protiviti®
Face the Future with Confidence

Luglio
2020

La Corte di giustizia europea dichiara invalido il Privacy Shield. Come trasferire i dati negli USA e al di fuori dell'UE?

Mercoledì 15 luglio la Corte di Giustizia dell'Unione Europea (CGUE) ha emesso la sentenza sul caso "Schrems II" (causa C-311/18 - Data Protection Commissioner v Facebook Ireland e Maximillian Schrems). Pur concludendo che le Standard Contractual Clauses (SCC) emesse dalla Commissione Europea per il trasferimento di dati personali al di fuori dell'Unione Europea sono ancora valide, la Corte ha invalidato il Privacy Shield - l'accordo che regolamenta il trasferimento di dati tra Unione europea e USA - perché è stato **ritenuto non essere adeguatamente tutelante per il diritto alla riservatezza dei cittadini europei**.

La pronuncia nasce a seguito di alcune battaglie legali da parte dell'attivista privacy austriaco Max Schrems, noto per le sue posizioni critiche sulle leggi statunitensi in materia di sorveglianza e sui rapporti tra Facebook e il governo degli Stati Uniti.

Il tema della sorveglianza da parte delle autorità americane è stato portato all'attenzione anche dalle rivelazioni di Edward Snowden, che ha reso pubblici i numerosi programmi di sorveglianza globale gestiti dalla NSA (National Security Agency degli Stati Uniti). L'inclusione dei dati dei cittadini europei in questi programmi ha portato alla prima apparizione di Schrems nel 2015 davanti alla CGUE. Schrems ha sostenuto con successo che le politiche sulla privacy adottate da Facebook non forniscono una "protezione adeguata" dei diritti fondamentali della privacy come richiesto dall'articolo 25 (trasferimento dei dati personali) della Direttiva europea in materia di protezione dei dati all'epoca vigente.

Adottando una posizione in favore di Schrems, la CGUE in passato aveva già invalidato il Safe Harbor, il precedente accordo per disciplinare il trasferimento dei dati personali dall'UE agli Stati Uniti.

In sostituzione del Safe Harbor, sono stati avviati dei negoziati tra UE e Stati Uniti per l'approva-zione, avvenuta nel 2016, di un nuovo accordo: il Privacy Shield UE-USA. Nonostante gli sforzi per migliorare il nuovo accordo e renderlo adatto per fornire un'adeguata protezione dei dati dell'UE secondo quanto richiesto dalla normativa europea, esso è stato oggetto di critiche fin dalla sua approvazione, anche da parte di membri delle Autorità Garanti europee per la protezione dei dati.

Nel 2019, Schrems si è trovato ancora una volta di fronte alla CGUE, questa volta per mettere in discussione l'efficacia del Privacy Shield, anch'esso invalidato dalla recente sentenza, che crea delle ripercussioni in generale sui meccanismi di trasferimento di dati.

Cosa significa la sentenza per le imprese che trasferiscono dati personali al di fuori dell'UE?

A seguito della sentenza Schrems II, che ha effetti immediati, le imprese che trasferiscono dati personali al di fuori dell'UE devono assicurare che tali trasferimenti garantiscano in concreto le stesse garanzie previste dal GDPR. In altre parole, i meccanismi messi a disposizione dal GDPR per trasferire i dati, come SCC o Binding Corporate Rules (**BCR**, le norme vincolanti d'impresa), non possono essere utilizzati senza una preventiva analisi sull'adeguatezza degli standard normativi del Paese in cui si vogliono esportare i dati personali.

Come chiarito anche nelle FAQ rilasciate dall'EDPB (**European Data Protection Board**, l'organo composto da tutti i garanti europei che ha preso il posto del Working Party 29):

1. L'invalidazione del Privacy Shield ha effetto immediato. Dunque, tutti i trasferimenti di dati verso gli Stati Uniti che erano basati su tale meccanismo sono da considerarsi illeciti. Ad oggi, sono **più di 5.000 le aziende statunitensi** di diverse dimensioni che **non possono più fare affidamento sul Privacy Shield** per trasferire i dati personali dall'UE agli Stati Uniti.

2. Anche fornire **l'accesso ai dati da un Paese extra-europeo**, ad esempio a fini amministrativi, equivale a un trasferimento.

3. Le aziende che esportano dati personali al di fuori dell'UE devono:

    - Comprendere se la normativa del Paese ricevente preveda **standard di protezione dei dati personali** in linea con quelli garantiti dal Regolamento Europeo sulla protezione dei dati personali (**GDPR**). Ad esempio, uno dei parametri su cui basare tale valutazione è l'esistenza nell'ordinamento del Paese di destinazione di diritti privacy effettivi e azionabili anche in sede amministrativa e giudiziaria, come ad esempio la possibilità di esercitare il diritto di accesso rispetto ai dati trattati da un'autorità pubblica del Paese di destinazione. Nel caso degli Stati Uniti, la CGUE ha già dichiarato che le leggi statunitensi non assicurano un livello di protezione del dato sufficiente.

    - Nel caso in cui la normativa del Paese ricevente non preveda standard di protezione adeguati e si intenda comunque effettuare il trasferimento, comprendere se - adottando **misure aggiuntive** (legali, tecniche organizzative) rispetto al meccanismo di trasferimento che si intende utilizzare (come, ad esempio, le **SCC** o le **BCR**) - si sia in grado di assicurare un livello di protezione adeguato. A tal proposito l'EDPB ha dichiarato che fornirà chiarimenti sulle tipologie di misure che potrebbero essere adottate in aggiunta alle SCC e BCR.

    - **Interrompere il trasferimento** di dati o, in alternativa, **comunicare** all'Autorità Garante competente il trasferimento, nel caso in cui non sia possibile garantire standard adeguati di protezione dei dati personali neanche con l'ausilio di misure aggiuntive alle SCC o BCR.

4. Gli obblighi derivanti dalla sentenza Schrems II si applicano anche ai trasferimenti tra responsabili del trattamento e sub-responsabili.

Come possono possono fare le aziende per fronteggiare questa situazione?

1. Condurre un'analisi volta a:
    - Identificare i trasferimenti di dati personali al di fuori dell'UE e, per ciascuno di essi, la tipologia di meccanismo di trasferimento utilizzata. L'analisi ovviamente deve essere condotta su tutti i trasferimenti extra-UE, non solo quelli verso gli Stati Uniti.
    - Comprendere se la normativa del Paese ricevente preveda standard di protezione dei dati personali in linea con quelli garantiti dal GDPR.
2. Stabilire una strategia per gestire i trasferimenti di dati verso Paesi al di fuori dell'UE sulla base dei contenuti della sentenza, coinvolgendo il DPO (se nominato) o l'ufficio competente per la gestione delle tematiche privacy. Ad esempio:
    - Valutare la possibilità di migrare i dati personali a cui si applica il GDPR su basi dati gestite all'interno dell'UE o in un Paese con una decisione di adeguatezza favorevole da parte della Commissione UE (ad esempio, Canada, Giappone, ecc.), tenuto conto della revisione delle modalità di accesso ai dati e dei relativi permessi.
    - Identificare e rivedere (se necessario) tutti i contratti che implicano un trasferimento di dati personali oltre i confini europei, tenendo in considerazione anche i Paesi dove vengono archiviati i dati e identificando il meccanismo più adeguato.
    - Per i trasferimenti che si vogliono basare sulle SCC o BCR, valutare di rafforzare tali clausole per garantire in concreto una protezione dei dati sostanziale. Tra i punti di miglioramento delle clausole, si potrebbe ad esempio prevedere l'adozione di misure di sicurezza a protezione del trasferimento, come misure di crittografia *end-to-end*.
3. Verificare se sia necessario aggiornare le informative privacy relativamente al meccanismo utilizzato per trasferire i dati personali al di fuori dell'UE.

* * *

Come può aiutare Protiviti?

Protiviti, grazie al suo team multidisciplinare di professionisti specializzati sulle tematiche Privacy & Data Protection, può aiutare le aziende ad affrontare questo importante cambiamento nella gestione dei dati personali attraverso diverse modalità di supporto, come ad esempio:

1. Mappare i trasferimenti di dati personali extra-UE avendo come base di partenza il registro dei trattamenti predisposto dall'azienda.
2. Aiutare l'azienda a decidere, caso per caso, se il trasferimento è necessario e - in caso positivo - il migliore meccanismo di trasferimento.
3. Aggiornare il registro dei trattamenti e le informative privacy, ove necessario.
4. Supportare l'azienda nel valutare il livello di compliance privacy interno per identificare eventuali aree di miglioramento.

5. Supportare l'azienda nel valutare il livello di compliance privacy dei fornitori che importano dati al di fuori dell'UE, anche al fine di comprendere se il trasferimento dei dati preveda adeguate misure di sicurezza.

6. Disegnare processi e soluzioni tecniche per monitorare e gestire i trasferimenti di dati personali, inclusa l'implementazione di misure di sicurezza.

* * *

Contatti

Enrico Ferretti – *Managing Director*

enrico.ferretti@protiviti.it

Andrea Gaglietto – *Senior Manager*

andrea.gaglietto@protiviti.it

Stefano Micci – *Manager*

stefano.micci@protiviti.it