OSSERVATORIO
TMT·DATA PROTECTION
di Morri Rossetti

Monthly Roundup

Novembre 2022

MONTHLY ROUNDUP

Novembre 2022

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

---

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

- **Provvedimenti del Garante e di altre autorità europee:**

- Fidelity card: il Garante privacy sanziona Douglas Italia per 1 milione e 400 mila euro [Link]
- Il Garante multa Vodafone, il call center deve dare informazioni comprensibili [Link]
- **Ireland**: Data Protection Commission announces decision in Facebook "Data Scraping" Inquiry [Link]
- **Germany**: Datenschutzkonferenz ("DSK") releases assessment of Microsoft 365 [Link]

- **Provvedimenti EDPB:**

- Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) [Link]

- **Commissione europea**

- Digital Services Act: EU's landmark rules for online platforms enter into force [Link]
- Digital Markets Act: rules for digital gatekeepers to ensure open markets enter into force [Link]

PRINCIPALI AGGIORNAMENTI

- Direttiva antiriciclaggio e protezione dati: il recente intervento della Corte di Giustizia Europea
- Ipotesi di contitolarità ai sensi dell'art. 26 del GDPR: come individuarle e come disciplinarle
- Trasferimenti di dati tra UE e Stati Uniti: Biden firma un nuovo Executive Order

Direttiva antiriciclaggio e protezione dati: il recente intervento della Corte di Giustizia Europea

*I giudici della Corte di Giustizia dell'Unione europea ("**CGUE**"), con la sentenza dello scorso 22 novembre, hanno considerato "invalida" la disposizione della direttiva antiriciclaggio [1] (la "**Direttiva Antiriciclaggio**") ai sensi della quale gli Stati rendono accessibili al pubblico le informazioni sulla titolarità effettiva delle società e delle altre entità giuridiche costituite nel loro territorio.*

Il provvedimento in esame è parte integrante di un complesso di regole comunitarie in materia di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo finalizzato ad armonizzare la normativa interna degli Stati Membri in un settore che spesso si caratterizza per l'elemento della transnazionalità nella commissione dei reati. La matrice transnazionale di numerosi fatti di riciclaggio e finanziamento del terrorismo ha, infatti, condotto il Legislatore Europeo ad interessarsi e a disciplinare il fenomeno sin dagli anni '90 al fine di garantire azioni efficaci di contrasto dinnanzi a fatti che possono cagionare danni economici di rilevante entità per gli Stati Membri.

Il caso

La pronuncia in esame trae origine dall'approvazione, nel 2019, di una legge lussemburghese [2] che, in conformità a quanto previsto dalla Direttiva Antiriciclaggio, istituiva un Registro dei titolari effettivi ("**Registro**") nel quale dovevano essere iscritte e conservate informazioni relative alla titolarità effettiva delle entità registrate, alcune delle quali, risultavano accessibili, attraverso Internet, al pubblico.

In tale contesto, una società lussemburghese e un titolare effettivo di una società lussemburghese presentavano due ricorsi al Tribunale circoscrizionale contro *Luxembourg Business Registers*, in quanto avevano chiesto a quest'ultimo, senza successo, di limitare l'accesso del pubblico alle informazioni che li riguardavano.

Il Tribunale, ritenendo che la divulgazione di tali informazioni fosse idonea a comportare un rischio sproporzionato di violazione dei diritti fondamentali dei titolari effettivi coinvolti, sottoponeva alla CGUE alcune questioni pregiudiziali aventi ad oggetto, da un lato, l'interpretazione di alcune disposizioni della Direttiva Antiriciclaggio e, dall'altro, un giudizio relativo alla validità di queste ultime alla luce della Carta dei diritti fondamentali dell'Unione europea ("**Carta**").

Investita della questione, la CGUE, con sentenza del 22 novembre 2022 nelle cause riunite n. C-37/20 e C-601/20, ha considerato "invalida" la disposizione della Direttiva Antiriciclaggio ai sensi della quale gli Stati rendono accessibili al pubblico le informazioni contenute nel Registro relative alla titolarità effettiva delle società e delle altre entità giuridiche costituite nel loro territorio.

Per i giudici della CGUE, infatti, la disposizione in oggetto implica una grave ingerenza nei diritti garantiti dagli artt. 7 e 8 della Carta, rispettivamente il diritto alla vita privata e alla protezione dei dati personali.

[1] Direttiva (UE) 2015/849, così come modificata dalla direttiva (UE) 2018/843.

2 Loi du 13 janvier 2019 instituant un Registre des bénéficiaires effectifs (mémorial A 15) (Law of 13 January 2019 establishing a Register of Beneficial Ownership).

Nello specifico, prosegue la CGUE, le informazioni divulgate grazie all'accessibilità del Registro al pubblico consentirebbero a un numero potenzialmente illimitato di persone di ricevere informazioni in merito alla situazione materiale e finanziaria del titolare effettivo, esponendo i dati personali delle persone interessate a un eventuale utilizzo abusivo, aggravato dalla circostanza che, una volta messi a disposizione del pubblico, tali dati potrebbero essere non solo liberamente consultati, ma anche conservati e diffusi.

Sebbene la CGUE ha ricordato che (i) lo scopo della Direttiva in esame è quello di prevenire il riciclaggio di denaro e il finanziamento del terrorismo attraverso una maggiore trasparenza, da intendersi come un "obiettivo di interesse generale" e quindi idoneo a giustificare ingerenze nei diritti fondamentali sanciti agli artt. 7 e 8 della Carta; (ii) l'accesso del pubblico alle informazioni sulla titolarità effettiva è funzionale alla realizzazione di tale obiettivo, tuttavia, nel caso di specie, la stessa Corte ha ritenuto che l'accesso del pubblico alle informazioni sulla titolarità effettiva abbia dato luogo a un'ingerenza nei diritti di cui agli artt. 7 e 8 della Carta non limitata allo stretto necessario né proporzionata all'obiettivo perseguito.

Infatti, a parere della CGUE, l'attuale regime della Direttiva Antiriciclaggio rappresenterebbe - rispetto al regime vigente anteriormente alla stessa (nell'ambito del quale, per accedere ai dati, era necessario dimostrare l'esistenza di un legittimo interesse) - una lesione considerevolmente più grave dei diritti fondamentali di cui agli artt. 7 e 8 della Carta e ciò senza che tale aggravamento sia compensato dagli eventuali benefici nella lotta contro il riciclaggio di denaro e il finanziamento del terrorismo.
La CGUE ha infine aggiunto che le disposizioni facoltative che consentono agli Stati membri, rispettivamente, di subordinare la messa a disposizione delle informazioni sulla titolarità effettiva ad una registrazione online e di prevedere, in circostanze eccezionali, talune deroghe all'accesso del pubblico a tali informazioni, non sono, di per sé, idonee a dimostrare né una ponderazione equilibrata tra l'obiettivo di interesse generale perseguito e i diritti fondamentali sanciti agli articoli 7 e 8 della Carta, né l'esistenza di sufficienti garanzie che consentano alle persone interessate di tutelare efficacemente i loro dati personali contro i rischi di abusi.

Ciò premesso, sarebbe auspicabile un intervento del Legislatore Europeo che, prendendo spunto dalle indicazioni fornite dalla CGUE, indichi agli Stati Membri interventi normativi idonei a garantire un bilanciamento tra gli interessi di cui agli artt. 7 e 8 della Carta e l'esigenza – anch'essa individuata dalla normativa comunitaria e interna agli Stati stessi – di effettuare efficaci controlli sul titolare effettivo.

* * *

Ipotesi di contitolarità ai sensi dell'art. 26 del GDPR: come individuarle e come disciplinarle

L'articolo 26 del Regolamento UE 2016/679 ("**GDPR**") prevede che *"allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di*

comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati".

Al fine di meglio comprendere quando sussiste un'ipotesi di contitolarità, rilevano altresì le *"Linee Guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR"* (le "**Linee Guida**") adottate *dall'European Data Protection Board* ("**EDPB**") il 7 luglio 2021, con particolare riferimento alla Parte I, sezione 3.

Il corretto inquadramento dei ruoli delle parti e, nel caso di specie, la corretta qualifica di contitolari del trattamento ha principalmente conseguenze in termini di ripartizione degli obblighi di rispetto delle norme in materia di protezione dei dati personali e, in particolare, per quanto concerne i diritti delle persone fisiche.

Come individuare un'ipotesi di contitolarità

Ai sensi dell'articolo 26 del GDPR, la contitolarità sussiste qualora due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento.

Per valutare l'esistenza di contitolari del trattamento è pertanto necessario considerare due criteri:

I. il trattamento non sarebbe possibile senza la partecipazione di entrambe le parti, nel senso che il trattamento da parte di ciascuna di esse è inseparabile, cioè inestricabilmente legato;
II. la partecipazione congiunta deve includere la determinazione delle finalità, da un lato, e la determinazione dei mezzi, dall'altro, dove:
III. le finalità definite congiuntamente non devono essere necessariamente le medesime ma, come precisato dalla giurisprudenza della Corte di Giustizia dell'Unione europea, i soggetti coinvolti possono perseguire anche finalità strettamente collegate o complementari (ad esempio, possono sussistere finalità collegate e complementari quando esiste un vantaggio reciproco[3] derivante dalla medesima operazione di trattamento, sebbene tale vantaggio (i) sia considerato quale valore meramente indicativo e (ii) la sola sussistenza di un vantaggio reciproco, anche economico, non comporta una contitolarità);
IV. l'influenza sulla determinazione dei mezzi non riguarda tutti i mezzi del trattamento ma ciò può avvenire in misura diversa tra i soggetti coinvolti. Inoltre, uno dei soggetti coinvolti più fornire i mezzi del trattamento che vengono altresì utilizzati dagli altri (ad esempio nel caso di piattaforme), sebbene l'uso di un sistema o di un'infrastruttura comune per il trattamento dei dati può non sempre comportare la sussistenza di un'ipotesi di contitolarità.

In ogni caso, la valutazione della contitolarità deve essere fondata su un'analisi fattuale *"dell'influenza effettivamente esercitata sulle finalità e sui mezzi del trattamento"* e della relativa partecipazione congiunta delle parti.

L'influenza esercitata da ciascuna parte deve essere, infatti, determinante sull'effettuazione del trattamento e sulle relative modalità. Tuttavia, come specificato dalle Linee Guida, la partecipazione può assumere forme diverse:

[3] Sul punto, si rimanda a quanto indicato nelle Linee Guida in merito alla sentenza Fashion ID della CGUE

I. può assumere la forma di decisione comune presa dai diversi soggetti coinvolti, intesa come "assunzione di una decisione e un'intenzione condivisa di adottare tale decisione"; oppure

II. può derivare da decisioni convergenti dei diversi soggetti coinvolti quando tali decisioni "si integrano a vicenda e sono necessarie affinché il trattamento abbia luogo, in modo tale da avere un impatto tangibile sulla determinazione delle finalità e dei mezzi del trattamento". Le Linee Guida forniscono ulteriori chiarimenti sul punto precisando che le decisioni convergenti non devono riguardare l'intero rapporto contrattuale, ma piuttosto devono riguardare gli aspetti rilevanti dei trattamenti dei dai dati personali che la parti intendono porre in essere. Sussiste una decisione convergente quando "il trattamento non sarebbe possibile senza la partecipazione di entrambe le parti alle finalità e ai mezzi, nel senso che i trattamenti di ciascuna parte sono tra loro indissociabili, ovvero indissolubilmente legati".

In aggiunta, rileva altresì specificare che:

- il fatto che una delle parti non abbia accesso ai dati personali trattati può non essere sufficiente per escludere la contitolarità;
- la contitolarità può sussistere solo con riferimento a quelle operazioni di trattamento rispetto al quale il singolo contitolare determina, insieme ad altri, i mezzi e le finalità di tale trattamento (e quindi non con riferimento a tutte le operazioni di trattamento);
- la sussistenza di un coinvolgimento diverso tra le varie parti (in fasi e in misura diversa) può determinare un livello di responsabilità diverso tra i soggetti coinvolti, da valutare in base alle circostanze concrete.
- È utile riportare un esempio previsto dalle Linee Guida dell'EDPB volto a chiarire come gli elementi concreti possono determinare o meno la sussistenza di una contitolarità.

Esempio: agenzia di viaggi

Un'agenzia di viaggi invia alla compagnia aerea e a una catena di alberghi i dati personali dei propri clienti, al fine di effettuare prenotazioni per un pacchetto turistico. La compagnia aerea e l'albergo confermano la disponibilità dei posti e delle camere richiesti. L'agenzia di viaggi rilascia ai clienti i documenti di viaggio e i buoni. Ciascuno dei soggetti tratta i dati per svolgere le proprie attività e utilizzando i propri mezzi. In questo caso, l'agenzia di viaggi, la compagnia aerea e l'albergo sono tre distinti titolari del trattamento che perseguono finalità autonome e separate e non sussiste una contitolarità del trattamento.

L'agenzia di viaggi, la catena alberghiera e la compagnia aerea decidono poi di partecipare congiuntamente alla creazione di una piattaforma comune su internet per la finalità comune di offrire pacchetti turistici. Concordano i mezzi essenziali da utilizzare, quali i dati da archiviare, le modalità di assegnazione e conferma delle prenotazioni e chi può avere accesso alle informazioni memorizzate. Inoltre, decidono di condividere i dati dei clienti al fine di effettuare operazioni di marketing congiunte. In questo caso, l'agenzia di viaggi, la compagnia aerea e la catena alberghiera determinano congiuntamente le finalità e le modalità di trattamento dei dati personali dei rispettivi clienti e saranno pertanto contitolari del trattamento per quanto riguarda le operazioni di trattamento relative alla piattaforma comune di prenotazione via internet e le operazioni congiunte di marketing. Tuttavia, ciascuna di esse manterrebbe la titolarità

esclusiva di altre attività di trattamento svolte al di fuori della piattaforma comune su internet.

Come disciplinare un'ipotesi di contitolarità

In considerazione di quanto sopra, i contitolari del trattamento, tenendo conto delle circostanze del caso specifico, determinano in modo trasparente e concordano, mediante un accordo, le rispettive responsabilità al fine di adempiere agli obblighi previsti dal GDPR. In particolare, la determinazione delle rispettive responsabilità deve riguardare e coprire:

a) l'esercizio dei diritti degli interessati e l'obbligo di fornire loro le informazioni di cui agli articoli 13 e 14 del GDPR, fermo restando che gli interessati possono esercitare i loro diritti nei confronti di ciascuno dei contitolari del trattamento;
b) altri obblighi del titolare del trattamento quali, ad esempio, il rispetto dei principi generali di protezione dei dati, l'individuazione della corretta base giuridica, l'implementazione di misure di sicurezza, la gestione della notifica delle violazioni dei dati, l'esecuzione di valutazioni d'impatto sulla protezione dei dati, l'utilizzo e la nomina di responsabili del trattamento, il trasferimento dei dati a paesi terzi e le disposizioni relative ai contatti con gli interessati e le autorità di controllo;
c) la designazione di un punto di contatto per gli interessati, che tuttavia non è una misura obbligatoria ma fortemente raccomandata dall'EDPB.

Come chiarito dalle Linee Guida dell'EDPB, non è necessario che gli obblighi del GDPR siano equamente distribuiti tra i contitolari del trattamento, in quanto agli stessi è riconosciuto un certo grado di flessibilità nel distribuire e ripartire gli obblighi tra loro.
Infatti, la *ratio* dell'articolo 26 del GDPR è quella di garantire che, in presenza di una pluralità di titolari del trattamento, la responsabilità per l'osservanza delle norme in materia di protezione dei dati sia chiaramente ripartita, al fine di evitare che la protezione dei dati personali sia ridotta o che un conflitto negativo di competenze porti a scappatoie per cui alcuni obblighi non siano rispettati da nessuna delle parti coinvolte nel trattamento.

In ogni caso, per rispettare il principio di *accountability*, l'EDPB raccomanda ai contitolari del trattamento di documentare debitamente l'analisi interna.

Quanto alla forma giuridica dell'accordo, l'articolo 26 del GDPR non fornisce indicazioni specifiche. Ne deriva che i contitolari del trattamento sono liberi di concordare la forma dell'accordo stesso. Tuttavia, poiché l'accordo è vincolante per ciascuno dei contitolari e attraverso lo stesso essi concordano e si impegnano reciprocamente a essere responsabili dell'adempimento dei rispettivi obblighi, le Linee guida dell'EDPB raccomandano ai contitolari di redigere un documento vincolante (ad esempio, un contratto).

Inoltre, come chiarito dall'articolo sopra citato, i contitolari del trattamento devono mettere a disposizione dell'interessato un estratto di tale accordo e sul punto e Linee guida dell'EDPB chiariscono che le informazioni principali da fornire riguardano:

a) tutti gli elementi dell'informativa di cui agli articoli 13 e 14 del GDPR;
b) la specificazione di quale contitolare del trattamento è responsabile di garantire il rispetto di tali elementi;
c) il punto di contatto, se designato.

La necessità di stabilire in un accordo formale le rispettive responsabilità di ciascun titolare del trattamento è rilevante anche (e soprattutto) dal

punto di vista del regime di responsabilità interna.

Infatti, considerato che l'articolo 83, paragrafo 4, del GDPR prevede espressamente che entrambi i titolari del trattamento rispondono solidalmente per l'intero ammontare del danno nei confronti dell'interessato (fatto salvo il diritto di regresso nei confronti dell'altro contitolare), l'eventuale ripartizione interna della responsabilità tra i contitolari è certamente rilevante in caso di azioni di regresso al fine di determinare la partecipazione di ciascun titolare al trattamento.

Inoltre, va notato che la mancata adozione dell'accordo interno tra i contitolari del trattamento è soggetta, ai sensi dell'articolo 83, paragrafo 4, del GDPR, a sanzioni amministrative pecuniarie fino a 10.000.000 di euro o, nel caso di un'impresa, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

In ogni caso, è importante notare che l'accordo interno non è vincolante per le autorità di protezione dei dati, ma può costituire un valido strumento per ricostruire il ruolo di ciascun titolare del trattamento rispetto al trattamento dei dati nella misura e nei limiti in cui rispecchia adeguatamente i rispettivi ruoli.

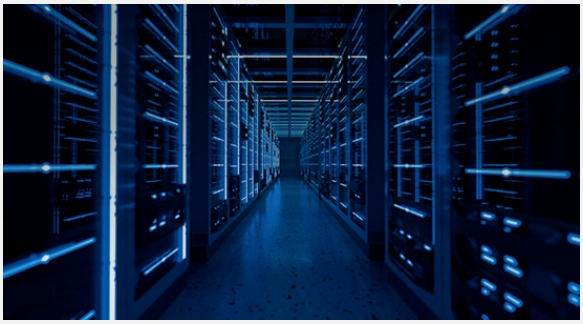
In conclusione: cosa fare per regolare correttamente la contitolarità?

Qualora si accerti che le finalità e i mezzi del trattamento sono stabiliti congiuntamente dai contitolari del trattamento, è necessario:

1. mappare tutti i trattamenti per valutare chi fa cosa e per quale scopo;
2. redigere un accordo che, da un lato, consenta ai contitolari di dimostrare il rispetto degli obblighi imposti dal GDPR e, dall'altro, fornisca informazioni generali sul trattamento congiunto, specificando in particolare l'oggetto e le finalità del trattamento, il tipo di dati personali e le categorie di interessati;
3. fornire agli interessati una descrizione essenziale del suddetto accordo, che dovrebbe essere inclusa nell'informativa sulla privacy;
4. nominare debitamente eventuali responsabili del trattamento coinvolti nel trattamento effettuato dai contitolari;
5. aggiornare il registro delle attività di trattamento ai sensi dell'articolo 30 del GDPR.

* * *

Trasferimenti di dati tra UE e Stati Uniti: Biden firma un nuovo Executive Order[4]



Lo scorso 7 ottobre, il Presidente degli USA Joe Biden ha firmato un nuovo Executive Order, indicante le misure che gli Stati Uniti adotteranno per attuare gli impegni contenuti nell'accordo di principio annunciato dalla Commissione europea e dal Governo statunitense stesso lo scorso marzo 2022.

In particolare, l'Executive Order (che, si ricorda, non è una legge, ma una direttiva interna), mira a rafforzare le garanzie a tutela della protezione dei dati personali e delle libertà civili degli interessati,

[4] Il contributo è stato realizzato per la Newsletter Norme & Tributi del mese di ottobre 2022 di AHK Italien dal Dipartimento TMT & Data Protection di Morri Rossetti.

limitando i poteri di accesso ai loro dati personali da parte delle agenzie di intelligence governative e consentendo un meccanismo di ricorso multilivello a cui possano ricorrere gli interessati stessi. L'Executive Order segue l'accordo di principio raggiunto dall'UE e dagli USA sul nuovo Trans-Atlantic Data Privacy Framework, dopo oltre due anni dall'invalidazione della decisione di adeguatezza sul Privacy Shield mediante la nota sentenza "Schrems II", e attraverso il quale il Governo statunitense si era impegnato ad implementare garanzie adeguate per una maggiore tutela dei diritti degli interessati.

L'accordo di principio era stato accolto con favore dall'EDPB, che aveva tuttavia specificato come questo non costituisse un idoneo meccanismo per il lecito trasferimento dei dati personali verso gli USA. In conseguenza di tale Executive Order, la Commissione europea ha pubblicato dei Q&A di chiarimento con indicazione degli step che seguiranno dall'adozione dell'Executive Order, annunciando altresì che inizieranno a predisporre una bozza di decisione di adeguatezza.

* * *

Per maggiori informazioni, potete contattare:

Carlo Impalà
Partner e Responsabile Dip. TMT e Data Protection
(Carlo.Impala@MorriRossetti.it)

LinkedIn

Morri Rossetti

Osservatorio

OSSERVATORIO
TMT·DATA PROTECTION
di Morri Rossetti

Morri Rossetti
Piazza Eleonora Duse, 2
20122 Milano

MorriRossetti.it
Osservatorio-dataprotection.it