DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

Il nuovo EU-U.S. Data Privacy Framework sul trasferimento di dati personali verso gli Stati Uniti

3 Agosto 2023

Stefano Mele, Partner, Gianni & Origoni
Francesco Cerciello, Associate, Gianni & Origoni

DB non solo diritto bancario

Stefano Mele, Partner, Gianni & Origoni

Francesco Cerciello, Associate, Gianni & Origoni

Stefano Mele

Stefano Mele è Partner dello studio Gianni & Origoni. Responsabile del Dipartimento di Cybersecurity e co-Responsabile del Dipartimento Privacy dello studio Gianni & Origoni. Esperto in materia di ICT, Privacy & Cybersecurity Law. Ha maturato venti anni di esperienza su questioni relative al proprio ambito di operatività e ha prestato la propria assistenza per importanti operazioni riguardanti questioni legali complesse e su più giurisdizioni in materia di nuove tecnologie e privacy, nonché su sicurezza cibernetica e crisis management a seguito di attacchi cyber. È membro del Consiglio Direttivo e Presidente della Commissione Sicurezza Cibernetica del Comitato Atlantico Italiano, oltre che Presidente del "Gruppo di lavoro sulla Cybersecurity" della Camera di Commercio americana in Italia (AmCham).

GIANNI & ORIGONI

Il 10 luglio scorso, la Commissione Europea ha adottato una nuova decisione tesa a dichiarare il livello di protezione dei dati personali offerto dagli Stati Uniti equivalente a quello dell'Unione Europea ("**Decisione**").

In altre parole, dall'11 luglio 2023, **è nuovamente ammesso il trasferimento di dati personali dall'Unione Europea alle società e alle pubbliche amministrazioni statunitensi partecipanti al c.d. "*EU-U.S. Data Privacy Framework*"** ("***Framework***") **senza l'obbligo di alcun ulteriore adempimento o garanzia** (*e.g.*, *Standard Contractual Clauses*) tra quelli attualmente previsti dal Regolamento (UE) 2016/679 ("**GDPR**").

La Decisione rappresenta un'importante *milestone* nell'ambito della tematica dei trasferimenti di dati personali tra Unione Europea e Stati Uniti. Infatti, essa non solo chiude – si spera non solo temporaneamente – tre anni di discussioni con il governo statunitense, ma supera il regime di incertezza generato dalla Corte di Giustizia dell'Unione Europea ("**CGUE**") nel caso "*Schrems II*", nel quale la Corte aveva invalidato il precedente meccanismo denominato *Privacy Shield*.

Ciò posto, alcuni accorgimenti devono essere tenuti ben in considerazione da parte delle società prima di affidarsi completamente al nuovo Framework.

1. Cosa fare prima di trasferire i dati personali verso gli Stati Uniti

L'adesione al nuovo *Framework*, infatti, si basa su un meccanismo di certificazione attraverso il quale le imprese statunitensi, tramite un'autocertificazione validata dal *Department of Commerce* ("**DoC**"), si impegnano al rispetto di alcuni principi e obblighi considerati da sempre cardinali per l'Unione europea in materia di protezione dei dati personali (*e.g.*, trasparenza, limitazione della finalità, *accountability*, etc.).

Dunque, per trasferire dati personali verso gli Stati Uniti senza ulteriori adempimenti o garanzie (ad esempio, ad un fornitore di servizi che agisce quale responsabile del trattamento) è necessario **verificare che il destinatario risulti tra le *certified organizations* inserite nella c.d. "*Data Privacy Framework List*"** ("**Elenco**").

L'Elenco, predisposto e aggiornato dal DoC[1] contiene **i riferimenti di tutte quelle imprese che hanno superato o rinnovato (in ragione dell'obbligo annuale) l'*iter* di certificazione**. In aggiunta, a maggior tutela per le imprese europee, *è possibile consultare anche* il registro delle organizzazioni rimosse dall'Elenco.

Oltre alla verifica dell'Elenco, è opportuno considerare fin da subito anche la **revisione documentale dell'organizzazione *privacy* di tutto ciò che sia collegato e riferito ai trasferimenti di dati personali verso gli Stati Uniti**. Si pensi, ad esempio, alle *privacy policy* o al registro delle attività di trattamento, o ancora, in ragione della successiva adesione al *Framework*, alla necessaria revisione di accordi sul trasferimento già stipulati con talune aziende americane (*e.g.*, *data transfer agreement*).

2. Cosa predisporre nel caso di trasferimenti di dati personali verso aziende americane che non aderiscono al Framework

Considerate le conseguenze e gli oneri che derivano dall'inclusione nel *Framework* (*e.g.*, soggezione ai poteri della *Federal Trade Commission* del *Department of Transportation*, etc.), risulterà certamente probabile, tuttavia, che alcuni trasferimenti di dati personali verso gli Stati Uniti possano non rientrare nell'ambito di applicazione della Decisione, in ragione, ad esempio, della mancata adesione da parte di determinate aziende americane.

In tal caso, **continuano a trovare applicazione le disposizioni e gli adempimenti che, a seguito di *Schrems II*, sono stati richiesti per trasferire verso gli Stati Uniti i dati personali**. In particolare, è anzitutto necessario:

- **adottare uno dei meccanismi di garanzia previsti dal GDPR** (*e.g.*, *Standard Contractual Clauses*, *Binding Corporate Rules*, etc.);
- verificare – tramite un ***transfer impact assessment*** (c.d. **TIA**) – che sia assicurato un adeguato livello di protezione dei dati personali, degli interessati e dei loro diritti.

1 Disponibile al link https://www.dataprivacyframework.gov/s/

3. Altri profili rilevanti della Decisione

In aggiunta a ciò che concerne all'adesione delle imprese americane al *Framework* e, di conseguenza, alle valutazioni rimesse alle aziende europee, *è opportuno tener conto anche degli ulteriori* principi e previsioni che sono stati introdotti dalla Decisione per garantire la conformità dei trasferimenti di dati personali alle richieste della CGUE e al livello di protezione dell'Unione europea.

In particolare, la Commissione Europea ha stabilito che:

- le **autorità pubbliche** e i **servizi di *intelligence* statunitensi** possano accedere esclusivamente ai dati personali necessari e proporzionati per le finalità perseguite (*i.e.*, persecuzione di reati federali) e che siano soggetti a specifiche condizioni e limitazioni. Ciò, coerentemente con quanto disposto dall'*executive order* del Presidente americano Biden "*Enhancing Safeguards for United States Signals Intelligence Activities*" del 7 ottobre 2022;
- siano adottati **meccanismi di ricorso e tutela dei diritti per gli interessati**, ai quali *è concessa la possibilità di sottoporre un reclamo direttamente alle imprese* aderenti al *Framework*. In alternativa, gli interessati possono rivolgersi all'organismo indipendente designato dalle imprese per la risoluzione delle controversie. Altresì, sono disposti ulteriori meccanismi di risoluzione delle controversie, sia di natura giudiziale che in forma di arbitrato. Ad esempio, per la gestione dei reclami che attengono alla violazione di leggi federali statunitensi sui servizi di *intelligence*, è stato istituto uno specifico "tribunale" (c.d. *Data Protection Review Court* o "DPRC"). In tali casi, i cittadini dell'Unione sono tenuti a depositare un'istanza presso l'Autorità Garante nazionale che, di concerto con lo European Data Protection Board, inoltra le richieste al *Civil Liberties Protection Officer* dell'*intelligence* statunitense.
- sia stabilito un **regime di *enforcement*** secondo cui le imprese aderenti al *Framework* siano sottoposte ai poteri specifici di indagine e di garanzia delle autorità statunitensi competenti (*i.e.*, *Federal Trade Commission* e DoC).

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it