LA PRIMA REVISIONE DEL DATA PRIVACY FRAMEWORK UE-USA

12 novembre 2024

AUTORI

Aurora Agostini
Partner

Giulietta Minucci
Counsel

Jessica Giussani
Associate

Giovanni Lombardi
Associate

Il 4 novembre 2024, l'European Data Protection Board (EDPB) ha pubblicato il suo primo rapporto sulla revisione periodica del **Data Privacy Framework (DPF)**, il nuovo accordo che disciplina i trasferimenti di dati personali tra l'Unione Europea e gli Stati Uniti. Questo *framework*, adottato dalla Commissione Europea il 10 luglio 2023, rappresenta un tentativo di superare le criticità sollevate dalla Corte di Giustizia dell'Unione Europea nelle sentenze *Schrems I* e *Schrems II*, che avevano invalidato i precedenti accordi Safe Harbour e Privacy Shield.

Aspetti commerciali del DPF

Sul fronte dell'implementazione commerciale, il Dipartimento del Commercio statunitense ha dimostrato un impegno significativo nel primo anno di operatività del *framework*: al momento della revisione, oltre 2800 organizzazioni risultavano attivamente certificate sotto il DPF, mentre più di 1100 si erano ritirate e 2600 erano elencate come inattive per mancato rinnovo della certificazione. Questa situazione ha sollevato interrogativi sulla gestione dei dati personali da parte delle organizzazioni inattive, considerando che il *framework* richiede loro di specificare se i dati ricevuti vengono restituiti, cancellati o conservati, con l'obbligo di continuare ad applicare i principi del DPF in quest'ultimo caso.

L'EDPB ha evidenziato come i meccanismi di ricorso indipendenti (*Independent Recourse Mechanism* - IRM) abbiano ricevuto un numero sorprendentemente basso di reclami ammissibili nel primo anno, con solo nove casi registrati, principalmente relativi a richieste di cancellazione o accesso ai dati. Questa scarsa attività di reclamo, unita all'assenza di verifiche d'ufficio sostanziali sulla conformità, ha portato l'EDPB a sollecitare un'intensificazione delle attività di controllo proattivo da parte delle autorità statunitensi.

La questione dei dati HR continua a rappresentare un punto di divergenza significativo tra le interpretazioni europee e americane: mentre il Dipartimento del Commercio USA ha tradizionalmente limitato la definizione di "dati HR" al trattamento dei dati dei dipendenti all'interno dello stesso gruppo aziendale, l'EDPB sostiene una interpretazione più ampia, che include qualsiasi dato personale relativo a un dipendente nel contesto di un rapporto di lavoro, indipendentemente dal fatto che il trasferimento avvenga all'interno di un gruppo

societario o verso un operatore commerciale diverso.

Accesso governativo ai dati

Un aspetto fondamentale della revisione ha riguardato l'implementazione dell'Executive Order (EO) 14086, che introduce importanti salvaguardie per l'accesso ai dati da parte delle autorità pubbliche statunitensi. L'EDPB ha riconosciuto l'aggiornamento delle politiche interne delle agenzie di intelligence per incorporare i principi di necessità e proporzionalità, pur sottolineando l'importanza di monitorarne attentamente l'applicazione pratica attraverso esempi concreti nelle prossime revisioni.

La recente riautorizzazione della sezione 702 del Foreign Intelligence Surveillance Act (FISA) attraverso il Reform Intelligence And Securing America Act (RISAA) ha introdotto modifiche significative, tra cui l'espansione della definizione di "fornitore di servizi di comunicazione elettronica": questa modifica, secondo le autorità statunitensi, mira a includere una specifica categoria di aziende precedentemente esclusa, ma la sua formulazione ampia ha sollevato preoccupazioni sulla potenziale estensione della sorveglianza.

Se il primo Privacy Shield era caduto per le sue debolezze sostanziali, il DPF rischia di inciampare sulla sua complessità procedurale

Un progresso significativo è rappresentato dall'istituzione della Data Protection Review Court (DPRC), con la nomina di otto giudici e due special advocates. Tuttavia, al momento della revisione, nessun reclamo era stato presentato attraverso questo nuovo meccanismo di ricorso, rendendo impossibile valutarne l'efficacia pratica; la revisione annuale del meccanismo da parte del Privacy And Civil Liberties Oversight Board (PCLOB) è ancora in sospeso.

Nuove sfide e prospettive future

Una questione emergente di particolare rilevanza riguarda l'acquisizione di dati personali da *broker* commerciali da parte delle agenzie di intelligence USA, una pratica non coperta dalle garanzie dell'EO 14086. Questo fenomeno richiede un'attenta valutazione dell'impatto sulla protezione dei dati e un monitoraggio approfondito delle pratiche di utilizzo, potenzialmente seguito da interventi normativi specifici.

Guardando al futuro, l'EDPB ha raccomandato che la prossima revisione avvenga entro tre anni, anziché quattro, per permettere una valutazione tempestiva dell'efficacia dei controlli sulla conformità e dell'esperienza pratica nella gestione dei reclami. Particolare attenzione dovrà essere dedicata agli sviluppi relativi alla Sezione 702 FISA, la cui prossima riautorizzazione è prevista tra due anni.

Per le organizzazioni che utilizzano il DPF, queste conclusioni suggeriscono l'importanza di prepararsi a controlli più rigorosi sulla conformità sostanziale e di

prestare particolare attenzione alle pratiche di trasferimento successivo dei dati e al trattamento dei dati HR.

Conclusione

La prima revisione del Data Privacy Framework evidenzia una dinamica che chi si occupa di *privacy* conosce bene: la distanza tra teoria e pratica nella protezione dei dati personali. Da un lato, il framework presenta sulla carta significativi miglioramenti rispetto ai suoi predecessori, con un apparato di garanzie formalmente robusto. Dall'altro, i numeri raccontano una storia diversa: migliaia di aziende che abbandonano la certificazione, pochissimi reclami presentati, una corte (la DPRC) ancora inutilizzata.

Viene da chiedersi se non stiamo assistendo alla creazione di un'architettura giuridica sempre più sofisticata ma potenzialmente disconnessa dalla realtà operativa delle imprese e dalle effettive esigenze di tutela degli interessati. Il vero successo del DPF non si misurerà sulla carta, ma nella sua capacità di diventare uno strumento vivo ed efficace per la protezione dei diritti fondamentali nel contesto dei flussi di dati transatlantici: la prossima revisione, auspicabilmente tra tre anni, ci dirà se questa sfida è stata vinta o se saremo di fronte all'ennesimo caso di *privacy on paper*.

Per un'analisi più approfondita sugli sviluppi normativi del trasferimento dati tra UE e USA, rimandiamo al nostro precedente articolo sul tema: https://www.lexia.it/2024/09/11/accordi-ue-usa/

AUTORI

Aurora Agostini

Partner

Giulietta Minucci

Counsel

Jessica Giussani

Associate

Giovanni Lombardi

Associate