Il nuovo valore dei dati nei mercati digitali: le opportunità per le imprese tra l'evoluzione del GDPR, le novità del Data Governance Act e gli scenari del Data Act.

Workshop di formazione pratica organizzato da Confindustria Udine - 4 Dicembre 2024.

FIVERS

L’evoluzione tecnologica e normativa in UE nel Decennio Digitale 2020-2030.

FIVERS

IL DECENNIO DIGITALE DELLA UE – AGENDA DIGITALE 2030

Il **9 marzo 2021** la Commissione ha presentato una visione e prospettive per la trasformazione digitale dell'Europa entro il 2030. Questa visione per il decennio digitale dell'UE si sviluppa intorno a quattro punti cardinali:

Competenze (Specialisti delle TIC: 20 milioni + convergenza di genere - Competenze digitali di base: min. 80% della popolazione)

Trasformazione digitale delle imprese (Introduzione della tecnologia: 75% delle imprese dell'UE che utilizzano cloud/IA/Big Data; Innovatori: aumentare scale-up e finanziamenti per raddoppiare gli "unicorni" dell'UE, attualmente 35 fondatori e amministratori delegati, facenti parte del gruppo di Unicorni europei selezionato dalla Commissione Ue, startup che si occupano di software, hardware, tecnologie avanzate e tecnologia ecologica che stanno già dialogando con le istituzioni comunitarie per progettare insieme il futuro del Vecchio Continente)

FIVERS

IL DECENNIO DIGITALE DELLA UE – AGENDA DIGITALE 2030

Digitalizzazione dei servizi pubblici (servizi pubblici fondamentali: 100% online; sanità online: cartelle cliniche disponibili al 100%; identità digitale: 80% cittadini che utilizzano l'ID digitale)

Infrastrutture digitali sicure e sostenibili (connettività: gigabit per tutti, 5G ovunque; semiconduttori all'avanguardia: raddoppiare la quota dell'UE nella produzione mondiale; Dati - Edge e Cloud: 10.000 nodi periferici altamente sicuri a impatto climatico zero; Informatica: primo computer con accelerazione quantistica).

Queste quattro linee direttrici (**Skills**, **Governance**, **Business**, **Infrastructures**) saranno tradotte in termini concreti per il 2030 attraverso obiettivi e tappe fondamentali, una solida struttura di governance, progetti multinazionali che combinano investimenti dell'UE, degli Stati membri e del settore privato.

Importante anche la prospettiva multilaterale e internazionale, per la quale la UE prevede partnership globali e progetto di cooperazione internazionale.

FIVERS

Il Decennio Digitale UE 2020-2030: una rassegna delle fondamentali normative in vigore.

FIVERS

LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

Regolamento (UE) 2024/1689 – Regolamento Generale UE sull'Intelligenza Artificiale

Il **Regolamento (UE) 2024/1689** del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea del 12 Luglio 2024.

Rappresenta la prima legge organica e completa al mondo per la disciplina dell'Intelligenza Artificiale e mira ad affrontare i rischi per la salute, la sicurezza e i diritti fondamentali. Inoltre, il Regolamento 2024/1689 tutela la democrazia, lo Stato di diritto e l'ambiente.

Il Regolamento 2024/1689 è entrato in **vigore il 1° agosto 2024** e sarà applicabile integralmente tra Febbraio 2025 e agosto 2027.

Il Regolamento 2024/1689 si applicherà ai soggetti pubblici e privati, all'interno e all'esterno dell'UE, a condizione che il sistema di IA sia immesso sul mercato dell'Unione o che il suo utilizzo abbia effetti su persone situate nell'UE.

Il Decennio Digitale UE 2020-2030: una rassegna delle fondamentali normative in vigore.

Regolamento 2022/2065 - Legge sui servizi digitali (Digital Service Act - DSA)

Il Regolamento UE 2022/2065 introduce una nuova disciplina organica delle piattaforme digitali e riscrive le regole su piattaforme, attività di fornitura di beni e servizi on line, tutela dei diritti fondamentali degli utenti europei, misure per contrastare contenuti illegali online, etc. Il Digital Services Act entra in vigore il 16 novembre 2022, e si applica a tutti dallo scorso **17 febbraio 2024**, mentre le piattaforme online di grandi dimensioni e i motori di ricerca online di grandi dimensioni sono già obbligati dal **25 agosto 2023** a conformarsi alle nuove norme

Regolamento (UE) 2022/1925 - Digital Markets Act - DMA

Il *Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (Regolamento sui mercati digitali*), anche noto come Digital Markets Act, **è applicabile dal 2 Maggio 2023**. Il DMA mira a rendere i mercati digitali più equi e competitivi, dopo che negli ultimi 10 anni l'Unione europea ha dovuto imporre multe record per alcune pratiche commerciali dannose da parte di operatori digitali molto grandi (le cosiddette Big Tech Companies). Per la prima volta al mondo il DMA vieterà direttamente alle piattaforme che fungono da "gatekeeper" nel settore digitale (veri e propri guardiani dell'accesso ai mercati degli operatori commerciali e che finiscono per diventare quelli che la Commissione UE ha chiamato "legislatori privati") talune pratiche sui servizi resi (dai motori di ricerca, ai social networks, alle piattaforme di condivisione video, fino agli assistenti vocali) e creerà uno spazio economico più equo e competitivo per i nuovi attori e le imprese europee.

Il Cybersecurity Package della UE

Regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativo alla **resilienza operativa digitale per il settore finanziario** e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (Regolamento DORA applicabile dal **17 Gennaio 2025**)

Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un **livello comune elevato di cybersicurezza** nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (**Direttiva NIS 2** – (recepita con decreto legislativo **4 settembre 2024, n. 138**).

Direttiva (UE) 2022/2557 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 del Parlamento europeo e del Consiglio relativa alla **resilienza dei soggetti critici** e che abroga la direttiva 2008/114/CE del Consiglio (recepito con decreto legislativo **4 settembre 2024, n. 134**).

Crypto-attività e Fintech

Regolamento (UE) 2023/1114 del Parlamento Europeo e del Consiglio del 31 maggio 2023 relativo ai **mercati delle cripto-attività** e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937 (**Regolamento MiCAR**, applicabile dal **30 Dicembre 2024**)

Regolamento (UE) 2022/858 del Parlamento Europeo e del Consiglio del 30 maggio 2022 relativo a un **regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito** e che modifica i regolamenti (UE) n. 600/2014 e (UE) n. 909/2014 e la direttiva 2014/65/UE (in vigore dal 24 Marzo 2023).

D.L. 17 marzo 2023, n. 25, recante "*Disposizioni urgenti in materia di emissioni e circolazione di determinati strumenti finanziari in forma digitale e di semplificazione della sperimentazione FinTech*".

Regolamento (UE) 2024/1183 – eIDAS 2

Il Regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale.

Il nuovo regolamento europeo – **in vigore dal 1° maggio 2024** - modifica il regolamento eIDAS del 2014 sull'identità digitale contiene numerose novità che riguardano la presenza di **nuovi servizi fiduciari** e una **nuova impostazione per quelli già presenti** nella versione precedente del regolamento.

I nuovi servizi fiduciari sono **l'attestazione elettronica degli attributi**, il **certificato di autenticazione di sito web**, la **gestione di dispositivi qualificati per la creazione di una firma elettronica (o un sigillo elettronico) a distanza**, **l'archiviazione elettronica** e i **registri elettronici**.

E' inoltre istitutiito il nuovo Portafoglio europeo dell'identità digitale (**EUID Wallet**).

Regolamento (UE) 2023/988 sulla sicurezza generale dei prodotti on line o con elementi digitali (GPSR)

Regolamento (UE) 2023/988 del Parlamento europeo e del Consiglio del 10 maggio 2023 relativo alla **sicurezza generale dei prodotti**, che modifica il regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio e la direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio, e che abroga la direttiva 2001/95/CE del Parlamento europeo e del Consiglio e la direttiva 87/357/CEE del Consiglio (*General Product Safety Regultion* – **GPSR**).

Il regolamento – **applicabile dal 13 Dicembre 2024** - prevede una serie di obblighi a carico di **produttori, venditori e mercati online** operanti all'interno dell'eurozona e si propone di regolamentare al meglio un **commercio digitale** sempre più rilevante. Tra le novità: l'ampliamento dei criteri di valutazione della sicurezza dei prodotti, come l'aspetto, in particolare quegli aspetti che imitano il cibo o che attraggono i bambini, e le **caratteristiche di cybersecurity** necessarie per proteggere il prodotto; la regolamentazione delle vendite online, che vengono equiparate a quelle offline, e **obblighi specifici per tutti gli operatori economici all'interno della catena di fornitura, inclusi i fornitori di mercati online, che dovranno implementare dei processi interni per la sicurezza dei prodotti e registrarsi sul portale Safety Gate per una corretta gestione di segnalazioni e richiami**.

Regolamento Europeo 2024/2847 relativo a requisiti orizzontali (ovvero generali) di cybersecurity per i prodotti con elementi digitali (Cyber Resilience Act – CRA).

Il Regolamento Europeo 2024/2847, pubblicato nella Gazzetta ufficiale dell'UE il 20 novembre 2024, **impone requisiti di sicurezza informatica per i prodotti con elementi digitali**. Specifica i requisiti essenziali per la gestione della sicurezza e delle **vulnerabilità**, delinea gli **obblighi per i fabbricanti**, **comprese le valutazioni della conformità e dei rischi**, e stabilisce gli obblighi di **segnalazione per le vulnerabilità** sfruttate attivamente.

Gli importatori e i distributori devono garantire il rispetto delle norme e la dovuta diligenza, con l'applicazione da parte delle autorità degli Stati membri, comprese eventuali **sanzioni pecuniarie fino a 15 milioni di euro**.

Il Regolamento entra in vigore il **10 dicembre 2024** e diventa **applicabile dall'11 dicembre 2027**, con obblighi di segnalazione a partire dall'11 settembre 2026.

Direttiva (UE) 2024/2853 sulla responsabilità da prodotto difettoso.

La Direttiva sulla responsabilità da prodotto difettoso (UE) 2024/2853, pubblicata il **18 novembre 2024 ed in vigore dall'8 dicembre 2024,** sostituisce la Direttiva 85/374/CEE del Consiglio, che stabilisce la responsabilità per i prodotti difettosi. La direttiva si applicherà ai prodotti immessi sul mercato o messi in servizio dopo il **9 dicembre 2026**.

Importante il capitolo sul danno da **Intelligenza Artificiale difettosa**. La direttiva definisce gli **sviluppatori** o i **produttori di software e di sistemi di intelligenza artificiale come "produttori" e affronta le implicazioni in termini di responsabilità delle modifiche apportate ai prodotti attraverso gli aggiornamenti del software, compreso l'apprendimento dell'intelligenza artificiale.**

La direttiva fornisce, inoltre, ai **tribunali nazionali specifiche linee guida per valutare la difettosità e il nesso di causalità caso per caso**, affermando che non è necessario che i ricorrenti dimostrino la **complessità tecnica dei sistemi di IA perché i tribunali riconoscano la difettosità del prodotto.**

Direttiva 2024/2831 relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali.

Con la pubblicazione nella Gazzetta Ufficiale della UE della Direttiva 2024/2831 si introducono nuove norme (**che gli Stati Membri dovranno recepire entro il 2 Dicembre 2026**) per **migliorare le condizioni di lavoro e la protezione dei dati personali nel lavoro mediante piattaforme digitali**. La nuova regolamentazione introduce misure volte a facilitare la determinazione della corretta situazione occupazionale delle persone che svolgono un lavoro mediante piattaforme digitali; promuove **la trasparenza, l'equità, la supervisione umana, la sicurezza e la responsabilità nella gestione algoritmica del lavoro mediante piattaforme digitali e migliora la trasparenza** del lavoro sulle piatteforme digitali, anche in situazioni transfrontaliere.

Vengono stabiliti **diritti minimi** che si applicano a tutte le persone che svolgono un lavoro mediante piattaforme digitali nell'Unione. Sono inoltre previste anche **specifiche norme volte a migliorare la protezione dei dati personali dei lavoratori delle piattaforme** in materia di i **sistemi di monitoraggio automatizzati o di sistemi decisionali automatizzati**, con specifiche misure su gestione algoritmica e profilazione del lavoratore.

Regolamento (UE) 2022/868 – Governance Data Act - DGA

Il *Regolamento (UE) 2022/868 del Parlamento Europeo e del Consiglio del 30 Maggio 2022 relativo alla governance europea dei dati e che modifica il Regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati)* introduce nuove norme **(applicabili dal 24 Settembre 2023 ai dati sia personali che non personali, mentre le nuove norme del decreto legislativo di coordinamento al DGA n. 144/2024 sono applicabili dal 17 Ottobre 2024)** su nuovi modelli di business per l'intermediazione dei dati (***data sharing***), sulla istituzione di solidi meccanismi per facilitare il riutilizzo di alcune categorie di dati protetti del settore pubblico; sulla promozione in tutta l'Unione Europea del cosiddetto **"*altruismo dei dati*"** (meccanismo per facilitare la scelta di privati e soggetti pubblici di rendere volontariamente disponibili i dati per il bene comune, come i progetti di ricerca medica basati du dati condivisi in tutta l'UE), sulla creazione di **Spazi comuni europei di dati** per la condivisione e la messa in comune dei dati specifici in settori specifici, fino alla istituzione di meccanismi che garantiscono il controllo da parte degli interessati e dei titolari dei dati sui dati che li riguardano e rafforzano la loro consapevolezza per l'esercizio efficace dei diritti.

Regolamento 2023/2854 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (Normativa sui dati – Data Act).

L'**11 Gennaio 2024** è entrato in vigore il regolamento sui dati, che sarà applicabile dal **12 Settembre 2025**. Le nuove norme definiscono i diritti di accesso ai dati generati da dispositivi o servizi connessi nell'UE e di utilizzo in tutti i settori economici e faciliteranno la condivisione dei dati, in particolare dei dati industriali.

Le nuove regole consentono agli utenti dei prodotti connessi di accedere ai dati generati da questi dispositivi e di condividerli con terze parti. La legge sui dati **protegge infatti le imprese europee dalle clausole contrattuali abusive** nei contratti di condivisione dei dati che una parte contraente impone unilateralmente all'altra. Ciò consentirà in particolare alle piccole e medie imprese (PMI) di partecipare più attivamente al mercato dei dati.

Inoltre, il Data Act consentirà ai clienti **di passare senza problemi (ed eventualmente gratuitamente) da un fornitore di servizi cloud all'altro.**

Gli enti pubblici saranno in grado di accedere ai dati detenuti dal settore privato e di utilizzarli per contribuire a rispondere a emergenze pubbliche e – infine – sono previste **misure volte a promuovere lo sviluppo di norme di interoperabilità** per la condivisione dei dati e per i servizi di trattamento dei dati.

FIVERS

LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

Di quali dati parliamo?

.

FIVERS

LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

Il concetto di «dati» nell'attuale panorama normativo.

«dati»: qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva; (art. 2, n. 24 del **Digital Markets Act - DMA**; art. 2, n. 1 del **Data Act**; art. 2, n. 1 del **Data Governance Act – DGA**).

«dati personali»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4, n. 1 del **GDPR**).

«dati non personali»: dati diversi dai dati personali (art. 3, n. 1 del Regolamento 2018/1807 sul quadro di libera circolazione dei dati non personali nell'Unione Europea).

Regolamento UE 2024/1689 sull'Intelligenza Artificiale – AI Act

Il concetto di «dati» nell'attuale panorama normativo.

Art. 3, n. 35 Regolamento eIDAS

«documento elettronico»: qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva.

Art. 2, n. 1, lettera (p) del CAD

«documento informatico»: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

FIVERS

Il Decennio Digitale UE 2020-2030: la Strategia europea dei Dati.

FIVERS

LA STRATEGIA EUROPEA DEI DATI

Che rapporto intercorre tra il Data Governance Act e la Strategia Europea dei Dati avviata dall'Unione Europea?

La **Strategia europea dei Dati** che la Commissione UE ha annunciato nel mese di febbraio 2020 si basa sula creazione di Spazi di libera circolazione e condivisione di dati (personali e non personali) in numerosi settori strategici: salute (primo spazio a essere istituito,), agricoltura, produzione, energia, mobilità e trasporti, ambiente e Green Deal, finanza, pubblica amministrazione, competenze, cloud europeo per la scienza aperta. Dal 2020, inoltre, sono emersi anche spazi di dati in altre aree importanti come i media e il patrimonio culturale.

L'obiettivo finale è che insieme gli spazi di dati formino un unico Spazio Europeo dei Dati e un vero mercato unico dei dati.

Gli Spazi europei di dati - comuni e interoperabili a livello dell'UE in settori strategici, i **"domini"** - riuniscono le pertinenti **infrastrutture di elaborazione** e le **regole normative** e tecniche della relativa governance, al fine di facilitare la messa in comune e la condivisione dei dati, liberando **l'enorme potenziale dell'innovazione basata sui dati**.

LA STRATEGIA EUROPEA DEI DATI

I dati (sia quelli personali che quelli non personali) rappresentano difatti il fulcro della trasformazione digitale. Infatti definiscono il modo in cui produciamo, consumiamo e viviamo.

L'accesso al crescente volume di dati e la capacità di utilizzarli sono essenziali per l'innovazione e la crescita. L'innovazione basata sui dati può comportare significativi e concreti benefici per i cittadini - ad esempio attraverso una medicina personalizzata o una mobilità più efficiente - e per l'economia europea, dal perfezionamento del processo decisionale al miglioramento dei servizi pubblici.

Per questo la Commissione UE ha approvato il **Regolamento (UE) 2022/868 sulla governance dei dati** che costituisce la cornice normativa generale della Strategia Europea dei Dati e fissa le regole nell'ambito della creazione di un **Mercato Unico dei Dati** all'interno del quale:

LA STRATEGIA EUROPEA DEI DATI

1. i **dati personali e non personali potranno circolare all'interno dell'UE e in maniera trans-settoriale**, a beneficio di tutti e nel pieno rispetto della normativa sulla tutela della vita privata e sulla protezione dei dati e del diritto della concorrenza;
2. le **norme relative all'accesso ai dati e al loro utilizzo sono eque, pratiche e chiare e promuovono lo sviluppo della *Value Data Economy***, una economia basata sul valore generato dalla circolazione dei dati (che entro il **2025 aumenterà del 530%, con un valore stimato di 829 miliardi di Euro**) e che creerà **nuovi servizi e opportunità, come i servizi di intermediazione dei dati**, e renderà sempre più attrattivo investire, ad esempio, in strumenti e infrastrutture di prossima generazione per l'archiviazione e l'elaborazione dei dati;
3. si determinano le **condizioni giuridiche, tecniche ed economiche per creare una capacità di cloud a livello europeo**, per condividere dati europei in settori chiave, con spazi di dati interoperabili e comuni (gli Spazi Europei dei Dati settoriali);
4. si introducono diritti, strumenti e competenze offerti agli **utenti** per consentire loro di mantenere il **pieno controllo dei propri dati.**

Il Regolamento 2022/868 recante le regole per la governance europea dei dati.
Data Governance Act - DGA.

FIVERS

Che cosa è il Data Governance Act?

Il *Regolamento (UE) 2022/868 del Parlamento Europeo e del Consiglio del 30 Maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati)* promuove la disponibilità e la condivisione dei dati personali e non personali (data sharing), creando uno Spazio europeo dei dati affidabile per facilitarne l'uso per la ricerca e la **creazione di nuovi servizi e prodotti innovativi nel settore sia pubblico che privato**.

Anche noto come *Data Governance Act* (DGA), il Regolamento UE introduce un **nuovo modello di business per l'intermediazione dei dati**, istituisce solidi meccanismi per facilitare il **riutilizzo di alcune categorie di dati protetti del settore pubblico** e promuove in tutta la UE il c.d. **altruismo** (cioè facilita per i privati e i soggetti pubblici la possibilità di rendere volontariamente disponibili i dati per il bene comune, come i progetti di ricerca medica dei dati in tutta l'UE).

Quando entra in vigore ed è applicabile il Data Governance Act?

Il Regolamento 2022/868 sulla Governance europea dei dati è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea del 3 Giugno 2022 ed è entrato in **vigore il 23 Giugno 2022.**

E' applicabile dal 24 Settembre 2023.

Entro il **24 settembre 2025** (quindi dopo il primo biennio applicativo) la Commissione effettuerà inoltre una valutazione del regolamento e presenterà al Parlamento europeo, al Consiglio UE e al Comitato economico e sociale europeo una relazione sulle principali conclusioni tratte. La relazione, se necessario, potrà essere corredata di proposte legislative.

Dopo questa prima valutazione **non sono previste rivalutazioni periodiche del DGA** (come al contrario avviene, ad esempio, per il GDPR, soggetto a valutazioni applicative periodiche ogni quattro anni).

La normativa italiana di coordinamento: il decreto legislativo 144/2024.

Il d.lgs. 144/2024 è la normativa nazionale di coordinamento che **rende operativo in Italia tutto il relativo quadro normativo del DGA**. Il decreto, in vigore e applicabile dal **22 ottobre 2024**, designa **l'Agenzia per l'Italia digitale** – AgID

- quale autorità' competente per **(i)** la procedura di **notifica** per i servizi di intermediazione dei dati, organismi che poi provvede a monitorare e controllare e **(ii)** per la **registrazione delle organizzazioni per l'altruismo dei dati**, emanando anche le relative norme tecniche inclusive del monitoraggio e del controllo di tali enti;

- quale organismo competente per assistere gli enti pubblici che concedono o rifiutano l'accesso al riutilizzo delle categorie di dati detenuti dai soggetti pubblici;

- quale sportello unico, estendendo compiti e funzioni già previste in qualità di punto d'accesso unico garantito dal catalogo nazionale dei dati aperti di cui all'articolo 9, comma 2, del decreto legislativo 24 gennaio 2006, n. 36.

La normativa italiana di coordinamento: il decreto legislativo 144/2024.

L'AgID opera in stretta cooperazione con **l'Agenzia per la cybersicurezza nazionale, l'Autorità' garante della concorrenza e del mercato e il Garante per la protezione dei dati personali** e, a tal fine, può stipulare con le altre Autorità specifici **accordi di collaborazione** che definiscono le forme e i modi di esercizio del coordinamento, anche endoprocedimentale, delle competenze, nell'ambito delle
rispettive attribuzioni in relazione alla materia trattata.

Quali sono gli obiettivi del Data Governance Act?

Come si legge nel *Considerando* (2) del DGA, nel corso dell'ultimo decennio le tecnologie digitali hanno trasformato l'economia e la società, influenzando tutti i settori di attività nonché la vita quotidiana. I dati sono al centro di tale trasformazione, come la Commissione UE ha evidenziato nella sua Comunicazione del 19 febbraio 2020 «*Strategia europea per i dati*», in cui ha descritto la visione di uno Spazio comune europeo di dati ora attuato dal DGA: un **mercato interno dei dati** nel quale questi ultimi **possano essere utilizzati indipendentemente dal loro luogo fisico di conservazione nell'Unione**, nel rispetto della normativa applicabile (tra l'altro, tale accesso e utilizzo si rivelano fondamentali anche per il rapido sviluppo delle **tecnologie di intelligenza artificiale**). Dunque, **l'innovazione guidata dai dati** in un ambiente che il DGA rende sicuro e affidabile genererà benefici enormi sia per i cittadini dell'Unione che per l'economia.

IL REGOLAMENTO UE 2022/868 SULLA GOVERNANCE EUROPEA DEI DATI - DGA

In questo scenario, il DGA mira a garantire:

1. l'introduzione di una **solida governance europea dei dati** e di un quadro di regole armonizzato per gli scambi dei dati quali presupposti per garantire condizioni di parità nella *Data Economy* (che deve essere antropocentrica e affidabile) a tutti i portatori di interessi;

2. l'istituzione di meccanismi per quanto riguarda il **riutilizzo di alcune tipologie di dati detenuti dagli enti pubblici** (il DGA non introduce comunque alcun obbligo di consentire il riutilizzo dei dati detenuti da enti pubblici, lasciando liberi gli Stati membri sul punto);

3. l'istituzione di adeguati meccanismi (mediante l'introduzione di regole per la notifica e il controllo) relativamente alla **fornitura di servizi di intermediazione dei dati da parte dei relativi fornitori di servizi di intermediazione dei dati (che possono certificarsi come tali ai sensi del DGA) agli interessati, ai titolari e agli utenti dei dati**;

4. l'istituzione di **meccanismi per la condivisione** dei dati.

IL REGOLAMENTO UE 2022/868 SULLA GOVERNANCE EUROPEA DEI DATI - DGA

5. la **creazione di spazi comuni europei di dati per la condivisione e la messa in comune dei dati specifici per dominio** in settori quali la sanità (per cui esistono già anche direttive specifiche sull'accesso ai dati sanitari), la mobilità (per cui esistono già anche Regolamenti UE e norme di Direttive specifiche sull'accesso ai dati dei veicoli e in generale sulla mobilità), l'industria manifatturiera, i servizi finanziari, l'energia, l'agricoltura, l'ambiente, la pubblica amministrazione etc, per rendere i dati **reperibili, accessibili, interoperabili e riutilizzabili** («***principi FAIR per i dati***»), garantendo nel contempo un elevato livello di cybersicurezza.

6. l'istituzione di **meccanismi che garantiscono neutralità dell'accesso ai dati**, creando fiducia tra gli individui e le imprese (anche attraverso una maggiore trasparenza per quanto riguarda la finalità dell'utilizzo dei dati e le condizioni in cui i dati sono conservati dalle imprese) per quanto riguarda l'accesso ai dati, la loro condivisione e il loro controllo, utilizzo e riutilizzo;

7. l'istituzione di **meccanismi che garantiscono portabilità e interoperabilità dei dati**;

8. misure volte ad evitare **effetti di dipendenza («lock-in»);**

IL REGOLAMENTO UE 2022/868 SULLA GOVERNANCE EUROPEA DEI DATI - DGA

9. l'istituzione di **meccanismi che garantiscono il controllo da parte degli interessati e dei titolari dei dati sui dati** che li riguardano e la loro consapevolezza per esercitare fattivamente i propri diritti;

10. l'istituzione di adeguati meccanismi per la raccolta e il trattamento dei dati messi a disposizione **a fini altruistici** da persone fisiche e giuridiche (c.d. "*altruismo dei dati*");

11. condizioni chiare **per agevolare l'accesso e l'utilizzo** dei dati in tutta l'Unione per la ricerca e l'innovazione europee da parte di soggetti pubblici e privati, **superando gli attuali ostacoli connessi a requisiti procedurali tecnici e giuridici** per poter avere accesso ai dati;

12. L'istituzione di un organismo europeo di monitoraggio competente sull'applicazione del DGA: il ***Comitato europeo per l'innovazione in materia di dati*.**

FIVERS

Il rapporto tra DGA, GDPR e Regolamento 2018/1807 sui dati non personali.

FIVERS

IL RAPPORTO TRA IL REGOLAMENTO UE 2022/868 E IL GDPR

Il Considerando (4) del DGA e l'articolo 1, comma 3, specificano che il Regolamento sulla governance europea dei dati **lascia impregiudicati** sia il **GDPR** che il **Regolamento 2018/1807** sui dati non personali (oltre che la Direttiva sulla tutela dei dati su reti di comunicazione elettronica 2002/58 e la Direttiva sul trattamento dei dati nel comparto di prevenzione e accertamento dei reati **2018/680**), **non** potendosi tra l'altro ritenere il DGA come **creazione di una nuova base giuridica per il trattamento dei dati personali** per nessuna delle attività regolamentate, né come **modifica dei requisiti in materia di informativa** stabiliti nel GDPR, né come **impedimento per i trasferimenti transfrontalieri** di dati in conformità al Capo V – articoli da 44 a 50 - del GDPR.

Tuttavia, al contrario, un **collegamento tra DGA e GDPR** è insito laddove il DGA prescrive che per quanto concerne i dati personali, il loro trattamento (ad esempio negli spazi europei dei dati) deve in generale essere **basato su una o più delle basi giuridiche per il trattamento dei dati personali previste agli articoli 6 e 9 del GDPR**.

In caso di conflitto tra il DGA, il GDPR e le normative nazionali di coordinamento sulla protezione dei dati personali, questi ultimi atti normativi **prevalgono sul DGA**.

IL RAPPORTO TRA IL REGOLAMENTO UE 2022/868 E IL GDPR

Che rapporto c'è tra il DGA e il Regolamento UE 2018/1807 sui dati non personali?

Intanto, il DGA lascia impregiudicata l'applicazione della disciplina di cui al Regolamento 2018/1807 sul trattamento e la libera circolazione dei dati non personali.

Inoltre, i concetti di "dati" e di "dato non personale" nei due testi normativi non appaiono essere così distanti dal punto di vista definitorio e il DGA amplia le condizioni di accesso, utilizzo, riutilizzo, impiego, condivisione e circolazione anche dei dati non personali, oltre che i diritti, il potere di controllo e le relative tutele per titolari di dati e utenti dei dati.

Ad esempio, l'articolo 2(6) del DGA introduce il concetto – estraneo al Regolamento 2018/1807 – di **«autorizzazione»:** il conferimento agli utenti dei dati di uno **specifico diritto al trattamento dei dati non personali per utilizzare i dati non personali a fini commerciali o non commerciali**.

L’ambito di applicabilità del Data Governance Act.

FIVERS

L'AMBITO DI APPLICABILITA' DEL DATA GOVERNANCE ACT

Il DGA si **applica:**

1. a qualsiasi persona giuridica, compresi gli enti pubblici e le organizzazioni internazionali, o persona fisica (cui non si riferiscono i dati) **che ha il diritto di concedere l'accesso** a determinati dati personali o dati non personali o di condividerli (l'articolo 2, n. 8 del DGA definisce tali soggetti come "**titolari dei dati**", da non confondere con i "titolari del trattamento" del GDPR);

2. a **qualsiasi persona fisica o giuridica che ha accesso legittimo a determinati dati personali o non personali** e che ha diritto, anche a norma del GDPR in caso di dati personali, di **utilizzare tali dati a fini commerciali o non commerciali** (l'articolo 2, n. 9 del DGA definisce tali soggetti come "**utenti dei dati**");

3. agli **interessati,** che ai sensi del GDPR sono le (sole) persone fisiche a cui si riferiscono i dati personali;

4. ai **fornitori del «*servizio di intermediazione dei* dati»** inteso come un servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra interessati, titolari dei dati e utenti dei dati;

L’AMBITO DI APPLICABILITA’ DEL DATA GOVERNANCE ACT

5. a **cooperative dei dati** costituite da interessati, imprese individuali o da PMI per la fornitura di servizi di intermediazione dei dati a favore dei propri membri;

6. a **enti pubblici, organismi di diritto pubblico, impese pubbliche o private** (se così decidono gli Stati Membri, **purché** nell’esercizio di funzioni del settore pubblico o che forniscono servizi di interesse generale: difatti **il DGA non si applica a imprese pubbliche**) come definiti rispettivamente all’articolo 2, punti nn. 17, 18 e 19 del DGA;

7. al «**rappresentante legale**» stabilito nell'Unione ed esplicitamente designato ad agire per conto di un fornitore di servizi di intermediazione dei dati non stabilito nell'Unione (cfr. anche la specifica definizione contenuta all’articolo 2, punto n. 21 del DGA).

FIVERS

I principali concetti giuridici del DGA.

FIVERS

I PRINCIPALI CONCETTI GIURIDICI DEL DATA GOVERNANCE ACT

Le **definizioni giuridiche contenute all'articolo 2 del DGA evidenziano aspetti e scelte legislative interessanti**.

Intanto: la stretta correlazione tra questo Regolamento e il GDPR, tanto che su 21 definizioni giuridiche, **6 sono tratte (o richiamano) il GDPR**, e in particolare: la definizione di "dato personale", "trattamento", "consenso", "interessato", "stabilimento principale".

La definizione di cui all'art. 2(20) di «*ambiente di trattamento sicuro*»: richiama invece la conformità dell'ambiente fisico o virtuale in cui avviene il trattamento e dei relativi mezzi organizzativi al GDPR quale presupposto di sicurezza.

Garantire un ambiente di trattamento **sicuro** implica ai sensi del DGA **assicurare** i diritti degli interessati, rispettare i **diritti di proprietà intellettuale** e la **riservatezza commerciale e statistica**; garantire **l'integrità e l'accessibilità**, mediante azioni di monitoraggio da parte della entità che fornisce l'ambiente di trattamento sicuro la quale deve essere in grado di **determinare e controllare tutte le azioni di trattamento** dei dati, compresi la visualizzazione, la conservazione, lo scaricamento, l'esportazione dei dati e il calcolo dei **dati derivati** mediante algoritmi computazionali.

I PRINCIPALI CONCETTI GIURIDICI DEL DATA GOVERNANCE ACT

Il **concetto di sicurezza** che può trarsi dalla definizione di cui all'articolo 2(20) del DGA è dunque **più ampio del concetto di sicurezza del GDPR**, che all'articolo 32 definisce un perimetro di security più specifico (con misure "*tecniche e organizzative adeguate*" di protezione dei dati personali, dei servizi e dei sistemi di trattamento, di cui devono essere garantite riservatezza, integrità, disponibilità e resilienza).

La sicurezza del GDPR – e la relativa valutazione del rischio – si incentrano sui dati, sul trattamento e sui sistemi/servizi di trattamento, con l'effetto di garantire mediante trattamenti sicuri i diritti e le libertà fondamentali dell'interessato.

La sicurezza del DGA riguarda invece il più ampio ambiente di trattamento che in parte implica l'obbligo di garantire una sicurezza che coincide con alcuni obblighi dell'articolo 32 del GDPR (ad esempio: la garanzia di integrità e accessibilità dell'ambiente di trattamento), per altro verso **va oltre il perimetro stabilito dal GDPR, includendo nel concetto di sicurezza anche quello di ampia *compliance* e conformità a svariate normative** (assicurare i diritti degli interessati, rispettare i diritti di proprietà intellettuale; rispettare la riservatezza – meglio sarebbe stato riferirsi al "segreto" commerciale - e statistica, etc).

I PRINCIPALI CONCETTI GIURIDICI DEL DATA GOVERNANCE ACT

Le **definizioni soggettive** di *titolare dei dati, utente dei dati, fornitore del servizio di intermediazione dei dati*, etc che sono state prima indicate implicano considerazioni di un certo interesse.

Ad esempio, la definizione di “titolare dei dati” esprime un concetto di “titolarità” **assai differente** da quella che ritroviamo nel GDPR.

Il Regolamento Generale sulla protezione dei dati, difatti, lega la titolarità al trattamento e non ai dati e individua la fonte e il presupposto della titolarità al potere (legale, da contratto, di fatto, etc) del Titolare di prendere le decisioni su finalità, modalità, mezzi essenziali e misure di sicurezza del trattamento.

Al contrario, **la titolarità del DGA è legata ai dati in quanto tali (sia personali che non personali, tra l’altro)** e al **potere del titolare dei dati** non di prendere decisioni ma di **concedere l'accesso** a determinati dati personali o dati non personali o di **condividerli,** conformemente al diritto dell'Unione o nazionale applicabile.

FIVERS

I PRINCIPALI CONCETTI GIURIDICI DEL DATA GOVERNANCE ACT

Tra l'altro, il **DGA qualifica e definisce in modo peculiare il concetto di *accesso ai dati*, avvicinando molto tale concetto a quello di *trattamento***, se è vero che la definizione insiste su una delle forme di trattamento come definito dal GDPR: **l'utilizzo dei dati**.

L'articolo 2(13) DGA definisce difatti come segue l'"***accesso***": **l'utilizzo dei dati**, conformemente a specifici requisiti tecnici, giuridici o organizzativi, che non implica necessariamente la trasmissione o lo scaricamento di dati. L'accesso è inoltre qualificato dal Legislatore come specifico utilizzo, sulla base – cioè - di particolari requisiti o tecnici o giuridici o organizzativi, senza dover implicare necessariamente talune operazioni che invece nel "mondo" GDPR sono un vero e proprio trattamento, come la trasmissione o il download dei dati.

I PRINCIPALI CONCETTI GIURIDICI DEL DATA GOVERNANCE ACT

Continuando l'analisi delle definizioni soggettive del DGA, l'articolo 2, nn. 17-19 qualifica tutta una serie di soggetti, enti, organismi e imprese del comparto pubblicistico.

Gli **enti pubblici** sono:

1. le autorità statali;
2. le autorità regionali;
3. le autorità locali;
4. gli organismi di diritto pubblico, purché dotati di personalità giuridica; istituiti per soddisfare specificatamente bisogni d'interesse generale; **privi di carattere industriale o commerciale** e **composti, finanziati e monitorati** in modo maggioritario dallo Stato, da autorità regionali o locali o da altri organismi di diritto pubblico;
5. le associazioni formate da una o più delle sopra citate autorità od organismi di diritto pubblico.

Spetta agli enti pubblici consentire il riutilizzo di determinate categorie di dati e gli Stati Membri devono favorire le condizioni che spingano gli enti pubblici a creare e mettere a disposizione i dati in conformità del principio dell'**«apertura fin dalla progettazione e per impostazione predefinita»** di cui all'articolo 5, paragrafo 2, della direttiva (UE) 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (cfr. Considerando n. 9 DGA).

I PRINCIPALI CONCETTI GIURIDICI DEL DATA GOVERNANCE ACT

Il DGA definisce poi «**impresa pubblica**» qualsiasi impresa su cui gli enti pubblici possono esercitare, direttamente o indirettamente, un'influenza dominante perché ne sono proprietari, vi hanno una partecipazione finanziaria, o in virtù di norme che disciplinano l'impresa in questione; oppure perché tali enti, direttamente o indirettamente, detengono la maggioranza del capitale sottoscritto dall'impresa; controllano la maggioranza dei voti cui danno diritto le azioni emesse dall'impresa; possono designare più della metà dei membri dell'organo di amministrazione, di direzione o di vigilanza dell'impresa.

Tuttavia, i dati detenuti da imprese pubbliche come sopra definite non rientrano nell'ambito di applicazione del DGA, al pari dei dati detenuti da istituti culturali, quali biblioteche, archivi e musei, nonché orchestre, compagnie d'opera o di balletto e teatri, e da istituti di istruzione in quanto le opere e gli altri documenti in loro possesso sono prevalentemente coperti da diritti di proprietà intellettuale di terzi.

La residua applicabilità del DGA alle imprese pubbliche è legata alla facoltà che il DGA lascia agli Stati Membri di prevedere nella legislazione nazionale, se del caso, l'applicazione del DGA alle imprese pubbliche o private che **esercitano funzioni del settore pubblico o forniscono servizi di interesse generale**.

I PRINCIPALI CONCETTI GIURIDICI DEL DATA GOVERNANCE ACT

Centrali, poi, appaiono essere le **definizioni oggettive**, a partire da quella di "***dati***".

Come detto, i "dati" sono definiti dal DGA come "*qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva*".

Come detto più sopra, tale ampia definizione potrebbe essere letta come inclusiva anche della definizione di "*dati personali"* di cui al GDPR come della definizione – soprattutto – di "dati non personali" ai sensi del Regolamento 1807/2018.

Tuttavia, nel DGA, i dati sono:

a) o l'esito di un processo di rappresentazione digitale avente ad oggetto atti, fatti o informazioni (nel senso che il dato è la rappresentazione digitale finale di un fatto evento della vita, di un atto o di informazioni) e la prima parte di tale definizione sembra difficilmente includere – tra gli altri – anche i dati personali;

b) o una qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva; e allora più facilmente tale parte della definizione si presta ad includere i dati personali (si pensi alla raccolta mediante registrazione sonora, visiva o audiovisiva di fatti o eventi che riguardano persone identificate o identificabili le cui voci o immagini senza dubbio rientrano nella categoria dei "dati personali").

I PRINCIPALI CONCETTI GIURIDICI DEL DATA GOVERNANCE ACT

Tuttavia, è anche vero che il legislatore del DGA, fornisce e utilizza nel testo - separatamente e specificatamente - le tre diverse definizioni di *"dati", "dati personali" e "dati non personali",* il che farebbe pensare ad una autonomia definitoria e separata di ciascuna delle tre categorie di giuridiche. **Ad ogni buon conto, possiamo fornire i seguenti esempi chiarificatori di categorie di informazioni che rientrano nelle tre definizioni**.

Il **dato personale** disciplinato dal GDPR è ovviamente qualsiasi informazione riguardante una persona fisica identificata o identificabile, direttamente o indirettamente, mediante il nome, un numero di identificazione, la sua ubicazione, un identificativo online, uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Il **dato non personale** – che il Regolamento 2018/1807 definisce come detto in negativo (essendo tale il dato – **tra l'altro solo in formato elettronico**, cfr. art. 2, comma 1, del reg. 2018/1807) - che non è personale) – fa riferimento soprattutto alle **informazioni generate da processi industriali e automatizzati di produzione** (tipicamente, l'Internet of Things - IoT e la sua versione avanzata dell'Industrial Internet of Things o IIoT, e l'operatività di sistemi di Intelligenza Artificiale rappresentano tipiche fonti di dati non personali). Fra gli esempi specifici di dati non personali figurano gli insiemi di dati aggregati e anonimizzati usati per l'analisi dei metadati, i dati sull'agricoltura di precisione che possono contribuire a monitorare e ottimizzare l'uso di pesticidi e acqua, o i dati sulle esigenze di manutenzione delle macchine industriali. A stretto rigore definitorio e formale, anche **i dati in formato elettronico sulle persone giuridiche dovrebbero rientrare nella definizione di dato non personale**.

I nuovi servizi di «intermediazione dei dati» introdotti dal Data Governance Act: aspetti pratici e opportunità.

FIVERS

I NUOVI SERVIZI DI «INTERMEDIAZIONE DEI DATI» INTRODOTTI DAL DATA GOVERNANCE ACT: ASPETTI PRATICI E OPPORTUNITÀ.

Occorre partire dalla analisi delle due definizioni che fanno **riferimento al cuore delle attività e dei (nuovi) servizi regolamentati dal DGA**: il *data sharing* e i *servizi di intermediazione dei dati*.

La prima definizione è quella di «***condivisione dei dati***», definita come la fornitura di dati da un interessato (e qui ci si riferisce a dati personali, stante la definizione di interessato che è la stessa del GDPR) o da un titolare dei dati a un utente dei dati ai fini dell'utilizzo congiunto (tra utente, titolare dei dati e interessato) o individuale (da parte del solo utente che li riceve) di tali dati, sulla base di accordi volontari o del diritto dell'Unione o nazionale (che sono i presupposti contrattuali o legali della condivisione), direttamente o tramite un intermediario (quest'ultimo fornitore del relativo servizio come in appresso definito), ad esempio nel quadro di **licenze aperte o commerciali, dietro compenso o a titolo gratuito.**

L'articolo 2(11) del DGA definisce poi il «***servizio di intermediazione dei dati***»: un servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, **rapporti commerciali** ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali.

I NUOVI SERVIZI DI «INTERMEDIAZIONE DEI DATI» INTRODOTTI DAL DATA GOVERNANCE ACT: ASPETTI PRATICI E OPPORTUNITÀ.

E' evidente come il cuore della definizione risulti essere **l'obiettivo della instaurazione** – mediante il nuovo servizio su mercati digitali – di **rapporti commerciali ai fini della condivisione dei dati**.

Il nuovo servizio di intermediazione volto alla condivisione dei dati è reso possibile attraverso **strumenti diversi: tecnici, giuridici o di altro tipo**. E la intermediazione volta al *data sharing* vede il fornitore del servizio di intermediazione dei dati interelazionarsi e intermediare fra un numero indeterminato di offerenti/fornitori di dati personali e/o non personali (l'interessato e il titolare dei dati) e le persone fisiche o giuridiche cui è concesso accesso legittimo ai dati per il loro utilizzo a scopi sia commerciali che non commerciali (gli "utenti dei dati").

Non rientrano nella definizione di «servizio di intermediazione dei dati»:

a) i servizi che ottengono dati dai titolari dei dati e li **aggregano, arricchiscono o trasformano** al fine di aggiungervi un valore sostanziale e concedono licenze per l'utilizzo dei dati risultanti agli utenti dei dati, senza instaurare un rapporto commerciale tra i titolari dei dati e gli utenti dei dati (il che conferma che l'instaurazione del rapporto commerciale tra titolari/interessati e utenti dei dati è ciò che qualifica il servizio);

b) servizi il cui obiettivo principale è **l'intermediazione di contenuti protetti da diritto d'autore** (che non sono "dati");

I NUOVI SERVIZI DI «INTERMEDIAZIONE DEI DATI» INTRODOTTI DAL DATA GOVERNANCE ACT: ASPETTI PRATICI E OPPORTUNITÀ.

c) servizi **utilizzati esclusivamente da un titolare dei dati per consentire l'utilizzo dei dati detenuti da tale titolare dei dati,** oppure utilizzati da varie persone giuridiche all'interno di un gruppo chiuso, anche nel quadro di rapporti con i fornitori o i clienti o di collaborazioni contrattualmente stabilite, in particolare quelli aventi come obiettivo principale quello di garantire **la funzionalità di oggetti o dispositivi connessi all'internet delle cose**;

d) servizi di **condivisione dei dati offerti da enti pubblici che non mirano a instaurare rapporti commerciali**.

I NUOVI SERVIZI DI «INTERMEDIAZIONE DEI DATI» INTRODOTTI DAL DATA GOVERNANCE ACT: ASPETTI PRATICI E OPPORTUNITÀ.

Quanto il legislatore europeo ritenga centrale la diffusione dei servizi di intermediazione dei dati per lo sviluppo dell'Economia dei Dati, dei nuovi servizi digitali e degli Spazi Comuni europei dei Dati (il primo dei quali, lo Spazio europeo dei dati sanitari – European Health Data Space – è stato già lanciato a Maggio 2022 dalla Commissione UE) è dimostrato chiaramente dal **Considerando 27 del DGA**, che proprio per questo merita riportare:

*I servizi di intermediazione dei dati specializzati, che sono indipendenti dagli interessati, dai titolari dei dati e dagli utenti dei dati, **potrebbero facilitare l'emergere di nuovi ecosistemi basati sui dati, indipendenti da qualsiasi operatore che detenga un grado significativo di potere di mercato**, prevedendo nel contempo un accesso **non discriminatorio** all'economia dei dati per **le imprese di tutte le dimensioni, in particolare le PMI e le start-up con mezzi finanziari, giuridici o amministrativi limitati**. Ciò sarà particolarmente importante nel contesto della creazione di spazi comuni europei di dati, ossia quadri interoperabili specifici o settoriali o intersettoriali di norme e prassi comuni per condividere o trattare congiuntamente i dati, anche ai fini **dello sviluppo di nuovi prodotti e servizi,** della ricerca scientifica o di iniziative della società civile. I servizi di intermediazione dei dati potrebbero includere la condivisione bilaterale o multilaterale dei dati o **la creazione di piattaforme o banche dati che consentano la condivisione o l'utilizzo congiunto dei dati, nonché l'istituzione di un'infrastruttura specifica per l'interconnessione di interessati e titolari dei dati con gli utenti dei dati".***

FIVERS

I NUOVI SERVIZI DI «INTERMEDIAZIONE DEI DATI» INTRODOTTI DAL DATA GOVERNANCE ACT: ASPETTI PRATICI E OPPORTUNITÀ.

Va preliminarmente premesso che ciò che connota un servizio di intermediazione dei dati e l'attività del relativo fornitore è la **finalità di instaurare un rapporto commerciale** tra le parti intermediate, e cioè i titolari dei dati e gli utenti dei dati consentendo al fornitore di acquisire informazioni in merito all'instaurazione del rapporto commerciale ai fini della condivisione dei dati.

Tra gli esempi di servizi di intermediazione dei dati figurano i seguenti:

Servizi di analisi dei dati per il marketing: un intermediario di dati può raccogliere e analizzare dati di comportamento dei consumatori da vari negozi online e fornire report dettagliati alle aziende per ottimizzare le loro strategie di marketing. Ad esempio, un'azienda di e-commerce può utilizzare questi dati per personalizzare le offerte e migliorare l'esperienza del cliente;

Marketplace di dati aziendali: un'azienda può utilizzare un intermediario di dati per condividere informazioni di produzione con i suoi fornitori e partner commerciali. Ad esempio, un produttore di automobili può condividere dati sulle prestazioni dei componenti con i fornitori per migliorare la qualità e l'efficienza della produzione.

I NUOVI SERVIZI DI «INTERMEDIAZIONE DEI DATI» INTRODOTTI DAL DATA GOVERNANCE ACT: ASPETTI PRATICI E OPPORTUNITÀ.

Servizi di intermediazione dei dati per le smart city: Un intermediario di dati può facilitare la condivisione di dati tra diverse entità all'interno di una smart city, come i dati sul traffico, l'energia e l'ambiente. Ad esempio, i dati raccolti dai sensori di traffico possono essere condivisi con le autorità cittadine per migliorare la gestione del traffico e ridurre l'inquinamento.

Piattaforme di condivisione dei dati sanitari: Un intermediario di dati può facilitare la condivisione di dati sanitari tra ospedali, cliniche e istituti di ricerca. Ad esempio, una piattaforma può raccogliere dati anonimi sui pazienti da vari ospedali e renderli disponibili ai ricercatori per studi epidemiologici, garantendo la privacy e la sicurezza dei dati.

Piattaforme di gestione dei dati agricoli: Gli agricoltori possono utilizzare un intermediario di dati per condividere informazioni sulle colture, le condizioni meteorologiche e le pratiche agricole con altre aziende agricole e istituti di ricerca. Questo può aiutare a migliorare la produttività e la sostenibilità delle pratiche agricole.

I NUOVI SERVIZI DI «INTERMEDIAZIONE DEI DATI» INTRODOTTI DAL DATA GOVERNANCE ACT: ASPETTI PRATICI E OPPORTUNITÀ.

Quali tipologie di servizi di intermediazione dei dati sono contemplate e regolate dal Data Governance Act?

Il DGA distingue **tre diverse tipologie di servizi di intermediazione**.

La **prima tipologia** è rappresentata dai **servizi di intermediazione tra i titolari dei dati e i potenziali utenti dei dati**. Si ricordi che il "titolare dei dati" è la persona fisica o giuridica, compresi gli enti pubblici e le organizzazioni internazionali, che ha il diritto di concedere l'accesso a determinati dati personali o dati non personali o di condividerli. Mentre l' "utente dei dati" è la persona fisica o giuridica che ha accesso legittimo a determinati dati personali o non personali e ha diritto a utilizzare tali dati a fini commerciali o non commerciali.

La prima tipologia di servizio di intermediazione tra i titolari dei dati e i potenziali utenti vede dunque l'intermediazione del fornitore del servizio volta a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, **rapporti commerciali tra titolari dei dati e utenti**. Il fornitore mette inoltre a **disposizione i mezzi tecnici o di altro tipo** per consentire il servizio, il quale si connota anche per la possibilità di includere **scambi di dati bilaterali o multilaterali** o la **creazione da parte del fornitore di piattaforme o banche dati** che consentono lo scambio o l'utilizzo congiunto dei dati. Altra caratteristica tecnica del servizio può essere **l'istituzione di infrastrutture specifiche per l'interconnessione di titolari dei dati con gli utenti dei dati.**

I NUOVI SERVIZI DI «INTERMEDIAZIONE DEI DATI» INTRODOTTI DAL DATA GOVERNANCE ACT: ASPETTI PRATICI E OPPORTUNITÀ.

La **seconda tipologia** è rappresentata dai servizi di intermediazione tra interessati che intendono mettere a disposizione i propri dati personali o persone fisiche che intendono mettere a disposizione dati non personali e potenziali utenti dei dati. Il fornitore mette a disposizione degli interessati (le sole persone fisiche) che gestiscono i loro dati personali (o non personali) **i mezzi tecnici o di altro tipo per consentire l'accesso degli utenti**.

E' molto interessante notare come il **Considerando n. 30** specifichi che "*una categoria specifica di fornitori di servizi di intermediazione dei dati comprende i fornitori che offrono i loro servizi agli interessati. Tali fornitori di servizi di intermediazione dei dati* ***cercano di rafforzare la capacità di agire degli interessati*** *e, in particolare,* ***il controllo*** *dei singoli individui in merito ai dati che li riguardano*".

In sostanza, il fornitore di servizi di intermediazione di questo tipo (tutti sostanzialmente riferiti alla gestione di dati personali ai sensi del GDPR) potenzia il **nucleo centrale** del diritto alla protezione dei dati personali (cioè il **potere di controllo** sulle proprie informazioni personali) rafforzando – mentre rende il servizio – la posizione del soggetto giuridico che di quei dati è – in veste di interessato – *l'owner.* Anche per questo una particolare attenzione nella resa di questo servizio di intermediazione è dedicata all'assistenza agli interessati nell'esercizio dei loro diritti data protection come previsti agli articoli da 15 a 22 del GDPR.

I NUOVI SERVIZI DI «INTERMEDIAZIONE DEI DATI» INTRODOTTI DAL DATA GOVERNANCE ACT: ASPETTI PRATICI E OPPORTUNITÀ.

I fornitori di servizi di intermediazione dei dati che rientrano in questa seconda tipologia assurgono al ruolo di veri e **propri consulenti o tutor data protection** nei confronti degli interessati (devono dunque essere entità che – al di là degli scopi di profitto commerciale nella resa del servizio - offrono **competenze specialistiche *data protection* adatte** per supportare gli interessati, aprendosi dunque ulteriori possibilità di mercato per le professionalità del comparto *data protection*).

In tale contesto, il Considerando 30 DGA sottolinea l'importanza che il **modello commerciale** di tali fornitori garantisca che non vi siano **incentivi disallineati** che incoraggino i singoli individui a utilizzare tali servizi per **mettere a disposizione più dati** che li riguardano di quanto non sia nel loro stesso interesse. In tale modello commerciale dovrebbe per esempio essere inclusa una **specifica offerta di consulenza ai singoli individui quanto ai possibili utilizzi dei loro dati e il controllo della dovuta diligenza degli utenti dei dati prima che sia consentito loro di contattare gli interessati,** al fine di evitare pratiche fraudolente.

I NUOVI SERVIZI DI «INTERMEDIAZIONE DEI DATI» INTRODOTTI DAL DATA GOVERNANCE ACT: ASPETTI PRATICI E OPPORTUNITÀ.

La **terza tipologia** è quella dei **servizi di cooperative di dati** e cioè servizi di intermediazione dei dati offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno **scambio di opinioni sulle finalità e sulle condizioni** del trattamento dei dati che **rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali**.

Come si diventa fornitore del servizio di intermediazione dei dati? La procedura di notifica dei servizi di «intermediazione dei dati».

FIVERS

LA NOTIFICA DEI SERVIZI DI «INTERMEDIAZIONE DEI DATI».

I servizi di intermediazione dei dati, **per poter essere forniti nel territorio della UE**, devono essere previamente **oggetto di una specifica procedura di notifica** da inoltrare **all'autorità competente**: per l'Italia tale autorità, come abbiamo visto, **è l'AgID**, individuata dal decreto legislativo 144/2024.

L'articolo **11 DGA** stabilisce una articolata disciplina della procedura di notifica, all'esito della quale si ottiene **una autorizzazione a prestare i servizi di intermediazione dei dati in tutti gli Stati Membri**, potendo il fornitore utilizzare il titolo di «*fornitore di servizi di intermediazione dei dati riconosciuto nell'Unione*» nelle sue comunicazioni scritte e orali, nonché un logo comune).

La notifica contiene le informazioni seguenti:

a) il nome del fornitore di servizi di intermediazione dei dati;

b) lo status giuridico, la forma giuridica, l'assetto proprietario, le pertinenti società controllate e, qualora il fornitore di servizi di intermediazione dei dati sia registrato nel registro delle imprese o in un altro registro pubblico nazionale analogo, il numero di registrazione del fornitore di servizi di intermediazione dei dati;

c) l'indirizzo **dell'eventuale stabilimento principale** del fornitore di servizi di intermediazione dei dati nell'Unione e, se opportuno, di eventuali **sedi secondarie** in un altro Stato membro o l'indirizzo del rappresentante legale;

LA NOTIFICA DEI SERVIZI DI «INTERMEDIAZIONE DEI DATI».

Art. 2(14) DGA: «stabilimento principale» di una persona giuridica: il luogo in cui è stabilita la sua amministrazione centrale nell'Unione.

Considerando 41 DGA: «*Lo stabilimento principale di un fornitore di servizi di intermediazione dei dati nell'Unione dovrebbe essere ove ha sede l'amministrazione centrale del fornitore nell'Unione in cui, in base a criteri oggettivi, si determina l'effettivo e reale svolgimento di attività di gestione*».

d) un **sito web pubblico** in cui sono reperibili informazioni complete e aggiornate sul fornitore di servizi di intermediazione dei dati e sulle sue attività, comprese almeno le informazioni di cui alle lettere a), b), c) e f);

e) le **persone di contatto e i recapiti** del fornitore di servizi di intermediazione dei dati;

f) una descrizione del servizio di intermediazione dei dati che il fornitore di servizi di intermediazione dei dati intende fornire e un'indicazione delle categorie elencate all'articolo 10 in cui rientra tale servizio di intermediazione dei dati;

g) la data prevista di inizio dell'attività, se diversa dalla data della notifica.

LA NOTIFICA DEI SERVIZI DI «INTERMEDIAZIONE DEI DATI».

Su richiesta del fornitore di servizi di intermediazione dei dati, l'autorità competente per i servizi di intermediazione dei dati:

- rilascia, entro una settimana dalla notifica debitamente e interamente completata, una dichiarazione standardizzata in cui conferma che il fornitore di servizi di intermediazione dei dati ha presentato la notifica e che la notifica contiene tutte le informazioni richieste;

- conferma, che il fornitore di servizi di intermediazione dei dati è conforme alle disposizioni sulla notifica e sulla prestazione dei servizi di intermediazione;

Una volta ricevuta detta conferma, il fornitore di servizi di intermediazione dei dati in questione può utilizzare il titolo **«fornitore di servizi di intermediazione dei dati riconosciuto nell'Unione»** nelle sue comunicazioni scritte e orali, nonché un logo comune.

Le notifiche alimentano **un registro UE dei fornitori dei servizi di intermediazione dei dati**, istituito e gestito dalla Commissione. Ai fini dell'aggiornamento di tale registro, nel caso di **cessazione dell'attività** il fornitore deve notificare entro 15 giorni all'autorità competente.

Per la notifica possono essere previste a applicate **tariffe**.

I requisiti e le condizioni per la fornitura dei servizi di «intermediazione dei dati».

FIVERS

I REQUISITI E LE CONDIZIONI PER LA FORNITURA DEI SERVIZI DI «INTERMEDIAZIONE DEI DATI».

Al fine di far crescere la fiducia e **sviluppare il mercato europeo dei servizi di intermediazione dei dati**, l'articolo 12 del DGA introduce regole armonizzate a livello europeo (che potranno essere ulteriormente potenziate e coordinate – per esempio in materia di interoperabilità di dati e servizi - mediante l'adozione di **specifici codici di condotta** europei, adottati con la supervisione della Commissione UE), al fine di garantire che gli interessati nonché i titolari e gli utenti dei dati abbiano un maggiore controllo sull'accesso ai dati e sul loro utilizzo.

Quanto ai **requisiti e alle condizioni per offrire i servizi di intermediazione dei dati**, assume particolare rilevanza l'interesse dichiarato dal legislatore europeo di **introdurre un modalità nuova, definita esplicitamente «europea», di governance dei dati**, con i fornitori che - sia in situazioni in cui la condivisione di dati avviene tra due imprese sia quando ha luogo tra impresa e consumatore – devono garantire una **separazione tra fornitura, intermediazione e utilizzo dei dati.**

Questa scelta di politica legislativa - commerciale e *corporate* - viene codificata all'articolo 12, comma 1, lettera (a) DGA che prevede – onde evitare conflitti di interesse - **una separazione strutturale tra il servizio di intermediazione dei dati e qualsiasi altro servizio fornito**: il servizio di intermediazione dei dati deve difatti essere fornito mediante una **persona giuridica distinta dalle altre attività prestate** dal medesimo fornitore di servizi di intermediazione dei dati.

I REQUISITI E LE CONDIZIONI PER LA FORNITURA DEI SERVIZI DI «INTERMEDIAZIONE DEI DATI».

Per la stessa finalità di evitare conflitti di interesse o comunque situazioni di violazione delle norme sulla concorrenza, i fornitori dei servizi di intermediazione dei dati **non possono inserire nelle condizioni contrattuali e commerciali** specifiche del servizio di intermediazione (che devono essere eque, trasparenti e non discriminatorie) **clausole che subordinano la fornitura del servizio alla circostanza che il titolare dei dati o l'utente dei dati utilizzino altri servizi forniti dallo stesso fornitore o da un'entità collegata** (per esempio: cloud, l'archiviazione dei dati, l'analisi, l'intelligenza artificiale o altre applicazioni basate sui dati).

Se il titolare dei dati o l'utente dei dati utilizzano già altri servizi del medesimo fornitore, le condizioni commerciali devono specificare in che misura i titolari dei dati o gli utenti utilizzano tali diversi servizi.

Alcune condizioni, poi, identificano il perimetro delle **attività consentite oppure vietate** al fornitore sui dati oggetto del servizio di intermediazione. Ad esempio, il fornitore:

I REQUISITI E LE CONDIZIONI PER LA FORNITURA DEI SERVIZI DI «INTERMEDIAZIONE DEI DATI».

1. **non può utilizzare i dati** per i quali fornisce servizi di intermediazione dei dati per scopi diversi dalla loro messa a disposizione agli utenti dei dati (principio cosiddetto della "*neutralità del fornitore dei servizi di intermediazione dei dati*", volto a favorire la costruzione di un ambiente competitivo);
2. può **adattare i dati scambiati**, ad esempio convertendoli in formati specifici, per migliorarne l'usabilità per l'utente o l'interoperabilità;
3. può – ma solo su richiesta o approvazione esplicita del titolare dei dati o dell'interessato – **utilizzare i dati per fornire servizi o strumenti accessori specifici per facilitare lo scambio dei dati**, come ad esempio la conservazione temporanea, la cura, la conversione, l'anonimizzazione e la pseudonimizzazione dei dati, impegnandosi tuttavia a non utilizzare i dati oggetto di tali servizi o strumenti supplementari per altri scopi;
4. può utilizzare i dati forniti dal titolare dei dati per migliorare i suoi servizi di intermediazione dei dati;

I REQUISITI E LE CONDIZIONI PER LA FORNITURA DEI SERVIZI DI «INTERMEDIAZIONE DEI DATI».

5. **può utilizzare i dati raccolti su qualsiasi attività di una persona fisica o giuridica** ai fini della fornitura del servizio di intermediazione (come ad esempio la data, l'ora e i dati di geolocalizzazione, la durata dell'attività e i collegamenti con altre persone fisiche o giuridiche stabiliti dalla persona che utilizza il servizio di intermediazione dei dati) **per l'individuazione di frodi o a fini di cybersicurezza** (mettendoli a disposizione dei titolari dei dati, su richiesta);

6.deve tenere un **registro specifico** delle attività di intermediazione dei dati.

I REQUISITI E LE CONDIZIONI PER LA FORNITURA DEI SERVIZI DI «INTERMEDIAZIONE DEI DATI».

I requisiti tecnici e le condizioni di sicurezza come presupposto per la fornitura del servizio di intermediazione dei dati.

Alcune condizioni del servizio di intermediazione dei dati sono poi eminentemente tecniche, come ad esempio la necessità che il fornitore – mediante la conversione in specifici formati dei dati così come ricevuti dal titolare dei dati o dall'interessato – **favorisca l'interoperabilità con altri servizi di intermediazione dei dati, all'interno di un settore e tra settori diversi** (l'interoperabilità deve essere o richiesta dall'utente dei dati o prescritta dal diritto dell'Unione o da norme di armonizzazione con le norme internazionali o europee in materia di dati).

E' una condizione tecnica anche l'obbligo di adottare le misure necessarie per garantire un **adeguato livello di sicurezza per la conservazione, il trattamento e la trasmissione di dati non personali.**

Infine, specifiche procedure tecniche devono essere predisposte da parte del fornitore per prevenire pratiche fraudolente o abusive in relazione a soggetti che richiedono l'accesso tramite i suoi servizi di intermediazione dei dati. A queste procedure tecniche si affianca an-che l'obbligo di **predisporre misure contrattuali che prevedono sanzioni in caso di tentativi di accesso o utilizzo abusivo dei dati**.

I REQUISITI E LE CONDIZIONI PER LA FORNITURA DEI SERVIZI DI «INTERMEDIAZIONE DEI DATI».

L’articolo 12, lettera (j) DGA prescrive poi al fornitore dei servizi di intermediazione dei dati di adottare “*adeguate misure tecniche, giuridiche e organizzative*” al fine di impedire il trasferimento di **dati non personali** o l'accesso a questi ultimi nel caso in cui **ciò sia illegale** a norma del diritto dell'Unione o del diritto nazionale dello Stato membro interessato (tra tali misure vi è anche l’obbligo di informare tempestivamente i titolari dei dati in caso di trasferimento, accesso o utilizzo illegale dei dati non personali).

Le condizioni di conformità al diritto della concorrenza come presupposto per la fornitura del servizio di intermediazione dei dati.

Altre procedure devono essere adottate – quale requisito per poter fornire i servizi di inter-mediazione dei dati – per garantire il rispetto del diritto della concorrenza. Ad esempio, vi possono essere **situazioni in cui la condivisione dei dati consente alle imprese di venire a conoscenza delle strategie di mercato dei loro concorrenti** effettivi o potenziali o di informazioni sensibili sotto il profilo della concorrenza come le **informazioni su dati dei clienti, prezzi futuri, costi di produzione, quantità, fatturato, vendite o capacità**.

I REQUISITI E LE CONDIZIONI PER LA FORNITURA DEI SERVIZI DI «INTERMEDIAZIONE DEI DATI».

Il DGA, allora, per impedire violazioni (volute o meno) del diritto alla concorrenza e dei diritti di proprietà industriale (come il know-how) o intellettuale prescrive al fornitore del servizio di intermediazione dei dati di dotarsi di adeguate procedure ad hoc, obbligandolo inoltre – anche sotto il profilo più tecnico – ad assicurare "***il massimo livello di sicurezza per la conservazione e la trasmissione di informazioni sensibili sotto il profilo della concorrenza***"[cfr. art. 12, lettera (l) DGA].

Tutta una serie di **condizioni** per la resa dei servizi di intermediazione dei dati sono poi specifiche quando viene in considerazione la **natura personale dei dati oggetto del servizio**. In tale prospettiva - e come prerequisito generale – il Considerando 35 DGA prevede che "*Il presente regolamento dovrebbe lasciare impregiudicati l'obbligo incombente ai fornitori di servizi di intermediazione dei dati di rispettare il Regolamento (UE) 2016/679 e la responsabilità delle autorità di controllo di garantire il rispetto di tale regolamento. Qualora i fornitori di servizi di intermediazione dei dati trattino dati personali, il presente regolamento non dovrebbe pregiudicare la protezione degli stessi. Qualora siano titolari del trattamento o responsabili del trattamento dei dati quali definiti nel regolamento (UE) 2016/679, i fornitori di servizi di intermediazione dei dati sono vincolati dalle norme di tale regolam*ento".

I REQUISITI E LE CONDIZIONI PER LA FORNITURA DEI SERVIZI DI «INTERMEDIAZIONE DEI DATI».

Il Considerando 33 DGA prevede poi che i fornitori di servizi di intermediazione dei dati, quando agiscono da intermediari tra singoli individui interessati e le persone giuridiche dovrebbero inoltre avere **l'obbligo fiduciario nei confronti degli interessati di garantire che agiscono nel loro migliore interesse**. Tale indirizzo è specificatamente codificato dall'articolo 12, lettera (m) DGA allorché prescrive che il fornitore di servizi di intermediazione dei dati che offre servizi agli interessati agisce "***nell'interesse superiore di questi ultimi***", facilitando l'esercizio dei loro diritti, **in particolare informandoli** e, se opportuno, fornendo loro **consulenza** in maniera concisa, trasparente, intelligibile e facilmente accessibile **sugli utilizzi previsti dei loro dati personali da parte degli utenti** dei dati e **sui termini e le condizioni** standard cui sono subordinati tali utilizzi, prima che gli interessati diano il loro consenso.

Il DGA aggiunge dunque – agli ordinari obblighi informativi del GDPR – **un diverso e ulteriore obbligo informativo**, specificatamente qualificato dalla norma.

Così come un altro specifico obbligo informativo prevede che qualora un fornitore di servizi di intermediazione dei dati **fornisca strumenti per ottenere il consenso degli interessati** esso **dovrà specificare** – "*se del caso*" - **la giurisdizione del paese terzo in cui l'utente tratterà/utilizzerà o dati personali** e fornisce agli interessati gli strumenti per dare e revocare il consenso (stesso meccanismo è previsto – specularmente – in caso di dati non personali).

Gli obblighi per i fornitori di servizi di intermediazione dei dati che non hanno il loro stabilimento principale nella UE ma offrono i servizi nella UE.

FIVERS

FORNITORI DEI SERVIZI DI «INTERMEDIAZIONE DEI DATI» CON SEDE EXTRA-UE.

Il Data Governance Act mutua integralmente dal GDPR i meccanismi di applicabilità territoriale – diciamo transnazionale e indipendente dal luogo di stabilimento del fornitore – delle norme sulla fornitura di servizi di intermediazione dei dati. E' un altro esempio di come il GDPR si continui a porre quale modello e paradigma di riferimento, tanto che i meccanismi normativi a tutela dei dati personali sono traslati e ora applicati anche ai dati non personali.

Il DGA prescrive che i fornitori di servizi di intermediazione dei dati devono avere il loro **stabilimento principale** [non la sede legale, ma il luogo in cui è stabilita l'effettiva amministrazione centrale, cfr. art. 2(14) DGA] nell'Unione.

Qualora un fornitore di servizi di intermediazione dei dati non stabilito nell'Unione offra ser-vizi nell'Unione, esso **deve designare un rappresentante legale** (sono chiari gli echi dell'art. 27 del GDPR), vista la delicatezza dei servizi offerti, con la gestione sia di dati personali che di dati commerciali riservati. Il Legislatore europeo ritiene dunque necessario il controllo ravvicinato del rispetto del DGA da parte di fornitori di servizi extra UE che li offrono nel territorio della UE.

FORNITORI DEI SERVIZI DI «INTERMEDIAZIONE DEI DATI» CON SEDE EXTRA-UE.

Appare opportuno evidenziare che il radicamento in un certo Stato membro (vuoi perché un fornitore del servizio di intermediazione dei dati ha lì il proprio stabilimento principale, vuoi perché in quello Stato Membro si trova il rappresentate legale designato del fornitore extra UE) non ha comportato – come forse sarebbe stato opportuno – la replica del meccanismo introdotto dal GDPR dell'"*one-stop-shop*".

Come è noto, tale principio stabilisce i titolari del trattamento hanno a che fare con una sola Autorità di controllo, cioè quella del paese dove hanno la sede principale, piuttosto che con le autorità di 27 Stati europei. La decisione presa dall'autorità di controllo nazionale trova applicazione anche negli altri paesi dell'Unione. Invece, l'articolo 14(7) del DGA prevede che se lo stabilimento principale o il rappresentante legale di un fornitore di servizi di intermediazione dei dati si trova in uno Stato membro, ma tale fornitore presta servizi in altri Stati membri, l'autorità competente per i servizi di intermediazione dei dati dello Stato membro dello stabilimento principale o in cui si trova il rappresentante legale e le autorità competenti per i servizi di intermediazione dei dati di tali altri Stati membri collaborano e si prestano assistenza reciprocamente, avendo dunque ciascuna Autorità il potere autonomo e concorrente di agire verso il fornitore.

Obblighi per i fornitori di servizi di intermediazione dei dati in caso di richieste di autorità internazionali.

OBBLIGHI PER I FORNITORI DI SERVIZI DI INTERMEDIAZIONE DEI DATI IN CASO DI RICHIESTE DI AUTORITÀ INTERNAZIONALI.

Cosa deve fare un fornitore di servizi di intermediazione dei dati che riceva da una autorità pubblica internazionale una richiesta di trasferimento dei dati non personali o di accesso dall'esterno della UE a tali dati?

Il fornitore di servizi di intermediazione dei dati è tenuto ad adottare tutte le ragionevoli misure tecniche, giuridiche e organizzative, compresi accordi contrattuali, **per impedire** il **trasferimento internazionale di dati non personali** detenuti nell'Unione o l'accesso a questi ultimi **da parte delle autorità pubbliche** qualora tale trasferimento o accesso sia in conflitto con il diritto dell'Unione o il diritto nazionale dello Stato membro pertinente.

Nel caso di **decisioni o sentenze di un'autorità giurisdizionale di un paese terzo extra UE o di decisioni di un'autorità amministrativa del paese terzo che dispongono che il fornitore di servizi di intermediazione dei dati trasferisca dati non personali** detenuti nell'Unione o vi dia accesso, tali atti giurisdizionali o amministrativi sono riconosciuti o assumono qualsivoglia carattere esecutivo **soltanto se basati su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione europea** (es: un trattato di mutua assistenza giudiziaria).

OBBLIGHI PER I FORNITORI DI SERVIZI DI INTERMEDIAZIONE DEI DATI IN CASO DI RICHIESTE DI AUTORITÀ INTERNAZIONALI.

Se tale **accordo internazionale non esiste** e il rispetto della decisione giurisdizionale o amministrativa emessa nel paese terzo extra UE rischia di mettere il destinatario in conflitto con il diritto dell'Unione o con il diritto nazionale dello Stato membro pertinente, il trasferimento dei dati non personali richiesti o l'accesso agli stessi da parte dell'autorità pubblica internazionale possono avvenire solo se:

1. l'ordinamento giuridico del paese terzo prescrive che la decisione giudiziaria o amministrativa **sia motivata, proporzionata ed abbia un carattere specifico** (ad esempio: i dati non personali sono richiesti rispetto a determinate persone sospettate o a determinate violazioni commesse nel paese terzo);
2. il fornitore di servizi di intermediazione dei dati destinatario della richiesta di accesso o di trasferimento **possa motivatamene obiettare alla decisione e le sue obiezioni sono oggetto di esame da parte di un'autorità giurisdizionale** competente del paese terzo;
3. l'autorità giurisdizionale competente del paese terzo che emette la decisione o la sentenza o esamina la decisione di un'autorità amministrativa ha il potere, in virtù del diritto di tale paese terzo, di **tenere debitamente conto dei pertinenti interessi giuridici del fornitore dei dati tutelati** a norma del diritto dell'Unione o dal diritto nazionale del pertinente Stato membro.

OBBLIGHI PER I FORNITORI DI SERVIZI DI INTERMEDIAZIONE DEI DATI IN CASO DI RICHIESTE DI AUTORITÀ INTERNAZIONALI.

Resta fermo in ogni caso il duplice obbligo del fornitore di intermediazione dei dati che procede al trasferimento internazionale dei dati o che concede all'autorità pubblica internazionale l'accesso ai dati perché sono soddisfatte le condizioni che precedono (esiste cioè un accordo internazionale tra lo Stato terzo e la Ue oppure sono verificate e soddisfatte le condizioni nell'ordinamento giuridico del paese terzo appena sopra analizzate) di:

3. **informare il titolare dei dati** dell'esistenza di una richiesta di accesso ai suoi dati da parte dell'autorità amministrativa del paese terzo prima di soddisfare tale richiesta, salvi i casi in cui la richiesta abbia fini di contrasto e per il tempo necessario a preservare l'efficacia dell'attività di contrasto;
4. fornire sempre "*la quantità minima di dati ammissibile in risposta a una richiesta, sulla base di un'interpretazione ragionevole della richiesta*" (cfr. articolo 31 DGA).

I servizi «analoghi» ai servizi di intermediazione dei dati esclusi dall’ambito di applicazione del DGA.

I SERVIZI «ANALOGHI» AI SERVIZI DI INTERMEDIAZIONE DEI DATI ESCLUSI DALL'AMBITO DI APPLICAZIONE DEL DGA.

Non sono considerati *servizi di intermediazione dei dati* soggetti alla disciplina del Capo III del DGA **i servizi che non creano rapporti commerciali tra le parti intermediate**.

Dunque i seguenti servizi - che pure hanno **caratteristiche simili** a quelli invece regolati dal DGA – **non** sono considerati servizi di intermediazione dei dati:

a)servizi che ottengono dati dai titolari dei dati e li aggregano, arricchiscono o trasformano al fine di aggiungervi un valore sostanziale e concedono licenze per l'utilizzo dei dati risultanti agli utenti dei dati, senza instaurare un rapporto commerciale tra i titolari dei dati e gli utenti dei dati (in questo caso manca l'aspetto della "intermediazione");

b)servizi il cui obiettivo principale è **l'intermediazione di contenuti protetti da diritto d'autore** (in questo caso non si tratta di intermediazione avente ad oggetto dati);

I SERVIZI «ANALOGHI» AI SERVIZI DI INTERMEDIAZIONE DEI DATI ESCLUSI DALL'AMBITO DI APPLICAZIONE DEL DGA.

c) **servizi utilizzati esclusivamente da un titolare dei dati** per consentire l'utilizzo dei dati detenuti da tale titolare dei dati, oppure utilizzati da varie persone giuridiche all'interno di un gruppo chiuso, anche nel quadro di rapporti con i fornitori o i clienti o di collaborazioni contrattualmente stabilite, in particolare quelli aventi come obiettivo principale quello di garantire la funzionalità di oggetti o dispositivi connessi all'internet delle cose (in questo caso il servizio è utilizzato e gestito direttamente dal titolare dei dati, senza intermediazione);

d) servizi di **condivisione dei dati offerti da enti pubblici che non mirano a instaurare rapporti commerciali** (in questo caso manca il carattere "mercantile" del servizio);

e) servizi di intermediazione dei dati offerti **dalle organizzazioni per l'altruismo dei dati**, a condizione che tali servizi **non creino un rapporto commerciale** tra potenziali utenti dei dati, da un lato, e interessati e titolari dei dati che mettono a disposizione i dati per motivi altruistici, dall'altro;

I SERVIZI «ANALOGHI» AI SERVIZI DI INTERMEDIAZIONE DEI DATI ESCLUSI DALL'AMBITO DI APPLICAZIONE DEL DGA.

f) **servizi di archiviazione sul cloud, di analisi, di software per la condivisione dei dati, di web browser, di plug-in per browser o di un servizio di posta elettronica, a condizione che tali servizi si limitino alla messa a disposizione di strumenti tecnici per gli interessati o per i titolari dei dati ai fini della condivisione di dati con altri**;

g) **tutti gli altri servizi non finalizzati a instaurare rapporti commerciali**, come i repository volti a consentire il riutilizzo dei dati della ricerca scientifica conformemente ai principi dell'accesso aperto.

Le cooperative dei dati.

FIVERS

LE COOPERATIVE DEI DATI

Oltre a introdurre un nuovo servizio ai fini del data sharing, il **DGA dà vita ad un particolare soggetto giuridico** : la "**cooperativa dei dati**" e ad una particolare qualificazione del servizio di intermediazione dei dati (con la previsione dei «**servizi di cooperative di dati**»).
L'articolo 2(15) DGA così definisce i particolari servizi di intermediazione dei dati offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura (ciò che appunto qualifica le cooperative), avente come obiettivi principali quelli di:

- **aiutare** i propri membri **nell'esercizio dei loro diritti** in relazione a determinati dati;

- compiere **scelte informate** prima di acconsentire al trattamento dei dati;

- procedere a uno **scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati** che rappresentino al meglio gli interessi dei propri membri in relazione ai loro dati;

- **negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri** prima di concedere **l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali**.

LE COOPERATIVE DEI DATI

Le **cooperative di dati** sono un soggetto giuridico-economico nuovo e in prospettiva assai interessante negli scenari della *Value Data Economy,* dove assume sempre più centralità il **valore della consapevolezza circa i propri dati, personali o non personali**.

Come chiarito dal *Considerando* n. 31 del DGA, le cooperative di dati mirano a raggiungere una serie di obiettivi, in particolare a rafforzare la posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati, **influenzando i termini e le condizioni, stabiliti dalle organizzazioni di utenti dei dati**, cui è subordinato l'utilizzo dei dati, in modo da **offrire scelte migliori ai singoli membri** del gruppo, o trovando possibili soluzioni alle posizioni contrastanti dei singoli membri di un gruppo in merito alle modalità di utilizzo dei dati laddove tali dati riguardino più interessati all'interno di tale gruppo.

Le cooperative di dati rappresenteranno anche uno strumento utile per imprese individuali e PMI che, in termini di conoscenze in materia di condivisione dei dati, sono spesso equiparabili ai singoli individui.

Il regime di riutilizzo dei dati protetti detenuti da enti pubblici previsto dal DGA.

IL REGIME DI RIUTILIZZO DEI DATI PROTETTI DETENUTI DA ENTI PUBBLICI PREVISTO DAL DGA.

Il Capo II – articoli da 3 a 9 – del Regolamento 2022/868 sulla Governance europea dei dati si occupa di disciplinare **il riutilizzo di determinate categorie di dati detenuti dagli enti pubblici** (come sopra definiti), stabilendo:

a) quali categorie di dati sono oggetto di riutilizzo e quali dati sono invece esclusi;
b) quale specifica procedura occorre seguire per inoltrare agli enti pubblici una richiesta di riutilizzo e come gli enti pubblici devono procedere;
c) quali tariffe possono essere applicate dagli enti pubblici per il riutilizzo;
d) quali sono le condizioni per il riutilizzo;
e) il divieto di accordi in esclusiva;
f) la designazione a livello di Stati Membri di organismi competenti e di sportelli unici informativi;

e lasciando comunque impregiudicati gli accordi internazionali della UE o di singoli Stati membri eventualmente vigenti in merito alla protezione dei dati oggetto del DGA e – soprattutto – le leggi nazionali o UE che disciplinano il **diritto di accesso ai documenti** (che è anche accesso – mediato – ai dati).

IL REGIME DI RIUTILIZZO DEI DATI PROTETTI DETENUTI DA ENTI PUBBLICI PREVISTO DAL DGA.

Riutilizzare i dati significa l'insieme di condizioni legali, tecniche ed organizzative in base alle quali una persona fisica o giuridica ha accesso legittimo a qualsiasi rappresentazione digitale di atti, fatti o informazioni e a qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva **in possesso di enti pubblici** e **utilizza tali dati a fini commerciali o non commerciali**, purché gli **scopi differiscano** da quelli iniziali nell'ambito dei compiti di servizio pubblico per i quali i dati sono stati prodotti.

Il **regime di riutilizzo** si applica a dati la cui fornitura è parte dei compiti di servizio pubblico degli enti pubblici, ai sensi del diritto o di altre norme vincolanti negli Stati membri.

I dati detenuti da enti pubblici che possono essere oggetto di riutilizzo **devono essere "protetti"** per motivi di:

a) riservatezza commerciale, compresi i segreti commerciali, professionali o d'impresa;
b) riservatezza statistica;
c) protezione dei diritti di proprietà intellettuale di terzi; o
d) protezione dei dati personali, nella misura in cui tali dati non rientrano nell'ambito di applicazione della direttiva (UE) 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico.

IL REGIME DI RIUTILIZZO DEI DATI PROTETTI DETENUTI DA ENTI PUBBLICI PREVISTO DAL DGA.

Esempi di riutilizzo:

Sviluppo di nuove applicazioni e servizi per i cittadini: i dati detenuti da enti pubblici, come i dati demografici, i dati sanitari e i dati relativi alla mobilità, possono essere utilizzati per sviluppare nuove applicazioni e servizi per i cittadini. Ad esempio, i dati demografici possono essere utilizzati per sviluppare applicazioni per la pianificazione urbana, i dati sanitari possono essere utilizzati per sviluppare applicazioni per la prevenzione delle malattie e i dati relativi alla mobilità possono essere utilizzati per sviluppare applicazioni per la condivisione dei mezzi di trasporto.
Ricerca e sviluppo: i dati detenuti da enti pubblici possono essere utilizzati per la ricerca e lo sviluppo di nuove tecnologie e soluzioni. Ad esempio, i dati meteorologici possono essere utilizzati per sviluppare nuove tecnologie per la previsione del tempo, i dati ambientali possono essere utilizzati per sviluppare nuove tecnologie per la protezione dell'ambiente e i dati relativi al traffico possono essere utilizzati per sviluppare nuove tecnologie per la gestione del traffico.
Miglioramento dell'efficienza della Pubblica Amministrazione: i dati detenuti da enti pubblici possono essere utilizzati per migliorare l'efficienza della Pubblica Amministrazione. Ad esempio, i dati relativi alle spese pubbliche possono essere utilizzati per identificare le aree in cui è possibile ridurre le spese, i dati relativi ai servizi pubblici possono essere utilizzati per migliorare la qualità dei servizi e i dati relativi ai dipendenti pubblici possono essere utilizzati per migliorare la gestione del personale.

IL REGIME DI RIUTILIZZO DEI DATI PROTETTI DETENUTI DA ENTI PUBBLICI PREVISTO DAL DGA.

In Italia, il **Comune di Milano** ha lanciato un progetto per riutilizzare i dati detenuti dall'ente per sviluppare nuove applicazioni e servizi per i cittadini. Il progetto prevede la creazione di un *data lake*, un archivio centralizzato di dati, che sarà utilizzato per sviluppare applicazioni per la mobilità, la sicurezza e la salute.

Il progetto è stato avviato nel 2023 e prevede la raccolta di dati da diverse fonti, tra cui il sistema di videosorveglianza del Comune, il sistema di trasporto pubblico e il sistema sanitario. I dati raccolti saranno anonimizzati e aggregati per garantire la privacy degli interessati.

Il progetto è ancora in fase di sviluppo, ma ha già prodotto alcuni risultati. Ad esempio, è stata sviluppata una nuova applicazione per la mobilità che utilizza i dati del sistema di trasporto pubblico per fornire informazioni in tempo reale sui mezzi in arrivo.

IL REGIME DI RIUTILIZZO DEI DATI PROTETTI DETENUTI DA ENTI PUBBLICI PREVISTO DAL DGA

In **Francia,** il governo ha lanciato un progetto per riutilizzare i dati detenuti dagli enti pubblici per sviluppare nuove tecnologie per la salute. Il progetto prevede la creazione di un data hub, un archivio centralizzato di dati sanitari, che sarà utilizzato per sviluppare nuove terapie e cure.

In **Germania**, la città di Berlino ha lanciato un progetto per riutilizzare i dati detenuti dall'ente per sviluppare nuove applicazioni per la partecipazione dei cittadini. Il progetto prevede la creazione di una piattaforma che consentirà ai cittadini di contribuire allo sviluppo di nuove politiche e servizi pubblici.

In **Spagna,** il governo ha lanciato un progetto per riutilizzare i dati detenuti dagli enti pubblici per sviluppare nuove tecnologie per l'agricoltura sostenibile. Il progetto prevede la creazione di un sistema di monitoraggio dell'agricoltura che utilizzerà i dati ambientali per migliorare la produttività e la sostenibilità delle colture

IL REGIME DI RIUTILIZZO DEI DATI PROTETTI DETENUTI DA ENTI PUBBLICI PREVISTO DAL DGA

Non possono essere invece oggetto di riutilizzo:

a) i dati detenuti da imprese pubbliche (a meno che non vi siano specifici regimi che gli Stati membri hanno facoltà di introdurre in sede locale);

b) i dati detenuti dalle emittenti di servizio pubblico e dalle società da esse controllate e da altri organismi o relative società controllate per l'adempimento di un compito di radiodiffusione di servizio pubblico;

c) i dati detenuti da enti culturali e di istruzione quali biblioteche, archivi e musei, nonché orchestre, compagnie d'opera o di balletto e teatri e da istituti di istruzione (ciò perché le opere e gli altri documenti in loro possesso sono prevalentemente coperti da diritti di proprietà intellettuale di terzi);

d) i dati detenuti da enti pubblici e protetti per motivi di pubblica sicurezza, difesa o sicurezza nazionale;

e) i dati la cui fornitura è un'attività che esula dall'ambito dei compiti di servizio pubblico degli enti pubblici.

IL REGIME DI RIUTILIZZO DEI DATI PROTETTI DETENUTI DA ENTI PUBBLICI PREVISTO DAL DGA.

Cosa significa che l'accesso ai dati detenuti dagli enti pubblici ha ad oggetto «dati protetti»?

L'art. 5, comma 3, DGA prescrive che gli **enti pubblici garantiscano la tutela della natura protetta dei dati**. Il contenuto minimo di questo obbligo di protezione (che è presupposto della facoltà di concedere l'accesso ai dati – appunto - "protetti") è rappresentato:

a) dalla **anonimizzazione**, in caso di richiesta di accesso/riutilizzo dei dati personali;

b) dalla **modifica, aggregazione o controllo** in qualsiasi altro modo dei dati in caso di richiesta di accesso/riutilizzo dei dati non personali come ad esempio le informazioni commerciali riservate, i segreti commerciali o i contenuti protetti da diritti di proprietà intellettuale;

c) dalla **predisposizione di un ambiente di trattamento sicuro** fornito o controllato dall'ente pubblico per l'accesso da remoto o fisico, in loco, del riutilizzatore.

IL REGIME DI RIUTILIZZO DEI DATI PROTETTI DETENUTI DA ENTI PUBBLICI PREVISTO DAL DGA.

Tuttavia, la **fornitura di dati anonimizzati o modificati potrebbe non rispondere alle esigenze del riutilizzatore** e dunque in tali ipotesi, il riutilizzatore può accedere a dati personali non anonimizzati a condizione che:

1. sia stata svolta una **valutazione d'impatto** in materia di protezione dei dati (anche nel caso in cui i rischi per i diritti e gli interessi degli interessati risultino minimi);
2. sia **stata comunque consultata l'autorità di controllo ai sensi degli articoli 35 e 36 del GDPR** (indipendentemente dall'esito, anche in caso di risk assessment positivo all'esito della DPIA);
3. l'accesso e il riutilizzo avvengano da remoto o in loco in un ambiente di trattamento sicuro.

«**ambiente di trattamento sicuro**»: *l'ambiente fisico o virtuale e i mezzi organizzativi per garantire la conformità al diritto dell'Unione, quale il regolamento (UE) 2016/679, in particolare per quanto riguarda i diritti degli interessati, i diritti di proprietà intellettuale e la riservatezza commerciale e statistica, l'integrità e l'accessibilità, per garantire il rispetto del diritto dell'Unione e nazionale applicabile, e per consentire all'entità che fornisce l'ambiente di trattamento sicuro di determinare e controllare tutte le azioni di trattamento dei dati, compresi la visualizzazione, la conservazione, lo scaricamento, l'esportazione dei dati e il calcolo dei dati derivati mediante algoritmi computazionali*»

FIVERS

IL REGIME DI RIUTILIZZO DEI DATI PROTETTI DETENUTI DA ENTI PUBBLICI PREVISTO DAL DGA.

Il collegamento, assai stretto, tra Data Governance Act e GDPR sta poi in quanto segue.

I dati personali possono essere trasmessi a terzi per il riutilizzo soltanto laddove il trattamento rappresentato dalla messa a disposizione e trasmissione dei dati personali si fondi su una **idonea una base di legittimità del trattamento** (cfr. articoli 6 e 9 del GDPR).

Ciò vale anche per i dati pseudonimizzati, in tutto e per tutto “personali”.

Nel caso si verifichi un superamento di quelle tutele volte ad impedire la identificazione degli interessati e vi sia dunque una **reidentificazione** della/delle persona/e fisica/che a cui si riferiscono i dati, si verificherà una **vera e propria data breach** e tale violazione non solo farà scattare i meccanismi e i processi di notifica e di comunicazione previsti dagli articoli 33 e 34 del GDPR, **ma imporrà un obbligo nuovo**: quello della **ulteriore notifica** della violazione dei dati **all’ente pubblico che ha concesso il riutilizzo**.

Va considerato che una reidentificazione dell’interessato (e dunque una violazione dei dati) **può verificarsi anche mediante combinazione di set di dati non personali**.

IL REGIME DI RIUTILIZZO DEI DATI PROTETTI DETENUTI DA ENTI PUBBLICI PREVISTO DAL DGA.

L'articolo 5.5 del DGA prescrive inoltre **specifici obblighi e divieti ai riutilizzatori** di dati personali, tra cui:

- il **divieto di reidentificare** gli interessati cui si riferiscono i dati personali;
- **l'obbligo di adottare misure tecniche e operative per impedire la reidentificazione**;
- l'obbligo di **notificare all'ente pubblico qualsiasi violazione dei dati** ("data breach") che comporti la reidentificazione degli interessati.

A questi obblighi ordinari si aggiunge dunque anche quello specifico di notifica della violazione dei dati personali all'ente pubblico detentore.

La specifica procedura per la notifica della data breach all'ente pubblico (aggiuntiva a quella ordinariamente prevista del GDPR) **è codificata nella più generale procedura sul riutilizzo che gli enti pubblici devono rendere nota e pubblicare ai sensi dell'art. 5.1 DGA**

IL REGIME DI RIUTILIZZO DEI DATI PROTETTI DETENUTI DA ENTI PUBBLICI PREVISTO DAL DGA.

L’articolo 5.6 DGA prevede poi che **qualora il riutilizzo dei dati non possa essere consentito** in base alle condizioni individuate dall’ente pubblico detentore (che fissa e rende pubbliche le condizioni trasparenti e non discriminatorie per il riutilizzo) e – per quanto riguarda i dati personali - **non vi sia alcuna base giuridica** per la trasmissione dei dati a norma del Regolamento (UE) 2016/679, l'ente pubblico si adopera al meglio per fornire assistenza ai potenziali riutilizzatori (anche mediante mezzi tecnici adeguati) nel richiedere il consenso degli interessati o l'autorizzazione dei titolari dei dati i cui diritti e interessi possono essere interessati da tale riutilizzo, ove ciò sia fattibile senza un onere sproporzionato per l'ente pubblico (per esempio, l’ente pubblico potrebbe **istituire meccanismi tecnici che permettano di trasmettere le richieste di consenso formulate dai riutilizzatori**, ove ciò sia fattibile nella pratica).

IL REGIME DI RIUTILIZZO DEI DATI PROTETTI DETENUTI DA ENTI PUBBLICI PREVISTO DAL DGA.

Anche se la rubrica dell'articolo 9 DGA ("*Procedura per le richieste di riutilizzo*") lascerebbe intendere che le relative disposizioni indichino aspetti pratici sulle modalità di inoltro all'ente pubblico di una richiesta di riutilizzo, in realtà questa norma si limita a prevedere solo la **tempistica** entro la quale l'ente pubblico deve rispondere (consentendo o negando l'accesso ai dati) e il **diritto di ricorso** (che può essere del richiedente o degli interessati dalla decisione) avverso una decisione (di accoglimento o di diniego di accesso, a seconda dei casi) emessa dall'ente pubblico competente. D'altra parte, l'articolo 5, comma 1, DGA demanda agli stessi enti pubblici che, a norma del diritto nazionale, hanno facoltà di concedere o negare l'accesso per il riutilizzo dei dati il compito (pratico) di rendere pubblica una procedura amministrativa per inoltrare le richieste di riutilizzo (anche attraverso un apposito sportello unico, si veda più oltre).

Quanto alla tempistica per il riscontro alle istanze di riutilizzo, gli enti pubblici adottano una decisione **entro due mesi dalla data di ricevimento della richiesta** (se il diritto nazionale lo prevede, tale termine può essere anche più breve). In caso di **richieste eccezionalmente cospicue e complesse per il riutilizzo**, tale periodo di due mesi **può essere prorogato al massimo di 30 giorni**. In tali casi, gli enti pubblici competenti notificano il prima possibile al richiedente (non è dunque previsto un termine specifico) che occorre più tempo per svolgere la procedura e la relativa motivazione per il ritardo.

IL REGIME DI RIUTILIZZO DEI DATI PROTETTI DETENUTI DA ENTI PUBBLICI PREVISTO DAL DGA.

Divieto di accordi di esclusiva per il riutilizzo dei dati e ipotesi eccezionali di deroga.

L'articolo 4, comma 1 DGA **introduce il divieto di accordi di esclusiva** e (in una prospettiva più ampia) il **divieto di attuare altre pratiche relativamente al riutilizzo di dati detenuti da enti pubblici**.

Il divieto è quello di **concedere diritti esclusivi** (mediante accordi) o implementare pratiche (distorsive della concorrenza) che hanno per oggetto o per effetto di concedere tali diritti esclusivi o di limitare la disponibilità di dati per il riutilizzo da parte di entità diverse dalle parti di tali accordi o per altre pratiche.

Accordi esclusivi sono possibili solo se giustificati e necessari per la fornitura di un **servizio o di un prodotto di interesse generale** "*che non sarebbe altrimenti possibile*" (cfr. art. 4, comma 2, DGA). Tale caso potrebbe presentarsi qualora l'utilizzo esclusivo dei dati rappresenti l'unico modo per massimizzare i benefici sociali dei dati in questione, ad esempio quando esiste un'unica entità (che si è specializzata nel trattamento di uno specifico set di dati) in grado di fornire il servizio o il prodotto che consente all'ente pubblico di fornire a sua volta un servizio o un prodotto di interesse generale (cfr. Considerando n. 13). In questi casi di deroga eccezionale al divieto di accordi di esclusiva, il DGA comunque introduce a garanzia specifici vincoli, e cioè:

IL REGIME DI RIUTILIZZO DEI DATI PROTETTI DETENUTI DA ENTI PUBBLICI PREVISTO DAL DGA.

1. **vincoli di forma dell'atto** (atto amministrativo o accordo contrattuale);

2. **vincoli di contenuto** (previsione di specifiche norme a tutela dei principi di trasparenza, parità di trattamento e non discriminazione);

3. **vincoli di durata** (la durata del diritto esclusivo di riutilizzo dei dati non può superare i **12 mesi** e - ove si concluda un contratto - la durata del contratto è la stessa della durata del diritto esclusivo);

4. **vincoli di trasparenza** (con la pubblicazione online dei motivi per cui è necessario concedere diritti di esclusiva, in una forma conforme al vigente quadro normativo in materia di appalti pubblici;

5. **vincoli di riesame periodico** basato su un'analisi di mercato al fine di accertare che l'esclusività concessa alle (stringenti) condizioni di deroga al divieto continui ad essere necessaria.

FIVERS

Le specifiche tariffe previste dal DGA per il riutilizzo dei dati protetti detenuti da enti pubblici.

FIVERS

IL REGIME DI RIUTILIZZO DEI DATI PROTETTI DETENUTI DA ENTI PUBBLICI PREVISTO DAL DGA.

L'articolo 6 del DGA prevede anche altre due opzioni, oltre a quella ordinaria di pagamento di una tariffa ufficiale: **(1)** consentire il riutilizzo dei dati gratuitamente, senza applicazione di tariffe; **(2)** consentire il riutilizzo dei dati a tariffe ridotte.

Per avvalersi del riutilizzo dei dati a tariffa nulla o ridotta, occorre che siano alternativamente integrati due requisiti: **uno soggettivo** – legato alla natura del richiedente (che deve essere una PMI, oppure una start-up oppure un istituto di istruzione oppure occorre essere esponenti della società civile) – ed uno **oggettivo**, legato alla tipologia di riutilizzo richiesto, che deve perseguire **fini non commerciali o fini di ricerca scientifica**. Il Considerando 25 specifica sul punto che i fini di ricerca scientifica includono qualsiasi tipo di finalità connessa alla ricerca, indipendentemente dalla struttura organizzativa o finanziaria dell'istituto di ricerca in questione, ad eccezione della ricerca condotta da un'impresa con finalità di sviluppo, miglioramento o ottimizzazione di propri prodotti o servizi.

Il trasferimento internazionale dei dati da parte del riutilizzatore: le condizioni.

FIVERS

IL REGIME DI RIUTILIZZO DEI DATI PROTETTI DETENUTI DA ENTI PUBBLICI PREVISTO DAL DGA.

L’articolo 5 del DGA, ai commi 9-14, introduce **un assai articolato regime per il trasferimento dei dati non personali verso paesi terzi**, stabilendo un interessante parallelismo con quanto il Capo V – artt. 44-50 - del GDPR prevede per il trasferimento verso Paesi od organizzazioni internazionali terze dei dati di natura personale. E questo è un altro ambito in cui il DGA e il GDPR sono “tangenti”: **ovvio che i dati personali che il riutilizzatore intenda trasferire in paesi terzi saranno soggetti alla specifica disciplina del Regolamento 679/2016**.

Qualora intenda **trasferire a un paese terzo dati non personali protetti per motivi di riservatezza commerciale, riservatezza statistica o protetti dalle norme sulla Proprietà intellettuale e industriale** che tutelano i diritti di terzi, il **riutilizzatore deve informare l'ente pubblico** della sua intenzione a trasferire tali dati e **della finalità di tale trasferimento** al **momento della richiesta di riutilizzo.** Inoltre, quando il riutilizzo avviene sulla base della specifica autorizzazione da richiedere al titolare dei dati (perché non sono applicabili le altre condizioni previste dall’articolo 5, commi 3 e 4 DGA, anonimizzazione, etc), il **riutilizzatore deve informare la persona giuridica i cui diritti possono essere impattati** anche della sua specifica interazione di trasferire i dati in un paese terzo, dettagliando le **finalità del trasferimento** e le **tutele adeguate che lo accompagnano**. In questi casi, l'ente pubblico non consente il riutilizzo a meno che la persona giuridica **non dia l'autorizzazione** al trasferimento.

IL REGIME DI RIUTILIZZO DEI DATI PROTETTI DETENUTI DA ENTI PUBBLICI PREVISTO DAL DGA.

Accanto ai sopra citati obblighi di informazione preventiva, ed al fine di corredare il trasferimento con l'implementazione di garanzie e tutele effettive e adeguate, come richiesto dal DGA, il **riutilizzatore deve impegnarsi contrattualmente affinché anche dopo il trasferimento dei dati nel paese terzo**:

1. siano rispettati e tutelati i diritti di proprietà intellettuale dei terzi;
2. i dati riservati non siano divulgati;
3. il **riutilizzatore successivo** accetti la competenza degli organi giurisdizionali dello Stato membro dell'ente pubblico che trasmette i dati in merito a qualsiasi controversia relativa al rispetto degli obblighi che precedono.

Inoltre, **le persone fisiche o giuridiche a cui è stato concesso il diritto di riutilizzo dei dati devono garantire, al momento della firma di accordi contrattuali con altre parti private**, che i dati non personali detenuti nell'Unione siano accessibili da parte di paesi terzi o ad essi trasferiti **solo in conformità del diritto dell'Unione o del diritto nazionale dello Stato membro interessato**.

IL REGIME DI RIUTILIZZO DEI DATI PROTETTI DETENUTI DA ENTI PUBBLICI PREVISTO DAL DGA.

Un altro ambito di particolare corrispondenza e similitudine tra GDPR/dati personali e DGA/dati non personali con specifico riferimento al **regime sul trasferimento dei dati verso paesi terzi,** è rappresentato dalla **previsione di clausole contrattuali standard per il trasferimento e dal possibile intervento della Commissione UE circa l'adeguatezza dell'ordinamento giuridico del paese terzo**.

Anche il data Governance Act, difatti, prevede con specifico riferimento ai dati non personali protetti che la Commissione UE possa adottare **clausole contrattuali tipo per il rispetto degli obblighi sopra elencati a cui il riutilizzatore deve sottoporre il trasferimento lecito dei dati**.

Inoltre, la stessa Commissione UE può dichiarare che le disposizioni legislative del paese terzo destinatario dei dati:

a) **garantiscono una protezione della proprietà intellettuale e dei segreti commerciali sostanzialmente equivalente** a quella garantita dal diritto dell'Unione;

b) sono applicate e fatte rispettare in modo efficace; e

c) consentono un ricorso giurisdizionale effettivo.

IL REGIME DI RIUTILIZZO DEI DATI PROTETTI DETENUTI DA ENTI PUBBLICI PREVISTO DAL DGA.

L’articolo 5, comma 13, DGA prevede che specifici atti legislativi dell'unione possono stabilire che **determinate categorie di dati non personali detenuti da enti pubblici siano considerate *altamente sensibili*** in quanto il loro trasferimento a paesi terzi potrebbe mettere a rischio gli obiettivi di politica pubblica dell'Unione, quali la sicurezza e la salute pubblica.

Per esempio, determinati set di dati detenuti da soggetti operanti nel sistema sanitario pubblico, quali gli ospedali pubblici, dovrebbero essere considerati dati sanitari altamente sensibili. Altri settori di elevata sensibilità dei dati sono quelli dei **trasporti, dell'energia, dell'ambiente e della finanza**.

Per garantire allora pratiche armonizzate in tutta l'Unione, tali tipologie di dati pubblici non personali altamente sensibili sono tutelati dal DGA in quanto la Commissione UE potrà adottare **atti delegati** integrativi del Regolamento **per fissare particolari condizioni a cui subordinare ulteriormente il trasferimento di tali dati ad elevata sensibilità verso paesi terzi** (es: condizioni sui rischi di reidentificazione dei singoli individui; termini applicabili per il trasferimento o modalità tecniche, quali l'obbligo di utilizzare un ambiente di trattamento sicuro, limiti relativi al riutilizzo dei dati nei paesi terzi o categorie di persone aventi facoltà di trasferire tali dati a paesi terzi o che possono accedere ai dati nel paese terzo fino alle restrizioni al trasferimento dei dati a paesi terzi per tutelare l'interesse pubblico

Gli organismi competenti di supporto agli enti pubblici.

IL REGIME DI RIUTILIZZO DEI DATI PROTETTI DETENUTI DA ENTI PUBBLICI PREVISTO DAL DGA.

Il DGA prevede l'istituzione di un "**organismo competente**" per **sostenere le attività degli enti pubblici che hanno facoltà di consentire o rifiutare il riutilizzo dei dati protetti**.

I **compiti** degli organismi competenti sono soprattutto di **assistenza specialistica, tecnica, organizzativa e amministrativa agli enti pubblici**, ma tra tali compiti vi può essere la stessa concessione dell'accesso ai dati (coincidendo in questo caso con il ruolo proprio degli enti pubblici detentori dei dati protetti che concedono il riutilizzo), ove previsto dalla legislazione settoriale dell'Unione o nazionale.

IL REGIME DI RIUTILIZZO DEI DATI PROTETTI DETENUTI DA ENTI PUBBLICI PREVISTO DAL DGA..

Se gli organismi competenti sono entità di supporto agli enti pubblici che concedono il riutilizzo dei dati, gli **sportelli unici** – la cui istituzione è specularmente prevista dall'articolo 8 DGA – **sono le specifiche entità di supporto ai riutilizzatori che chiedono l'accesso ai dati**.

Lo **sportello unico ha in primo luogo compiti informativi**, dovendo chiarire ai riutilizzatori le condizioni per l'utilizzo dei dati (in base a quanto previsto all'articolo 5 del DGA) e le tariffe – se previste – applicabili. Non solo. Lo sportello unico deve infatti mettere a disposizione dei riutilizzatori, elettronicamente, **una panoramica delle risorse contenente tutte le fonti di dati disponibili,** comprese, se del caso, quelle fonti di dati disponibili presso i punti di informazione settoriali, regionali o locali, con pertinenti informazioni riguardo **ai dati disponibili** (es: informazioni su **formato dei dati, dimensioni dei dati**, etc). Tutte le informazioni – in ogni caso - devono essere "*disponibili e facilmente accessibili*".

Lo sportello unico, oltre ad essere **competente per il ricevimento delle richieste di informazioni e delle richieste di riutilizzo dei dati, le trasmette** poi, ove possibile e opportuno, con mezzi automatizzati, **agli enti pubblici competenti** o, se del caso, agli organismi competenti: è dunque una struttura tipicamente di interfaccia tra i soggetti protagonisti del riutilizzo dei dati.

Il terzo pilastro del DGA: il cosiddetto «altruismo dei dati».

IL TERZO PILASTRO DEL DGA: IL COSIDDETTO «ALTRUISMO DEI DATI».

Il Capo IV – articoli da 16 a 24 DGA – introduce le regole per quello che può definirsi il terzo pilastro del nuovo regime di governance europea dei dati: il cosiddetto "**altruismo dei dati**".

Tale istituto si connota per l'**utilizzo/riutilizzo finalizzato al perseguimento di obiettivi di interesse generale**:

1. di dati personali messi a disposizione su base volontaria dagli interessati, sulla base del consenso informato di questi ultimi; oppure
2. di dati non personali messi a disposizione dai titolari.

Quali sono gli "*obiettivi di interesse generale*" che giustificano la messa a disposizione gratuita di tali dati (salva la compensazione dei soli costi sostenuti per mettere a disposizione i dati)?

Essi comprendono **l'assistenza sanitaria** (si pensi all'utilità per la lotta alle pandemie che ha l'enorme mole di dati raccolti in questi anni di lotta al COVID), **la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche europee, il miglioramento della fornitura dei servizi pubblici, o delle politiche pubbliche, il sostegno alla ricerca scientifica**.

IL TERZO PILASTRO DEL DGA: IL COSIDDETTO «ALTRUISMO DEI DATI».

Per divenire una **organizzazione per l'altruismo dei dati riconosciuta nell'Unione europea** occorre:

1. **essere una persona giuridica (sostanzialmente una ONG, ma non solo) che opera senza scopo di lucro** e garantisce giuridicamente l'indipendenza da qualsiasi entità che operi a scopo di lucro;
2. svolgere, ovviamente, attività di altruismo dei dati e mediante una **struttura funzionalmente separata dalle sue altre attività;**
3. rispettare il **codice di deontologia** che la Commissione promuoverà per integrare il DGA in merito alle organizzazioni per l'altruismo dei dati (art. 22 DGA).

Le organizzazioni per l'altruismo dei dati:

- **devono adottare misure appropriate per garantire la protezione dei dati personali**. Queste misure devono essere in linea con le disposizioni del Regolamento generale sulla protezione dei dati (GDPR);

- devono iscriversi al **registro delle organizzazioni per l'altruismo dei dati istituito** presso l'autorità competente di ciascun Stato membro;

IL TERZO PILASTRO DEL DGA: IL COSIDDETTO «ALTRUISMO DEI DATI».

- devono **tenere registri interni "*completi e accurati*"** per dare evidenza – nella massima trasparenza – delle principali attività, dei soggetti che trattano o utilizzano i dati, delle relative modalità e finalità.

In particolare, detti registri devono censire:

a) tutte le persone fisiche o giuridiche cui è stata data la possibilità di trattare i dati detenuti dall'organizzazione per l'altruismo dei dati riconosciuta, e i loro recapiti;

b) la data o la durata del trattamento dei dati personali o dell'utilizzo di dati non personali;

c) le finalità del trattamento, quali dichiarate dalla persona fisica o giuridica cui è stata data la possibilità di effettuarlo;

d) le eventuali tariffe pagate dalle persone fisiche o giuridiche che trattano i dati.

I rimedi amministrativi e giurisdizionali del Data Governance Act.

FIVERS

I RIMEDI AMMINISTRATIVI E GIURISDIZIONALI DATA GOVERNANCE ACT.

In relazione a qualunque aspetto che rientri nell'ambito di applicazione del DGA le persone fisiche e giuridiche (es: titolari dei dati, utenti, riutilizzatori, etc) hanno il diritto di presentare un **reclamo individuale** o, se del caso, **collettivo** alla pertinente autorità nazionale.

Il reclamo sarà indirizzato alla autorità nazionale per i servizi di intermediazione dei dati competente nel caso di contestazioni nei confronti di un fornitore di servizi di intermediazione dei dati.

Gli interessati si rivolgeranno invece alla all'autorità competente per la registrazione delle organizzazioni per l'altruismo dei dati quando il reclamo riguarda appunto una organizzazione per l'altruismo dei dati riconosciuta.

I fornitori di servizi di intermediazione dei dati hanno poi il diritto a un **ricorso giurisdizionale** effettivo contro le decisioni giuridicamente vincolanti emesse dalle autorità di monitoraggio e sorveglianza di detti fornitori (cfr. art. 14 DGA).

Le organizzazioni per l’altruismo dei dati hanno il diritto a un ricorso giurisdizionale effettivo contro le decisioni giuridicamente vincolanti emesse dalle autorità che hanno il compito di accettare o meno la registrazione delle organizzazioni e conferire loro il riconoscimento ufficiale, e di procedere al loro monitoraggio e alla loro sorveglianza (cfr. art. 19 e 24 DGA).

L’impianto sanzionatorio del Data Governance Act e le misure sanzionatorie del decreto legislativo italiano di coordinamento n. 144/2024.

FIVERS

L’IMPIANTO SANZIONATORIO DEL DATA GOVERNANCE ACT.

L’impianto sanzionatorio previsto dal DGA ha una struttura particolarmente articolata.

In primo luogo, **la determinazioni delle sanzioni è demandata ai singoli Stati Membri per specifiche violazioni**, quali:

1. violazione da parte della persona fisica o giuridica a cui è stato concesso il diritto di riutilizzo dei dati non personali degli obblighi in materia di trasferimento a paesi terzi (possono essere trasferiti dati non personali in paesi terzi per i quali sono soddisfatti i requisiti di cui ai paragrafi 10, 12 e 13 del DGA);
2. violazione da parte di un ente pubblico, o della persona fisica o giuridica cui è stato concesso il diritto di riutilizzo dei dati o da parte del fornitore di servizi di intermediazione dei dati o da parte dell’organizzazione per l'altruismo dei dati riconosciuta del divieto di trasferimento internazionale dei dati non personali ad autorità di paesi terzi che richiedono l’accesso o il trasferimento dei dati non personali al di fuori delle condizioni previste;
3. violazione dell'obbligo di notifica alla autorità competente da parte dei fornitori di servizi di intermediazione dei dati;
4. violazione delle **condizioni per la fornitura di servizi di intermediazione dei dati**;
5. violazione delle **condizioni per la registrazione come organizzazione per l'altruismo dei dati riconosciuta.**

L’IMPIANTO SANZIONATORIO.

L’articolo 4 del decreto legislativo di coordinamento al DGA n. 144/2024 introduce la disciplina sanzionatoria del DGA a livello nazionale, prevedendo che ferma restando **l'applicazione della disciplina in materia di protezione dei dati personali,** salvo che il fatto costituisca **reato,** in caso di violazione:

i. degli obblighi in materia di **trasferimento di dati non personali a Paesi terzi** a norma dell'articolo 5, paragrafo 14, e dell'articolo 31 del DGA;

ii. dell'obbligo di **notifica per i fornitori di servizi di intermediazione dei dati** a norma dell'articolo 11 del DGA;

iii. delle **condizioni per la fornitura di servizi di intermediazione dei dati** a norma dell'articolo 12 del DGA;

iv. delle condizioni per la **registrazione come organizzazione per l'altruismo dei dati riconosciuta** a norma degli articoli 18, 20, 21 e 22 del DGA da parte dei fornitori di servizi di intermediazione dei dati e delle organizzazioni per l'altruismo dei dati;

l'AgID può comminare **sanzioni amministrative pecuniarie da un minimo di euro 10.000 fino a un massimo di euro 100.000**, ovvero, per le **imprese, fino al 6 per cento del fatturato mondiale totale annuo dell'esercizio precedente.**

FIVERS

Il Comitato europeo per l’Innovazione in materia di dati.

IL COMITATO EUROPEO PER L'INNOVAZIONE IN MATERIA DI DATI.

Il Legislatore pone al vertice del nuovo sistema di governance europea dei dati il **Comitato europeo per l'Innovazione in materia di dati,** organismo sovranazionale che richiama ruolo e funzioni – declinate però nel settore della *governance* dei dati – di enti analoghi già in funzione (come il Comitato europeo per la protezione dei dati personali istituto dall'art. 70 del GDPR) o comunque previsti, settorialmente, dalle varie norme del Decennio Digitale della UE in corso di approvazione mentre si scrive (dal *Comitato europeo per i Servizi Digitali*, previsto dalla Legge sui Servizi Digitali, al *Comitato europeo per l'Intelligenza Artificiale*, istituito dal Regolamento UE su IA, fino al *Comitato Consultivo europeo per i Mercati Digitali*, previsto dalla Legge sui Mercati Digitali).

L'articolo 29 DGA affida alla Commissione – che lo presiede - il compito di istituire – rispettando l'equilibrio geografico e di genere tra i membri che lo compongono - il Comitato europeo per l'Innovazione in materia di dati che sarà composto come gruppo di esperti:

IL COMITATO EUROPEO PER L'INNOVAZIONE IN MATERIA DI DATI.

- da rappresentanti delle autorità competenti per i servizi di intermediazione dei dati di tutti gli Stati membri;
- da rappresentanti delle autorità competenti per la registrazione delle organizzazioni per l'altruismo dei dati di tutti gli Stati membri;
- da rappresentanti del Comitato europeo per la protezione dei dati;
- dal Garante europeo della protezione dei dati (European Data protection Supervisor – EDPS);
- da rappresentanti dell'Agenzia dell'Unione europea per la cybersicurezza (ENISA);
- da rappresentanti della Commissione UE;
- dal rappresentante dell'UE per le PMI o da un rappresentante nominato dalla rete dei rappresentanti per le PMI;
- da altri rappresentanti di organi pertinenti di settori specifici nonché di organi con competenze specifiche.

IL COMITATO EUROPEO PER L'INNOVAZIONE IN MATERIA DI DATI.

I compiti del Comitato sono in primo luogo **consultivi e di assistenza alla Commissione UE** per lo sviluppo di **prassi coerenti** che vengano poi applicate in maniera omogenea in tutta l'Unione da parte degli **enti pubblici** che consentono – ai sensi del DGA – il riutilizzo dei dati, o da parte delle **organizzazioni per l'altruismo dei dati** o da parte delle **autorità competenti** per i **servizi di intermediazione dei dati** o da parte delle autorità competenti per la registrazione delle organizzazioni per l'altruismo dei dati.

In sostanza, il Comitato supporta la Commissione nella scrittura di prescrizioni applicative, linee guida operative e orientamenti per i vari organismi e le varie procedure previste dal DGA per (1) il riutilizzo dei dati; (2) il data sharing; (3) l'altruismo dei dati (4) le procedure di abilitazione e registrazione.

Di particolare interesse è il compito – sempre consultivo e di assistenza alla Commissione UE – che il Comitato svolge nella elaborazione di "***orientamenti coerenti***" sulle **modalità per la più efficace protezione - rispetto ad un accesso illecito che comporti il rischio di furto della proprietà intellettuale o di spionaggio industriale - dei "*dati commerciali sensibili non personali*"** [così li definisce l'articolo 30, comma 1, lettera (d) del DGA], rappresentati in particolare da segreti commerciali e da dati non personali che costituiscono un contenuto protetto da diritti di proprietà intellettuale

IL COMITATO EUROPEO PER L'INNOVAZIONE IN MATERIA DI DATI.

Il settore dello sviluppo di **norme intersettoriali per l'utilizzo dei dati e la condivisione inter-settoriale dei dati tra spazi di dati** comuni europei nonché quello del rafforzamento dell'interoperabilità transfrontaliera e intersettoriale dei dati e dei servizi di condivisione dei dati tra diversi settori e ambiti mediante l'integrazione delle norme europee, internazionali o nazionali esistenti (si pensi alla piattaforma multilaterale per la normazione delle TIC, ai Core *Vocabularies* o ai *Building Blocks*) sono due ulteriori ambiti nei quali è richiesto il supporto consulenziale del Comitato per l'Innovazione. In questo ambito il Comitato deve tenere conto delle esistenti attività di **normazione tecnica per l'elaborazione di norme tecniche e giuridiche per la trasmissione di dati tra ambienti di trattamento che renda possibile l'organizzazione degli spazi di dati**.

Infine, il **Comitato ha anche compiti di assistenza degli Stati membri e degli organismi nazionali di questi chiamati a dare esecuzione al DGA**. In particolare, il Comitato facilita la cooperazione tra gli Stati membri in merito alla definizione di condizioni armonizzate per il riutilizzo dei dati detenuti da enti pubblici nell'intero mercato interno e promuove la cooperazione tra le autorità competenti per i servizi di intermediazione dei dati e le autorità competenti per la registrazione delle organizzazioni per l'altruismo dei dati attraverso lo sviluppo di capacità e lo scambio di informazioni.

Il Data Act - Regolamento (UE) n. 2023/2854

REGOLAMENTO 2854/2023 – LA NORMATIVA DATI (DATA ACT)

La **Normativa sui Dati** – o **Data Act** - è stata pubblicata nella Gazzetta ufficiale dell'UE il 22 dicembre 2023 ed è entrata in vigore l'**11 Gennaio 2024**. Diventerà applicabile a partire dal **12 settembre 2025**.

Essa **integra** il **Data Governance Act** (Regolamento 2022/868/UE) già operativo dallo scorso **23 Settembre 2023**, chiudendo il cerchio della **Strategia europea dei Dati della UE:** se da un lato il DGA **aumenta la fiducia nei meccanismi di condivisione volontaria** dei dati, dall'altro il **Data Act fornisce chiarezza giuridica in merito all'accesso e all'utilizzo dei dati**.

Insieme ad altre misure politiche e opportunità di finanziamento, **questi due regolamenti contribuiranno alla creazione di un mercato unico dei dati nell'UE**, rendendo l'Europa leader **nell'economia dei dati** e sfruttando il potenziale delle quantità sempre crescenti di dati, **in particolare quelli industriali,** a vantaggio dell'economia e della società europee.

REGOLAMENTO 2854/2023 – LA NORMATIVA DATI (DATA ACT)

Intanto occorre partire dalle definizioni che a vario titolo sono fornite dall'articolo 2 del Data Act e che interessano i dati:

«dati»: qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva;

«dati personali»: i dati personali quali definiti all'articolo 4, punto 1, del regolamento (UE) 2016/679;

«dati non personali»: i dati diversi dai dati personali;

«metadati»: una descrizione strutturata del **contenuto o dell'uso** dei dati che agevola la ricerca o l'utilizzo di tali dati;

Il Data Act si applica **ai dati personali e non personali,** inclusi i dati nei seguenti contesti:

Quale ambito di applicabilità copre il Data Act?

REGOLAMENTO 2854/2023 – LA NORMATIVA DATI (DATA ACT)

Il Data Act si applica, tra l'altro:

- alla **messa a disposizione** dei **dati** del **prodotto connesso** e di un **servizio correlato all'utente** del prodotto connesso o del servizio correlato;
- alla **messa a disposizione** di **dati** da parte dei **titolari dei dati** ai **destinatari dei dati;**
- alla **messa a disposizione** di **dati** da parte dei **titolari dei dati** agli **enti pubblici**, alla Commissione, alla Banca centrale europea e a organismi dell'Unione, a **fronte di necessità eccezionali** per tali dati, per **l'esecuzione di un compito specifico svolto nell'interesse pubblico;**
- alla **facilitazione del passaggio da un servizio di trattamento dei dati all'altro**;
- all'introduzione di **garanzie contro l'accesso illecito di terzi ai dati non personali**;
- allo sviluppo di **norme di interoperabilità** per i dati a cui accedere, da trasferire e utilizzare.

REGOLAMENTO 2854/2023 – LA NORMATIVA DATI (DATA ACT)

- ai dati, ad eccezione del contenuto, **relativi alle prestazioni, all'uso e all'ambiente dei prodotti connessi e dei servizi correlati** (specificandosi che nei casi in cui il Data Act fa riferimento a «*prodotti connessi o servizi correlati*» tali riferimenti comprendono **anche gli assistenti virtuali**, nella misura in cui interagiscono con un prodotto connesso o un servizio correlato;

- a tutti i **dati del settore privato soggetti a obblighi di condivisione dei dati** previsti dalla legge;

- a tutti i **dati del settore privato il cui accesso e utilizzo si basano su contratti tra imprese**;

- a tutti i **dati non personali del settore privato**;

- a tutti i **dati e servizi trattati dai fornitori di servizi di trattamento dei dati**;

- a tutti i **dati non personali detenuti nell'Unione da fornitori di servizi di trattamento dei dati**.

Esempi di prodotti connessi: prodotti di consumo (ad esempio auto connesse, dispositivi di monitoraggio della salute, dispositivi per la casa intelligente), altri prodotti (ad esempio aerei, robot, macchine industriali).

Esempio di servizio correlato: un utente acquista una lavatrice e installa un'applicazione che gli consente di misurare l'impatto ambientale del ciclo di lavaggio in base ai dati provenienti dai diversi sensori presenti all'interno della macchina e di regolare il ciclo di conseguenza; un'app per regolare la luminosità delle luci o la temperatura di un frigorifero.

Esempi di servizi aftermarket e accessori: servizi di riparazione e manutenzione, assicurazione basata sui dati.

Qual è l’ambito di applicazione soggettivo del Data Act?

FIVERS

REGOLAMENTO 2854/2023 – LA NORMATIVA DATI (DATA ACT)

Il Data Act si applica ai **seguenti soggetti:**

a) ai **fabbricanti di prodotti connessi immessi sul mercato dell'Unione** e ai **fornitori di servizi correlati**, inclusi gli assistenti virtuali, indipendentemente dal loro luogo di stabilimento di tali fabbricanti e fornitori;

b) agli **utenti nell'Unione di** prodotti connessi o servizi correlati di cui alla lettera a);

c) ai **titolari dei dati**, **indipendentemente dal loro luogo di stabilimento**, che **mettono dati a disposizione dei destinatari** dei dati nell'Unione;

d) ai **destinatari dei dati nell'Unione** a disposizione dei quali sono messi i dati;

e) e) agli **enti pubblici**, alla Commissione, alla Banca centrale europea e agli organismi dell'Unione che chiedono ai titolari dei dati di mettere i dati a disposizione nel caso tali dati siano necessari a fronte di una necessità eccezionale per l'esecuzione di un compito specifico svolto nell'interesse pubblico e ai titolari dei dati che forniscono tali dati in risposta a tale richiesta;

f) ai **fornitori di servizi di trattamento dei dati, indipendentemente dal loro luogo di stabilimento**, che forniscono **tali servizi a clienti nell'Unione**;

g) ai **partecipanti agli spazi di dati**, ai **venditori di applicazioni che utilizzano contratti intelligenti** e alle persone la cui attività commerciale, imprenditoriale o professionale comporti **l'implementazione di contratti intelligenti per altri** nel contesto dell'esecuzione di un accordo.

REGOLAMENTO 2854/2023 – LA NORMATIVA DATI (DATA ACT)

Dopo le **disposizioni generali (Capo I),** che stabiliscono l'ambito di applicazione del regolamento e definiscono i termini chiave, il Data Act è strutturato nei seguenti Capi:

Capo II sulla **condivisione dei dati business-to-business e business-to-consumer nel contesto dell'IoT**: gli utenti di oggetti IoT possono accedere, utilizzare e trasferire i dati che generano congiuntamente attraverso l'uso di un prodotto connesso.

Capo III sulla **condivisione dei dati tra imprese**: chiarisce le condizioni di condivisione dei dati ogni volta che un'impresa è obbligata per legge, anche attraverso il Data Act, a condividere i dati con un'altra impresa.

Capo IV sulle **clausole contrattuali abusive**: queste disposizioni tutelano tutte le imprese, in particolare le PMI, contro le clausole contrattuali abusive imposte loro.

REGOLAMENTO 2854/2023 – LA NORMATIVA DATI (DATA ACT)

Capo V sulla **messa a disposizione dei dati a favore degli enti pubblici in determinate situazioni di necessità eccezionale** per prendere decisioni basate su dati concreti grazie a misure di accesso a determinati dati in possesso del settore privato.

Capo VI sul **passaggio tra servizi di elaborazione dati**: i fornitori di servizi di cloud ed edge computing devono soddisfare requisiti minimi per facilitare l'interoperabilità e consentire il passaggio.

Capo VII sull'accesso illegale ai dati da parte di governi di Paesi terzi: i dati non personali conservati nell'UE sono protetti da richieste di accesso illegali da parte di governi stranieri.

REGOLAMENTO 2854/2023 – LA NORMATIVA DATI (DATA ACT)

Capo VIII sull'interoperabilità: i partecipanti agli spazi dati devono soddisfare i criteri per consentire il flusso dei dati all'interno e tra gli spazi dati. Un archivio dell'UE stabilirà gli standard e le specifiche pertinenti per l'interoperabilità del cloud

Capo IX sull'applicazione: Gli Stati membri devono designare una o più autorità competenti per il controllo e l'applicazione della legge sui dati. Nel caso in cui vengano designate più autorità, deve essere nominato un "coordinatore dei dati" che funga da unico punto di contatto a livello nazionale.

Capo X sul cosiddetto **«diritto sui generis» relativo alle banche dati elettroniche.** La direttiva sulle banche di dati ha introdotto, tra l'altro, un diritto "sui generis" specifico a proteggere la banca dati se il suo costitutore ha effettuato un investimento sostanziale anche senza essere l’autore.

Il Data Act **chiarisce che il diritto "sui generis" di cui alla direttiva sulle banche di dati (direttiva 96/9/CE) non si applica alle banche dati contenenti dati generati o ottenuti mediante l'uso di prodotti o di servizi correlati** e in tal modo garantisce che il diritto "sui generis" non interferisca con i diritti delle imprese e dei consumatori di accedere ai dati, utilizzarli e condividerli di cui al presente regolamento.

Capo XI sulle disposizioni finali.

Applicazione pratica delle regole del Data Act.

REGOLAMENTO 2854/2023 – LA NORMATIVA DATI (DATA ACT)

Accesso ai dati generati dall’uso dei prodotti connessi e dei servizi correlati.

Il Data Act conferisce **agli individui** e **alle imprese** il **diritto di accedere ai dati prodotti attraverso il loro utilizzo di oggetti, macchine e dispositivi intelligenti**.

Gli utenti dei **prodotti connessi** o dei **servizi correlati** possono poi scegliere di **condividere questi dati con terze parti.** Ciò consentirà ai **fornitori di servizi post-vendita** (ad esempio di riparazione) di migliorare e innovare i loro servizi, promuovendo una concorrenza leale con servizi simili forniti dai fabbricanti. Di conseguenza, gli utenti di prodotti connessi, compresi i consumatori, gli agricoltori, le compagnie aeree, le imprese di costruzione o i proprietari di edifici, avranno la possibilità di scegliere **fornitori di riparazione e manutenzione più efficienti in termini di costi** (o di svolgere essi stessi tali compiti), il che porterà a prezzi potenzialmente più bassi sul mercato.

l **soggetto terzo scelto dall'utente compensa il fabbricante** per i costi di concessione dell'accesso ai dati, vale a dire per le modalità tecniche di messa a disposizione dei dati, come le interfacce per programmi applicativi.

REGOLAMENTO 2854/2023 – LA NORMATIVA DATI (DATA ACT)

Accesso ai dati generati dall'uso dei prodotti connessi e dei servizi correlati.

La **Commissione UE, prima del 12 settembre 2025,** elabora e raccomanda **clausole contrattuali tipo non vincolanti relative all'accesso ai dati e al relativo utilizzo, comprese clausole su un compenso ragionevole e sulla protezione dei segreti commerciali.**

FIVERS

REGOLAMENTO 2854/2023 – LA NORMATIVA DATI (DATA ACT)

Clausole contrattuali abusive relative all'accesso ai dati e al relativo utilizzo tra imprese.

Il Data Act individua i criteri per l'individuazione delle clausole contrattuali abusive tra imprese in caso di abuso di una posizione negoziale più forte. La stragrande maggioranza delle clausole contrattuali che dal punto di vista commerciale sono più favorevoli a una parte rispetto all'altra, comprese quelle che sono normali nei contratti tra imprese, sono una normale espressione del principio della libertà contrattuale e continuano ad applicarsi. Ai fini del Data Act, tra le pratiche che si discostano considerevolmente dalle buone prassi commerciali figurerebbe, tra l'altro, quella di **pregiudicare oggettivamente la capacità della parte alla quale la clausola è stata unilateralmente imposta di tutelare il suo legittimo interesse commerciale con riferimento ai dati forniti o generati nel corso del contratto con la controparte**.

Per garantire la certezza del diritto, il Data Act stabilisce un **elenco di clausole che sono sempre considerate abusive** e un **elenco di clausole che si presumono abusive**. In quest'ultimo caso, l'impresa che impone la clausola contrattuale dovrebbe **poter confutare** la presunzione di abusività dimostrando che la clausola contrattuale inclusa nell'elenco del presente regolamento non è, nel caso di specie, abusiva.

REGOLAMENTO 2854/2023 – LA NORMATIVA DATI (DATA ACT)

Portabilità dei contratti/servizi cloud e dei servizi di trattamento dei dati.

Sarà più facile **trasferire da un fornitore all'altro** dati e applicazioni (da archivi fotografici privati fino all'intera amministrazione di un'impresa) **grazie ai nuovi obblighi che eliminano in particolare gli ostacoli pre-commerciali, commerciali, tecnici, contrattuali e organizzativi frapposti dai fornitori per passare ad altri fornitori o che vietano di utilizzare più fornitori di servizi cloud contemporaneamente.**

Il Data Act introduce per i fornitori di servizi cloud anche un nuovo quadro di normazione per **l'interoperabilità dei dati e del cloud**.

A decorrere dal 12 gennaio 2027, i fornitori di servizi di trattamento dei dati non potranno imporre al cliente tariffe di passaggio per il processo di passaggio ad altri fornitori, mentre a decorrere dall'11 gennaio 2024 e fino al 12 gennaio 2027, i fornitori di servizi cloud possono imporre al cliente **tariffe di passaggio ridotte** per il passaggio ad altri fornitori che non siano **superiori ai costi direttamente connessi al pertinente processo di passaggio sostenuti dal fornitore di servizi di trattamento dei dati.**

REGOLAMENTO 2854/2023 – LA NORMATIVA DATI (DATA ACT)

Portabilità dei contratti/servizi cloud e dei servizi di trattamento dei dati.

La **Commissione UE, prima del 12 settembre 2025,** elabora e raccomanda **clausole contrattuali tipo non vincolanti** per i contratti di cloud computing per assistere le parti nella stesura e nella **negoziazione di contratti equi, ragionevoli e non discriminatori dal punto di vista dei diritti e degli obblighi contrattuali**.

FIVERS

REGOLAMENTO 2854/2023 – LA NORMATIVA DATI (DATA ACT)

Obbligo di mettere a disposizione i dati sulla base di necessità eccezionali.

Qualora un ente pubblico, la Commissione, la Banca centrale europea o un organismo dell'Unione dimostri una necessità eccezionale di utilizzare taluni dati, **ivi compresi i pertinenti metadati necessari per interpretare e utilizzare tali dati**, per svolgere le proprie funzioni statutarie nell'interesse pubblico, i **titolari dei dati che sono persone giuridiche diverse da enti pubblici e che detengono tali dati li mettono a disposizione su richiesta motivata**.

Protezione avversi l'accesso illegale ai dati non personali da parte di governi extra SEE.

Inoltre Il **Data Act introduce garanzie obbligatorie per proteggere i dati contenuti nelle infrastrutture cloud nell'UE.** Ciò impedirà **l'accesso illecito da parte di governi non appartenenti all'UE/al SEE.** Con queste misure la normativa sui dati sosterrà l'adozione del cloud in Europa, che a sua volta stimolerà una condivisione efficiente dei dati all'interno dei settori e tra di essi.

Grazie per l’attenzione.

Prof. Avv. Alessandro del Ninno

@ alessandro.delninno@5rs.it

www.5rs.it

www.alessandrodelninno.it

FIVERS