

# Alert

## Privacy - Review

### Trasferimenti extra-UE dei dati

#### LA SITUAZIONE DI STALLO PER LE IMPRESE ESPORTATRICI

Le imprese che per il proprio *business* necessitano di trasmettere i dati personali trattati verso Paesi al di fuori dell'UE (*rectius*, dello Spazio Economico Europeo), si trovano al momento a fronteggiare la difficoltà del gestire legittimamente tali trasferimenti, a seguito della ormai nota sentenza “*Schrems II*” della Corte di Giustizia UE che ha invalidato il *Privacy Shield* e dell'applicazione estensiva di tale sentenza avallata dalle istituzioni europee di settore che non hanno finora fornito una risposta univoca e operativa a fronte del *vulnus* verificatosi.

Far ricadere infatti sulle imprese complesse valutazioni in merito alle garanzie offerte dai Paesi terzi destinatari dei dati le onera di una *probatio diabolica* circa la conformità al GDPR delle scelte aziendali anche in relazione ai *tool* e ai *provider* globali di cui si servono e che tali trasferimenti utilizzano, provider che spesso vengono percepiti come essenziali e, di fatto, insostituibili anche in virtù della loro posizione di *leadership* sul mercato, ponendo di fatto le imprese di fronte all'unica alternativa di rinunciarvi onde evitare la violazione della disciplina in materia di protezione dei dati.

#### Strumenti previsti dal GDPR per i trasferimenti dei dati extra-SEE.

La materia dei trasferimenti dei dati è disciplinata dal Capo V del GDPR (artt. 44-50) ove è previsto, in sintesi, che si possa procedere legittimamente al trasferimento dei dati personali verso quei Paesi non appartenenti allo SEE (composto da UE + Norvegia, Liechtenstein, Islanda) che:

- 1) siano coperti da una decisione di adeguatezza della Commissione europea che ha valutato a monte che tali Paesi garantiscono un livello di protezione dei dati, delle libertà e dei diritti fondamentali adeguato e sostanzialmente equivalente a quello garantito dal GDPR all'interno dell'UE, essendo pertanto possibile trasferirvi dati personali senza ulteriori adempimenti. Al momento risultano “adeguati” Andorra, Argentina, Canada, Faer Oer, Giappone, Guernsey, Isola di Man, Israele, Jersey, Nuova Zelanda, Svizzera e Uruguay. Rientrano nella medesima lista anche gli USA mediante lo strumento del Privacy Shield sino alla sentenza Schrems, con le implicazioni analizzate a seguire;
- 2) pur in assenza di decisioni di adeguatezza, qualora i soggetti esportatori e i loro destinatari in tali Paesi abbiano adottato garanzie adeguate di natura contrattuale o pattizia fra cui sono annoverate le norme vincolanti di gruppo d'impresa (le c.d. BCR) e le clausole contrattuali standard (SCC) adottate dalla Commissione UE, oltre ai codici di condotta e ai meccanismi di certificazione ancora inapplicati. Si aggiungono, benché non di immediata utilizzabilità in quanto soggette ad una

# Alert

## Privacy - Review

individuale previa autorizzazione da parte del Garante anche le clausole contrattuali ad hoc frutto di negoziazione tra le parti;

- 3) pur in assenza di ogni altro presupposto, in quei casi in cui si possano applicare le deroghe al divieto di trasferimento solo in presenza di specifiche e raramente verificabili circostanze (ad esempio il consenso esplicito di ogni singolo interessato che si stato specificamente informato dei rischi del trasferimento per i propri dati).

Gli strumenti pertanto sinora più diffusamente utilizzati per legittimare i trasferimenti dei dati extra-SEE sono stati le decisioni di adeguatezza, ivi incluso il Privacy Shield per gli USA, le SCC che avevano il vantaggio di poter essere semplicemente sottoscritte e allegate ai contratti commerciali cui accedevano e, più limitatamente, le BCR.

### **Applicabilità principi Schrems II a tutti gli strumenti pattizi**

In virtù della decisione di adeguatezza della Commissione UE nei confronti degli USA sulla base l'accordo Privacy Shield del 2016 siglato tra le autorità UE e il Governo Statunitense, alle imprese era consentito trasferire regolarmente i dati personali dall'Europa agli USA essendo a tal fine sufficiente verificare che l'impresa importatrice fosse regolarmente iscritta nel registro tenuto dal Dipartimento del Commercio USA.

La stabilità dei flussi è stata travolta dalla sentenza 16 luglio 2020 nella causa C-311/18 (Schrems II) della Corte di Giustizia UE (CGUE) che ha invalidato il Privacy Shield avendo accertato che la normativa statunitense non fornisce in realtà un livello di protezione sostanzialmente equivalente a quello dell'Unione - il che costituiva il presupposto della decisione di adeguatezza - e ciò in particolare a causa del grado di ingerenza creato dai programmi di sorveglianza previsti dalla normativa statunitense (quelli fondati sull'articolo 702 del FISA e sull'E.O. 12333) nei diritti fondamentali delle persone i cui dati sono oggetto di trasferimento.

La stessa CGUE tuttavia, come confermato anche dalle FAQ del 23 luglio 2020 dello European Data Protection Board (EDPB), non limita la propria valutazione alla sola decisione di adeguatezza, dichiarando applicabili i medesimi principi a qualsiasi trasferimento di dati verso gli USA, quindi anche alle SCC e alle BCR di cui sopra.

### **Processo valutativo richiesto alle imprese esportatrici**

Premesso che il processo valutativo previsto dalla CGUE per i trasferimenti di dati verso gli USA si applica a qualsiasi paese terzo, la Corte, in questo avallata dall'EDPB, ha sostanzialmente posto in capo alle imprese esportatrici dei dati (con il supporto eventuale delle importatrici) il compito di verificare il rispetto, nel paese terzo, del livello di protezione equivalente a quello richiesto nell'UE con specifico esame della normativa locale non solo in materia di protezione dei dati ma anche di

# Alert

## Privacy - Review

sicurezza e sorveglianza da parte delle autorità locali, al fine di determinare se le garanzie previste dalle SCC o dalle BCR possano essere rispettate nella pratica. Diversamente, sarà necessario che le imprese valutino la possibilità di applicare “misure supplementari” che possano impedire di fatto le ingerenze e l’accesso indiscriminato ai dati eventualmente consentiti dal diritto del paese terzo. Qualora nemmeno così si possa dire raggiunto un livello di protezione equivalente, i trasferimenti devono essere immediatamente sospesi e l’unica soluzione è negoziare un emendamento o una clausola supplementare al contratto al fine di vietare i trasferimenti verso tali Paesi.

Nonostante la Corte stessa abbia suggerito un intervento collaborativo delle autorità in seno all’EDPB per garantire approcci coerenti, e la stessa EDPB si fosse riproposta interventi operativi, finora l’unico supporto proposto è rappresentato dalle *Raccomandazioni relative alle misure supplementari* del 10 novembre 2020, peraltro non ancora formalmente adottate dall’EDPB a seguito della consultazione pubblica.

Tali Raccomandazioni appaiono tuttavia di limitata utilità per le imprese in quanto, se da un lato suggeriscono alcuni rimedi tecnologici, organizzativi e contrattuali utili a trasferire i dati in una forma tale da garantire l’impossibilità per le autorità del paese terzo di avere accesso a dati riconducibili a persone identificate/ibili (per esempio con la cifratura in caso di servizio di mero backup), d’altro lato espressamente ammettono – in relazione al caso ben più diffuso di trasferimento a fornitori di servizi cloud o ad altri provider che richiedono l’accesso ai dati in chiaro – di non “*essere in grado di prevedere una misura tecnica efficace*” laddove “*il potere concesso alle autorità pubbliche del paese destinatario di accedere ai dati trasferiti va oltre quanto necessario e proporzionato in una società democratica*” pur non escludendo che “*l’ulteriore sviluppo tecnologico possa offrire misure in grado di conseguire gli scopi commerciali previsti, senza richiedere l’accesso in chiaro*”.

È evidente come l’onere economico e commerciale di tale incertezza gravi al momento solo sulle singole imprese esportatrici dei dati ritenute responsabili della valutazione di legittimità di tali trasferimenti.

### Conclusioni

In virtù dei summenzionati gravosi oneri valutativi che incombono sulle imprese esportatrici dei dati (anche in termini di costi correlati al reperimento e analisi delle informazioni rilevanti sui sistemi normativi/democratici dei Paesi terzi) che non consentono più, di fatto, di utilizzare direttamente le SCC e le BCR, possono ormai considerarsi come efficacemente utilizzabili per i trasferimenti le sole decisioni di adeguatezza verso i Paesi dell’elenco di cui al punto 2 sopra, eccetto, per l’appunto, gli Stati Uniti d’America.

Almeno per gli USA, che rappresentano senz’altro la più ricorrente destinazione del trasferimento, la più urgente soluzione auspicabile potrebbe essere quella di ordine diplomatico/politico che consenta

# Alert

## Privacy - Review

l'adozione di una nuova decisione di adeguatezza da parte della Commissione UE che sostituisca - rafforzandone i cardini e risolvendone le criticità - il Privacy Shield.

Analoga soluzione di ordine politico è stata d'altronde preferita di recente anche per legittimare i trasferimenti verso Sud-Korea (la cui bozza di decisione di adeguatezza è prossima all'adozione formale, terminata la fase dei negoziati politici il 30 marzo 2021) e UK in era post-Brexit (per la quale il procedimento che porterà a decisione di adeguatezza risulta avviato in data 19 febbraio 2021), soluzione che appare auspicabile - in un contesto di sempre maggiore circolazione globale dei dati ormai necessaria anche per le piccole e medie imprese locali che si servono di provider su scala globale - anche nei confronti degli altri Paesi maggiormente impattati dai trasferimenti e tuttavia non ancora coperti da decisioni di adeguatezza.

Sembrerebbe peraltro che una soluzione realmente operativa e organica non possa provenire nemmeno dall'attesa revisione delle SCC (i cui testi non risultano ancora formalmente adottati dalla Commissione UE a seguito della chiusura della consultazione pubblica) essendo pur sempre ivi previsto che le parti che decidano di integrarle nei propri accordi commerciali siano obbligate a garantire di *“non avere motivo di ritenere che le leggi del paese terzo di destinazione applicabili al trattamento dei dati personali da parte dell'importatore di dati, inclusi eventuali requisiti di divulgazione dei dati personali o misure che autorizzano l'accesso da parte delle autorità pubbliche, impediscano all'importatore l'adempimento dei propri obblighi ai sensi delle presenti clausole”*.

In assenza di soluzioni operative individuate a livello politico dagli organi istituzionali, non può essere infatti rimesso ai privati, mediante iniziative contrattuali individuali, l'affrontare e risolvere tematiche politiche internazionali inerenti gli assetti politici e democratici di Paesi terzi, gravandole altresì del connesso rischio commerciale e sanzionatorio derivante dalla descritta situazione di stallo.

28.04.2021

**La presente Newsletter ha il solo scopo di fornire aggiornamenti e informazioni di carattere generale. Non costituisce pertanto un parere legale né può in alcun modo considerarsi come sostitutivo di una consulenza legale specifica.**

**Laura Sini, Associate**  
**E:** l.sini@nmlex.it  
**T.:** +39 02 657 5181

**Per chiarimenti o informazioni potete contattare l'autore oppure il Vostro Professionista di riferimento all'interno dello Studio.**

[www.nunziantemagrone.it](http://www.nunziantemagrone.it)