L'evoluzione degli accordi sul trasferimento dati tra Unione Europea e Stati Uniti

10 settembre 2024

AUTORI

Aurora Agostini
Partner

Giulietta Minucci
Counsel

Jessica Giussani
Associate

L'evoluzione normativa del trasferimento dati UE-USA riflette la crescente rilevanza della protezione dei dati nell'era digitale: in questo articolo analizziamo gli sviluppi più recenti, inclusi la decisione di adeguatezza 2023 e le FAQ 2024, e come queste norme cercano di a bilanciare gli scambi di dati internazionali con la salvaguardia del diritto alla *privacy*.

▼ ▼ ▼

DALL'ACCORDO *SAFE HARBOUR* AL *PRIVACY SHIELD*

Il percorso verso un quadro normativo stabile per il trasferimento dei dati tra UE e USA è stato caratterizzato da diversi ostacoli e revisioni. Questo iter riflette la crescente importanza attribuita alla protezione dei dati personali e le differenze tra gli approcci normativi delle due sponde dell'Atlantico.

Safe Harbour (2000-2015). L'accordo Safe Harbour, adottato nel 2000, rappresentava il primo tentativo di creare un framework per il trasferimento dei dati personali tra UE e USA. Questo accordo permetteva alle aziende americane di autocertificarsi, dichiarando di aderire a principi di protezione dei dati simili a quelli europei. Tuttavia, le crescenti preoccupazioni sulla sorveglianza di massa da parte delle agenzie di intelligence statunitensi portarono a un esame critico di questo accordo.

Sentenza Schrems I (2015). La svolta si ebbe con la sentenza Schrems I della Corte di Giustizia dell'Unione Europea (CGUE) nell'ottobre 2015. Maximillian Schrems, un attivista austriaco per la privacy, contestò il trasferimento dei suoi dati da Facebook Ireland a Facebook Inc. negli USA. La CGUE dichiarò invalido l'accordo Safe Harbour, sostenendo che non forniva una protezione adeguata contro l'accesso indiscriminato ai dati personali da parte delle autorità statunitensi.

Privacy Shield (2016-2020). In risposta alla sentenza Schrems I, l'UE e gli USA negoziarono rapidamente un nuovo accordo: il *Privacy Shield*, adottato nel 2016. Questo *framework* mirava a garantire una maggiore protezione dei dati personali dei cittadini europei trasferiti negli USA, imponendo obblighi più stringenti alle aziende americane e limitazioni all'accesso ai dati da parte delle autorità pubbliche statunitensi. Il *Privacy Shield* includeva anche meccanismi di ricorso per i cittadini europei e la nomina di un mediatore negli USA per gestire i reclami relativi all'accesso ai dati da parte delle agenzie di intelligence.

Sentenza Schrems II (2020). Nonostante i miglioramenti introdotti dal *Privacy Shield,* persistevano dubbi sulla sua efficacia: nel luglio 2020, la CGUE, con la sentenza Schrems II (Causa C-311/18), invalidò anche il Privacy Shield. La Corte ritenne che le leggi statunitensi sulla sorveglianza non fornissero ancora garanzie sufficienti per la protezione dei dati dei cittadini europei, in particolare riguardo al principio di proporzionalità nell'accesso ai dati da parte delle autorità pubbliche.

Conseguenze e soluzioni temporanee. L'invalidazione del Privacy Shield creò notevoli incertezze per le aziende che trasferivano dati tra UE e USA. In risposta, l'European Data Protection Board (EDPB) emise nel 2020 le raccomandazioni 01/2020, fornendo linee guida alle società per il trasferimento dei dati in assenza di una decisione di adeguatezza. Queste includevano l'uso di clausole contrattuali standard (SCC) e l'implementazione di misure supplementari per garantire un livello di protezione equivalente a quello dell'UE.

Questa serie di eventi ha evidenziato la complessità e l'importanza di trovare un equilibrio tra la libera circolazione dei dati, essenziale per il commercio internazionale, e la protezione dei diritti fondamentali alla *privacy* dei cittadini europei; ha anche sottolineato la necessità di un approccio più robusto e duraturo al trasferimento transoceanico dei dati, che ha portato agli sviluppi più recenti come la decisione di adeguatezza del 2023 e le FAQ del 2024, di cui *infra*.

LA DECISIONE DI ADEGUATEZZA DEL LUGLIO 2023

Il 10 luglio 2023 ha segnato una svolta decisiva nel dialogo transatlantico sulla protezione dei dati personali. In questa data, la Commissione Europea ha adottato la decisione di adeguatezza per l'EU-US Data Privacy Framework (DPF), aprendo un nuovo capitolo nella complessa storia dei trasferimenti di dati tra l'Unione Europea e gli Stati Uniti. Questa misura rappresenta il culmine di anni di negoziati e revisioni, mirando a stabilire un delicato equilibrio tra la necessità di trasferimenti di dati fluidi e la tutela dei diritti fondamentali dei cittadini europei.

Il DPF introduce un quadro normativo più robusto e affidabile rispetto ai suoi predecessori: le società americane che aderiscono a questo *framework* sono ora tenute a rispettare standard di protezione dei dati più elevati, basati sui principi cardine di proporzionalità e necessità. Questi principi si estendono anche alle autorità di intelligence americane, il cui accesso ai dati provenienti da Paesi terzi è stato significativamente regolamentato. In particolare, l'Executive Order 14086, firmato dal Presidente Biden nell'ottobre 2022, ha introdotto nuove salvaguardie per le attività di intelligence statunitensi, inclusa la creazione di un meccanismo di ricorso indipendente per i cittadini dell'UE.

Un aspetto particolarmente innovativo del DPF è la sua applicazione semplificata per le società incluse nella Data Privacy Framework List. Per queste entità, la decisione di adeguatezza si applica automaticamente, eliminando la necessità di

implementare ulteriori misure di sicurezza. Questa semplificazione promette di ridurre notevolmente gli oneri burocratici e i costi associati al trasferimento di dati transoceanico; tuttavia, il *framework* mantiene una certa flessibilità: le società non presenti nella lista possono comunque effettuare trasferimenti di dati, pur dovendo fornire garanzie aggiuntive ai sensi dell'articolo 46 del GDPR.

La Commissione Europea, consapevole della natura dinamica del panorama digitale, ha incorporato un meccanismo di revisione nella decisione: dopo il primo anno dalla sua entrata in vigore, il DPF sarà sottoposto a un'attenta valutazione per verificarne l'efficacia e l'adeguatezza agli obiettivi prefissati. Questo approccio proattivo dimostra l'impegno delle istituzioni europee nel mantenere elevati standard di protezione dei dati, adattandosi al contempo alle evoluzioni tecnologiche e geopolitiche.

L'adozione del DPF va oltre la mera conformità normativa: rappresenta un importante passo avanti nella ricerca di un terreno comune tra gli approcci europeo e americano alla protezione dei dati e riflette gli sforzi congiunti per costruire un *framework* che rispetti sia le esigenze di sicurezza nazionale degli Stati Uniti che gli elevati standard di *privacy* dell'UE. In un'epoca in cui i dati sono diventati il nuovo petrolio dell'economia digitale, questa decisione di adeguatezza mira a fornire alle imprese la certezza giuridica necessaria per operare in un contesto globale sempre più interconnesso, senza compromettere i diritti fondamentali degli individui.

Nonostante l'ottimismo che circonda il DPF, numerosi esperti hanno sollevato preoccupazioni significative sulla sua solidità giuridica, prefigurando potenziali sfide legali simili a quelle che hanno portato all'invalidazione dei precedenti accordi. Max Schrems, l'attivista per la privacy che ha già contestato con successo il Safe Harbor e il Privacy Shield, ha espresso scetticismo sulla capacità del DPF di resistere a un esame approfondito da parte della Corte di Giustizia dell'Unione Europea (CGUE), evidenziando la presenza di gravi criticità:

- nonostante le modifiche apportate dall'Executive Order 14086, alcuni esperti ritengono che le leggi statunitensi sulla sorveglianza, come la Sezione 702 del FISA, continuino a consentire una raccolta di dati su larga scala che potrebbe essere considerata sproporzionata secondo gli standard UE;
- sebbene il DPF introduca un nuovo meccanismo di ricorso, questo potrebbe non soddisfare pienamente i requisiti di indipendenza e imparzialità richiesti dalla CGUE nella sentenza Schrems II;
- imentre il DPF introduce il concetto di "necessità e proporzionalità" nella raccolta dei dati, l'interpretazione di questi principi potrebbe differire significativamente tra UE e USA;

- c'è preoccupazione che futuri cambiamenti nell'amministrazione statunitense possano alterare l'implementazione o l'interpretazione dell'Executive Order, minando potenzialmente le basi del DPF.

La solidità del DPF è dunque destinata ad essere messa alla prova non solo nella sua implementazione pratica, ma anche nel suo fondamento giuridico: la sua capacità di resistere a potenziali contestazioni legali sarà cruciale per garantire una stabilità a lungo termine nei flussi di dati tranfrontalieri e per mantenere la fiducia sia delle imprese che dei cittadini europei.

NUOVE LINEE GUIDA PER IL TRASFERIMENTO DEI DATI PERSONALI

A quasi un anno di distanza dall'adozione del DPF, il 16 luglio 2024, l'European Data Protection Board (EDPB) ha pubblicato una serie di FAQ volte a chiarire l'ambito di applicazione del DPF e fornire indicazioni concrete a individui e imprese sul processo di valutazione dell'adeguatezza dei trasferimenti di dati.

Requisiti per le imprese statunitensi. Per aderire al DPF, le imprese statunitensi devono soddisfare criteri specifici:

- sottoporsi al controllo della US Federal Trade Commission e del Dipartimento dei Trasporti;
- rinnovare annualmente un'autocertificazione, includendo tutte le categorie di dati rilevanti;
- essere inserite in un elenco pubblico di adesione al DPF.

Nel caso di gruppi societari, è necessaria una specifica estensione del certificato della capogruppo alle controllate.

Ruoli delle imprese nel trattamento dei dati. Le imprese statunitensi possono agire sia come titolari che come responsabili del trattamento dei dati:

- come titolari, devono garantire una base giuridica adeguata per il trattamento, in conformità con l'art. 6 del GDPR;
- come responsabili, devono operare secondo un accordo congiunto conforme all'articolo 28 del GDPR, fornendo tutte le informazioni necessarie al titolare e gestendo i dati secondo le istruzioni ricevute.

Diritti dei cittadini europei e meccanismi di reclamo. L'EDPB fornisce chiarimenti (ed i *link* alla documentazione necessaria) su come i cittadini europei possano esercitare i propri diritti nell'ambito del DPF:

- possibilità di presentare reclami in caso di violazioni, sia direttamente all'azienda interessata che tramite le autorità nazionali per la protezione dei dati (DPA);
- due scenari di gestione dei reclami: (a) un panel informale di DPA dell'UE per questioni relative ai dati raccolti nell'ambito di rapporti di lavoro, ovvero (b) Il rinvio alle autorità statunitensi competenti per altri casi.

CONCLUSIONE E PROSPETTIVE FUTURE

L'introduzione del DPF e le successive FAQ pubblicate dall'EDPB segnano un importante passo avanti nella regolamentazione dei flussi di dati transoceanici. Tuttavia, questi sviluppi portano con sé sia opportunità che sfide significative per le imprese e i responsabili della protezione dei dati.

Le FAQ ci ricordano chiaramente che l'applicazione del DPF non è universale, ma richiede una valutazione caso per caso. Questa flessibilità, se da un lato permette di adattare il *framework* a diverse situazioni, dall'altro impone alle organizzazioni un'attenta analisi dei propri flussi di dati e delle proprie pratiche: le imprese dovranno sviluppare competenze interne o affidarsi a esperti esterni per navigare efficacemente questo nuovo panorama normativo.

Il DPF e le relative FAQ rappresentano uno strumento prezioso per la compliance GDPR nei trasferimenti di dati verso gli USA: offrono una base più solida per le aziende che operano su entrambe le sponde dell'Atlantico, riducendo l'incertezza giuridica che ha caratterizzato gli anni precedenti. Tuttavia, la conformità rimane un processo dinamico che richiede un monitoraggio continuo e adattamenti in risposta all'evoluzione della giurisprudenza e delle interpretazioni normative.

È imperativo che le imprese verifichino tempestivamente la conformità e la trasparenza dei loro flussi transfrontalieri di dati. Questo processo dovrebbe includere:

- una revisione approfondita delle attuali *policy* sul trasferimento dati;
- l'aggiornamento delle valutazioni d'impatto sulla protezione dei dati (DPIA);
- la modifica delle procedure interne per allinearle ai requisiti del DPF;
- la formazione del personale sulle nuove normative e procedure.

In conclusione, mentre il DPF e le FAQ associate forniscono una guida preziosa, il vero test sarà nella sua implementazione pratica e nella sua capacità di adattarsi alle sfide future: le organizzazioni che adotteranno un approccio proattivo e flessibile alla protezione dei dati saranno meglio posizionate per navigare con successo in questo complesso panorama normativo, trasformando potenziali ostacoli in opportunità di crescita e innovazione.

AUTORI

Aurora Agostini
Partner

Giulietta Minucci
Counsel

Jessica Giussani
Associate