali abusi dei dati e errori, nonché per garantire che il Titolare dei dati /

Destinatario dei dati (o il suo agente) abbia fornito gli aggiornamenti necessari dei dati durante la condivisione continua.

- Creare un ambiente "sandbox" per la condivisione dei dati in cui gli utenti possano sperimentare in modo sicuro con i dati.

A causa del tipo specifico di dati trattati dal Data Act, il trasferimento dei dati tramite API (Application Programming Interfaces) potrebbe essere il metodo più comunemente utilizzato. Le API supportano lo scambio sicuro di dati personali e non personali tra i titolari dei dati e i terzi autorizzati. Le API generalmente offrono un livello di sicurezza più elevato rispetto alle piattaforme di condivisione dei dati o ai servizi di posta elettronica, attraverso i quali il rischio di violazioni dei dati può essere ridotto durante la condivisione.

Le API sono uno strumento preferito per la condivisione dei dati, in particolare quando:

- Grandi volumi di dati vengono aggiornati frequentemente,
- I terzi devono accedere regolarmente ai dati per soddisfare le richieste di accesso degli utenti, soprattutto quando ci sono molte richieste,
- Il terzo trasferisce direttamente i dati all'utente senza memorizzare permanentemente i dati.

Domanda n. 10: Quali sono gli obblighi per il Titolare dei dati?

Il Data Act dell'UE stabilisce diverse obbligazioni chiave per i Titolari dei Dati.

Accesso ai Dati per Progettazione e di Default

I Titolari dei Dati devono progettare e produrre prodotti connessi o servizi correlati (come i dispositivi intelligenti) affinché i dati generati dal dispositivo siano accessibili di default e gratuitamente per l'utente. Ciò include i metadati necessari per interpretare e utilizzare i dati. L'accesso deve essere facile, sicuro, completo, strutturato e fornito in un formato comune e leggibile da macchina.

Richieste di Accesso ai Dati

Se gli utenti non possono accedere direttamente ai dati tramite il dispositivo intelligente, il Titolare dei Dati deve condividere i dati su richiesta. Tali richieste devono essere soddisfatte senza indebito ritardo, in un formato comune e leggibile da macchina, gratuitamente e, se pertinente e fattibile, in modo continuo e in tempo reale. Inoltre, gli utenti possono richiedere che il Titolare dei Dati condivida i dati generati dal dispositivo con un terzo. Nel soddisfare tale richiesta, il Titolare dei Dati deve fornire i dati alle stesse condizioni descritte sopra. Tuttavia, a differenza della

condivisione dei dati con l'utente, in questo scenario il Titolare dei Dati può richiedere una compensazione ragionevole dal terzo per la condivisione dei dati. Il Titolare dei Dati deve garantire che le richieste di accesso possano essere elaborate in modo semplice e senza essere gravate da procedure o richieste di informazioni inutili da parte dell'utente.

Trasparenza

Prima di stipulare un contratto per l'acquisto, il noleggio o il leasing di un prodotto connesso, il Titolare dei Dati deve fornire all'utente informazioni chiare e comprensibili. Queste informazioni devono includere dettagli sul tipo e sul volume dei dati, i periodi di conservazione dei dati, se il prodotto genera dati continuamente e in tempo reale, e se i dati sono memorizzati in remoto o sul dispositivo. L'utente deve anche essere informato su come esercitare i propri diritti di accesso, recupero o cancellazione dei dati.

Analogamente, prima di stipulare un contratto per servizi correlati a un prodotto connesso, il Titolare dei Dati deve informare l'utente sul tipo e volume dei dati, i periodi di conservazione dei dati, i terzi che potrebbero utilizzare i dati e gli scopi per cui i dati sono utilizzati. Il Titolare dei Dati deve anche spiegare come l'utente può richiedere la condivisione dei dati con un terzo, terminare la condivisione dei dati e presentare un reclamo in caso di non conformità con il Data Act.

Portabilità dei Dati

Il Data Act consente agli utenti di trasferire i propri dati a un terzo, facilitando il passaggio tra fornitori di servizi o l'uso dei dati con applicazioni diverse. Il Titolare dei Dati deve rendere questo processo senza soluzione di continuità e garantire che i dati siano forniti in un formato comunemente utilizzato e leggibile da macchina.

Domanda n. 11: Come posso formalizzare la condivisione dei dati in un contesto Business-to-Business?

I termini e le condizioni per la condivisione dei dati devono essere formalizzati in un contratto tra le parti coinvolte. L'accordo deve essere equo, ragionevole, non discriminatorio e trasparente, il che è particolarmente importante quando la parte contraente è una piccola o media impresa, un'organizzazione senza scopo di lucro o un istituto di ricerca.

Quando un titolare dei dati condivide i dati con un'altra impresa (il destinatario dei dati) ai sensi della legge sui dati, può richiedere al destinatario dei dati un compenso ragionevole per i dati forniti.

Domanda n. 12: La mia organizzazione è un titolare del trattamento dei dati. Posso rifiutarmi di rendere disponibili i dati?

L'utente e il Titolare dei Dati possono limitare l'accesso ai dati se tale accesso potrebbe compromettere i requisiti di sicurezza del prodotto imposti dalla legge. Possono anche concordare di limitare o proibire l'accesso, l'uso o la condivisione ulteriore dei dati.
Nei casi che coinvolgono segreti commerciali, il Titolare dei Dati è autorizzato a stabilire accordi per mantenere la riservatezza dei dati e proteggere i segreti commerciali. Ciò include l'accordo su misure tecniche e organizzative per garantire la riservatezza.
Inoltre, non vi è alcun obbligo per il Titolare dei Dati di condividere i dati con un terzo situato al di fuori dell'UE.

Domanda n. 13: Qual è l'impatto del Data Act sulla gestione dei diritti degli interessati nei casi in cui i dati siano dati personali?

Il Data Act non modifica i diritti e gli obblighi stabiliti dal GDPR. Al contrario, rafforza e facilita il diritto alla portabilità dei dati. In particolare, il Data Act richiede ai Titolari dei Dati di consentire ai clienti di trasferire i propri dati entro 30 giorni.
Quando si trattano dati personali, il Titolare dei Dati in molti casi agirà come titolare del trattamento e dovrà gestire le richieste di accesso ai dati in conformità con il GDPR. Nei casi in cui l'utente sia un'organizzazione, l'utente diventa il titolare del trattamento. Il titolare del trattamento deve verificare se sono coinvolti dati personali e garantire che vi sia una base giuridica per rendere tali dati disponibili, soprattutto se l'utente non è il soggetto dei dati.

Domanda n. 14: Quali sono le basi giuridiche che possono essere utilizzate per il trattamento dei dati personali, a cui si applica il Data Act?

Il Data Act opera senza pregiudizio per il GDPR, il che significa che il GDPR prevale sul Data Act (Art. 1(5), Rec. 7 del Data Act). Di conseguenza, ogni trattamento di dati personali deve avere una base giuridica valida.
I Titolari dei Dati hanno basi giuridiche ai sensi dell'Art. 6 del GDPR. Se il soggetto dei dati è anche l'unico utente, la situazione è semplice, in quanto il Titolare dei Dati può fare affidamento sulla

base giuridica dell'adempimento di un obbligo legale (vedi Art. 6(1)(c) del GDPR, Art. 4 del Data Act). Tuttavia, se l'utente è un'organizzazione con più individui che utilizzano il dispositivo connesso, la situazione può diventare più complessa. Ad esempio, se una società utilizza un veicolo condiviso, la società deve selezionare una base giuridica che consideri i dati dei dipendenti. In tali casi, il trattamento dei dati personali generati dai dipendenti che utilizzano un veicolo aziendale potrebbe dover essere basato sul consenso (Art. 6(1)(a) e Art. 9(2) del GDPR) o sull'esecuzione di un contratto (Art. 6(1)(b) del GDPR). È importante notare che il Data Act si basa fortemente su accordi contrattuali, complementando così l'Art. 6(1)(b) del GDPR per il trattamento dei dati personali nell'ambito di un contratto. Ad esempio, in base a un contratto, un utente può condividere i dati personali con un terzo per fornire un servizio, utilizzando l'Art. 6(1)(b) come base giuridica.
Infine, nella maggior parte dei casi, il Destinatario dei Dati tratterà i dati per conto del Titolare dei Dati o dell'utente.

Domanda n. 15: La mia organizzazione è un Utente e vorrebbe elaborare i dati messi a disposizione dal Titolare dei dati sulla base del Legittimo Interesse. È possibile?

Secondo l'Articolo 6(1) f del primo paragrafo dell'Articolo 6(1) del GDPR, il trattamento può essere considerato necessario per gli interessi legittimi perseguiti dal titolare del trattamento o da un terzo, solo a condizione che:

- il titolare del trattamento abbia informato gli utenti di un interesse legittimo che viene perseguito tramite il trattamento dei dati;
- tale trattamento dei dati sia effettuato solo nella misura strettamente necessaria per gli scopi di tale interesse legittimo; e
- che risulti da un bilanciamento degli interessi contrastanti, tenendo conto di tutte le circostanze rilevanti, che gli interessi o le libertà e i diritti fondamentali degli utenti non prevalgano su tale interesse legittimo del titolare del trattamento o di un terzo.

Il test di bilanciamento pesa essenzialmente gli interessi contrastanti del titolare del trattamento contro gli interessi o i diritti e le libertà fondamentali dei soggetti dei dati.

Valutazione delle limitazioni e restrizioni

L'uso dei dati personali generati da dispositivi connessi può essere limitato o restritto in conformità

con le leggi nazionali e dell'UE applicabili. Ad esempio, le leggi nazionali sul lavoro possono regolamentare il monitoraggio dei dipendenti che utilizzano dispositivi connessi sul posto di lavoro.

Inoltre, l'interesse legittimo non può essere utilizzato come base giuridica quando i dati ricevuti dal Titolare dei Dati rientrano nelle categorie speciali di dati personali definite nell'Articolo 9 del GDPR. Questo include i dati biometrici e i dati relativi alla salute generati da dispositivi medici connessi.

Inoltre, quando i dati ricevuti dal Titolare dei Dati sono trattati per decisioni automatizzate che producono effetti giuridici riguardo al soggetto dei dati o lo influenzano in modo significativo (come nel caso del punteggio di credito automatizzato), l'interesse legittimo non può essere utilizzato come base giuridica valida. In questi casi, sarà necessaria una base giuridica diversa.

Esempi di interessi o diritti fondamentali e libertà del soggetto dei dati

I diritti e le libertà in gioco dipendono, in linea di principio, dalle circostanze specifiche del caso concreto[3].
Ad esempio, la condivisione o l'uso – non concordato con l'utente – dei dati personali generati da un'auto connessa o da un assistente domestico può rappresentare una minaccia:

- per la vita privata e familiare dei soggetti dei dati, protetta dall'Articolo 7 della Carta dei Diritti Fondamentali dell'UE (la "Carta");
- per il diritto alla sicurezza, protetto dall'Articolo 6 della Carta.

Come il DPO può assistere in questo processo

Il test di bilanciamento deve essere effettuato caso per caso, tenendo conto di tutti i rischi potenziali per i soggetti dei dati. Secondo l'Opinione 06/2014 del WP29 sulla nozione di interessi legittimi del titolare del trattamento, il titolare del trattamento dovrebbe:

- Identificare i diritti fondamentali e gli interessi del soggetto dei dati che potrebbero essere influenzati.
- Considerare le aspettative ragionevoli dei soggetti dei dati.
- Valutare gli impatti sui soggetti dei dati e confrontarli con i benefici attesi dal trattamento da parte del titolare del trattamento.

[3] Sentenza della Corte Rīgas satiksme, C-13/16, EU:C:2017:336, paragrafo 31

È importante notare che i minori meritano una protezione specifica riguardo ai loro dati personali, in quanto potrebbero essere meno consapevoli dei potenziali rischi.

Sebbene il ruolo del DPO nella valutazione degli interessi legittimi non sia specificamente regolato dal GDPR, è analogo al ruolo del DPO in una Valutazione d'Impatto sulla Protezione dei Dati (DPIA). Pertanto, il DPO dovrebbe fornire consulenza, quando richiesto dal titolare del trattamento, riguardo al test di bilanciamento e monitorarne l'esecuzione.

Domanda n. 16: La mia organizzazione è un ente pubblico. In quali situazioni la mia organizzazione può richiedere dati sulla base di una “necessità eccezionale”?

Il concetto di "necessità eccezionale" viene introdotto all'inizio del Data Act, dove l'Articolo 1(1) stabilisce che uno degli scopi del regolamento è armonizzare le norme sulla disponibilità dei dati detenuti dal Titolare dei Dati verso gli enti pubblici quando esiste una "necessità eccezionale" dei dati per eseguire un compito specifico di interesse pubblico. Questo stabilisce uno standard elevato, limitando la disposizione agli enti di tipo pubblico e richiedendo una "necessità eccezionale", specificamente per un compito di interesse pubblico. I dati resi disponibili sono limitati al soddisfacimento di questa necessità eccezionale.

Se esistessero mezzi alternativi per svolgere il compito, alcuni potrebbero sostenere che questa disposizione non si applichi. Il termine "eccezionale" tende a escludere l'uso normale e regolare, implicando che solo le circostanze veramente straordinarie possano qualificarsi. Inoltre, deve esserci un compito predefinito, identificato, che sia eccezionale e che attivi questa necessità. Se un ente pubblico non può chiaramente identificare e documentare tale "necessità eccezionale" e "compito specifico" in anticipo, potrebbe non essere in grado di invocare questa disposizione.

Inoltre, la disposizione sul campo di applicazione dovrebbe essere letta in combinazione con i dettagli specifici su cosa costituisce una necessità eccezionale e quando si applica, come ulteriormente sviluppato nel Data Act. L'Articolo 1(3) rafforza queste potenziali limitazioni, affermando che i dati possono essere resi disponibili "solo quando c'è una necessità eccezionale". Questo solleva un avviso che la disposizione sul campo di applicazione potrebbe limitare inavvertitamente l'applicazione delle disposizioni successive, forse in modi non previsti dalla legislazione.

Le principali definizioni nel Data Act non definiscono esplicitamente "necessità eccezionale". Tuttavia, l'Articolo 2(29) raggruppa "emergenza pubblica" e "situazioni eccezionali", il che potrebbe portare alcuni a interpretare la necessità eccezionale come limitata alle emergenze pubbliche. Il

termine "circostanze eccezionali" è anche menzionato in vari contesti, come negli Articoli 4(7) e 5(11), inclusi quelli relativi alla proprietà intellettuale.

Le disposizioni principali riguardanti la necessità eccezionale sono dettagliate nel Capitolo V. L'Articolo 14, intitolato "Obbligo di rendere disponibili i dati sulla base di una necessità eccezionale", stabilisce che quando un ente del settore pubblico, la Commissione, la Banca Centrale Europea o un ente dell'Unione dimostra una necessità eccezionale, come definito nell'Articolo 15, per utilizzare determinati dati – compresi i metadati necessari per interpretare e utilizzare tali dati – questi enti devono presentare una richiesta debitamente motivata.

Le entità legali, diverse dagli enti del settore pubblico, che detengono i dati pertinenti, sono quindi tenute a renderli disponibili.

L'Articolo 15 specifica che la "necessità eccezionale" deve essere limitata sia nel tempo che nell'ambito e può esistere solo in determinate circostanze, che sono chiaramente enumerate in un elenco fisso. Ad esempio, l'Articolo 15(1)(a) tratta delle risposte a un'emergenza pubblica, mentre l'Articolo 15(12)(b) copre altre circostanze che non devono coinvolgere dati personali. Va notato che c'è un'esclusione per le micro e piccole imprese nell'Articolo 15(2), sebbene anche le piccole imprese con un fatturato modesto possano gestire quantità significative di dati.

L'Articolo 17 sottolinea che l'ente pubblico deve "dimostrare" la necessità eccezionale, il che implica uno standard di prova più elevato rispetto al semplice etichettare una necessità come eccezionale. Questa richiesta potrebbe escludere situazioni che non sono realmente eccezionali. L'Articolo 17(1)(c) menziona specificamente la necessità di spiegare come i dati personali saranno trattati, sollevando potenziali questioni controverse riguardo all'interpretazione e all'applicazione. Inoltre, l'Articolo 17(2)(e) menziona il requisito di pseudonimizzazione, e l'Articolo 17(2)(c) sottolinea l'importanza della proporzionalità nella valutazione della necessità eccezionale, limitandone ulteriormente l'applicazione.

L'Articolo 18(2) tratta del processo per rispondere alle richieste di dati, inclusi i tempi, le modifiche e le distinzioni tra emergenza pubblica e altre necessità eccezionali. La compensazione per la fornitura dei dati può essere presa in considerazione, come stabilito nell'Articolo 20. Inoltre, la condivisione dei dati per la ricerca e le organizzazioni statistiche nel contesto di necessità eccezionali è discussa nell'Articolo 21.

I riferimenti alla necessità eccezionale compaiono in tutto il Data Act, in particolare nei considerando 5, 31, 63, 65, 66, 69, 70-73, 75, 77, 103 e 107, tra gli altri. Questi riferimenti e gli articoli specifici forniscono il quadro per comprendere e applicare il concetto di necessità eccezionale all'interno del Data Act.

Domanda n. 17: Come viene definita la profilazione ai sensi della legge sui dati?

La stessa definizione di profilazione è utilizzata sia nel GDPR che nel Data Act, ovvero nell'articolo 4, paragrafo 4, del GDPR, che definisce la profilazione come «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzare dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di tale persona».

Domanda n. 18: La profilazione è vietata ai sensi della legge sui dati?

Il profiling generalmente non è vietato dal Data Act. Tuttavia, il profiling non è consentito in un contesto molto specifico, ovvero quando l'utente (spesso il soggetto dei dati) condivide i dati con le organizzazioni. L'Articolo 6(2)b del Data Act rafforza i diritti dell'utente e fornisce un altro strumento per proteggersi da pratiche di profiling indesiderato.

Questa situazione è enunciata nell'Articolo 6(2)b del Data Act:

6.2 Il Terzo non deve:

...(b) nonostante l'Articolo 22(2), punti (a) e (c), del Regolamento (UE) 2016/679, utilizzare i dati che riceve per il profiling, a meno che non sia necessario per fornire il servizio richiesto dall'utente;

Per chiarezza interpretativa, riportiamo di seguito le parti pertinenti dell'Articolo 22 del GDPR. L'Articolo 22(1) afferma:

1. Il soggetto dei dati ha il diritto di non essere sottoposto a una decisione basata esclusivamente su un trattamento automatizzato, compreso il profiling, che produca effetti giuridici nei suoi confronti o che lo riguardi in modo altrettanto significativo.

Successivamente, l'Articolo 22(2) punti (a) e (c) del GDPR stabilisce:
(a) Il paragrafo 1 non si applica se la decisione: è necessaria per l'ingresso in un contratto, o per l'esecuzione di un contratto, tra il soggetto dei dati e il titolare del trattamento;
(b) ...

(c) si basa sul consenso esplicito del soggetto dei dati.

Potrebbe esserci qualche confusione nell'interpretare entrambi i testi insieme, soprattutto data la presenza di dichiarazioni negative. La clausola "nonostante l'Articolo 22(2), punti (a) e (c), del

Regolamento (UE) 2016/679" deve essere intesa come "nonostante gli Articoli 22(2) punti (a) e (c)". In circostanze normali, l'Articolo 22(2) del GDPR delinea due eccezioni all'Articolo 22(1). Tuttavia, queste due eccezioni non si applicano nel contesto dell'Articolo 6(2)(b) del Data Act.

Per maggiore chiarezza, l'Articolo 6(2)(b) deve essere interpretato in combinazione con l'Articolo 5 del Data Act. Se lo si fa, diventa chiaro che il profiling è vietato nelle situazioni in cui si applicano i seguenti tre criteri cumulativi:

- I dati personali in questione fanno parte di un prodotto (ad esempio una macchina per espresso automatica) o di dati relativi a servizi creati attraverso l'uso di prodotti connessi,
- I dati personali sono condivisi dall'utente della macchina per espresso con la tua azienda, e la tua azienda non è il Titolare dei Dati,
- Il profiling non è necessario per fornire il servizio richiesto dal soggetto dei dati.

Una volta chiarita questa interpretazione, la prossima domanda cruciale riguarda la determinazione di cosa costituisce "necessario per fornire il servizio richiesto dall'utente". Questo sarà probabilmente interpretato caso per caso. Ad esempio, un utente di un servizio di streaming musicale condivide i suoi dati di utilizzo con un'altra compagnia di intrattenimento multimediale, affinché possa godere delle stesse raccomandazioni personalizzate. Questo richiede che la compagnia di intrattenimento multimediale (Destinatario dei Dati) effettui il profiling. Poiché la richiesta proviene dall'utente e il profiling è necessario per fornire il servizio richiesto, questo tipo di profiling da parte del Destinatario dei Dati sarà molto probabilmente consentito. Tuttavia, la compagnia di intrattenimento multimediale non può effettuare il profiling per scoprire l'orario in cui i podcast vengono ascoltati, al fine di migliorare i propri processi operativi. Questo violerebbe probabilmente l'Articolo 6(2)(b).

L'ipotesi sottostante potrebbe essere che i Destinatari dei Dati non siano i Titolari originari dei Dati; quindi, avrebbero probabilmente un controllo limitato o una comprensione su come i dati sono stati raccolti o su come l'utente intendesse utilizzarli. Il profiling per servizi non correlati al prodotto o servizio per cui l'utente si è iscritto sarebbe visto come un'intrusione nei diritti di protezione dei dati dell'utente ai sensi del GDPR e per una buona ragione.

Considera il seguente scenario: una compagnia di servizi potrebbe potenzialmente utilizzare i dati del termostato delle abitazioni residenziali relativi al consumo energetico per il proprio beneficio finanziario. La compagnia potrebbe analizzare i modelli di consumo energetico e identificare i momenti di maggiore utilizzo, come le serate e i fine settimana, e rendere queste informazioni disponibili ai proprietari delle abitazioni. Potrebbero anche essere in grado di confrontare i modelli di consumo energetico tra abitazioni simili o tipi di edifici per fornire parametri di riferimento ai proprietari delle abitazioni. Immagina una situazione in cui un cliente della compagnia di servizi

decide di passare a un'altra compagnia di servizi. Potrebbe essere fatta una richiesta per condividere i dati del termostato in modo che la nuova compagnia possa fornire consigli per il risparmio energetico, e il cliente possa utilizzarli dal primo giorno del passaggio. Se il profiling è necessario per questo scopo, è consentito farlo in questo scenario.

La nuova compagnia di servizi potrebbe quindi considerare la creazione di un profilo di fedeltà che possa essere utilizzato per scegliere piani energetici incentivanti che vincolino la persona a un contratto a lungo termine con una tariffa scontata. Se il proprietario della casa passa al nuovo piano, la nuova compagnia di servizi beneficerà della stabilità finanziaria e il proprietario della casa avrà costi ridotti. Tuttavia, poiché la creazione di un profilo non è strettamente necessaria per fornire il servizio al proprietario della casa, il Data Act vieta questo profiling da parte della nuova compagnia di servizi.

Domanda n. 19: Perché la trasparenza è fondamentale ai sensi del Data Act?

Quando consideriamo tradizionalmente i dati e la trasparenza, ci concentriamo sulle norme di trasparenza relative alla fornitura di dettagli anticipati su come i dati personali saranno utilizzati e sull'ottenimento di un consenso chiaro e equo per la loro raccolta. La trasparenza svolge anche un ruolo nell'assicurare che gli individui siano consapevoli dei propri diritti sui dati e possano esercitarli. Inoltre, la trasparenza è cruciale nei contratti sui dati, nelle politiche e nei termini e condizioni tra entità, nonché tra entità e individui.

Nel contesto del Data Act, tuttavia, lo scopo della trasparenza cambia leggermente. Mentre le tradizionali norme sulla protezione dei dati rimangono in vigore, il Data Act enfatizza la trasparenza nel contesto della condivisione dei dati tra entità. Ad esempio, l'Articolo 5 sottolinea la necessità di trasparenza e condizioni eque, non discriminatorie, quando i Titolari dei Dati rendono i dati disponibili ai Destinatari dei Dati, in particolare nei trasferimenti di dati tra entità. Qui, la trasparenza potrebbe allinearsi maggiormente con le norme sulla concorrenza che con le tradizionali norme sulla protezione dei dati.

Possono sorgere disaccordi riguardo questa interpretazione, ma questi problemi molto probabilmente diventeranno più chiari man mano che gli organi di risoluzione delle controversie istituiti dall'Articolo 10 inizieranno a giudicare su questioni come la trasparenza. Sarà importante vedere se queste regole procedurali considerano solo il Data Act o se prenderanno in considerazione anche le norme sulla protezione dei dati.

L'Articolo 28 del Data Act fa riferimento al modello tradizionale di fornitura di informazioni preventive, in particolare riguardo agli obblighi contrattuali relativi all'accesso internazionale ai dati

e al loro trasferimento. Sebbene la sezione non menzioni esplicitamente la "trasparenza", gli obblighi di informazione preventiva tramite i siti web sono chiari, e i professionisti dovranno affrontare pienamente questi requisiti per evitare potenziali problematiche.

La trasparenza è anche trattata nell'Articolo 19, che introduce "obblighi di trasparenza" che potrebbero richiedere la conservazione dei dati in determinate circostanze, potenzialmente prevalendo sui requisiti di cancellazione o eliminazione dei dati. Questo si applica in particolare agli enti del settore pubblico.

Inoltre, anche in assenza di espliciti requisiti di trasparenza, tali requisiti potrebbero essere necessari o impliciti per far funzionare efficacemente altre disposizioni. Ad esempio, potrebbe essere difficile giustificare un'azione se determinati aspetti sono stati eseguiti in modo poco trasparente. Questo è strettamente legato al concetto di comprendere e rispettare le aspettative ragionevoli degli individui. Un esempio pratico potrebbe essere considerare se l'uso storico dei dati possa essere esteso a una nuova applicazione di intelligenza artificiale senza violare tali aspettative.

Infine, la trasparenza è anche menzionata in diversi Considerando del Data Act, tra cui i Considerando 5, 24, 25, 34, 42, 51, 65, 69 e 73, che i lettori potrebbero voler esaminare per ulteriori dettagli contestuali.

Link Utili

- Data Act testo https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng
- Informazioni relative alla Strategia Digitale UE https://digital-strategy.ec.europa.eu/en/policies/strategy-data
- Sito web della Commissione riguardante il Data Act https://digital-strategy.ec.europa.eu/en/policies/data-act, compresivo di FAQ riguardo il Data Act: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act
- Regolamento sul quadro normativo per la libera circolazione dei dati non personali nell'Unione europea https://eur-lex.europa.eu/eli/reg/2018/1807/oj
- Linee guida sul regolamento relativo a un quadro per la libera circolazione dei dati non personali nell'Unione europea https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2019:250:FIN
- GDPR https://eur-lex.europa.eu/eli/reg/2016/679/oj
- Linee guida della CNIL: Raccomandazione sull'uso delle interfacce di programmazione delle applicazioni (API) per la condivisione sicura dei dati personali (in francese) https://www.cnil.fr/sites/cnil/files/2023-07/recommandation_api.pdf

Disclaimer

Le informazioni fornite in queste FAQ hanno solo scopo informativo e didattico. Non devono essere interpretate come consulenza legale. Per indicazioni specifiche relative alla tua situazione, ti invitiamo a consultare un professionista legale qualificato.