LO SCUDO UE - USA PER LA PRIVACY ("PRIVACY SHIELD")

FAQ PER LE IMPRESE EUROPEE

(Gruppo di lavoro Articolo 29 – WP245 del 13 dicembre 2016)

1. Che cos'è il *Privacy Shield*?

Il *Privacy Shield*,[1] ovvero lo "scudo per la privacy" fra UE e USA, è un meccanismo di autocertificazione per le società stabilite negli USA che intendano ricevere dati personali dall'Unione europea. In particolare, le società si impegnano a rispettare i principi in esso contenuti e a fornire agli interessati (i.e. ovvero tutti i soggetti i cui dati personali siano stati trasferiti dall'Unione europea) adeguati strumenti di tutela, pena l'eliminazione dalla lista delle società certificate ("Privacy Shield List") da parte del Dipartimento del Commercio statunitense e possibili sanzioni da parte della *Federal Trade Commission* (Commissione federale per il commercio). La Commissione europea ha ritenuto che esso offra un livello adeguato di protezione per i dati personali trasferiti da un soggetto nell'UE a una società stabilita negli Stati Uniti che disponga di tale autocertificazione e che, pertanto, lo *Shield* costituisca una fonte di garanzie giuridiche con riguardo ai trasferimenti di dati in questione.

Per maggiori informazioni si possono consultare le pagine seguenti:

- La decisione di adeguatezza pubblicata sulla Gazzetta Ufficiale dell'Unione europea
- La Guida al *Privacy Shield* pubblicata dalla Commissione europea
- Il sito dedicato al *Privacy Shield* e curato dal *Department of Commerce* (Ministero del commercio) degli USA

2. Quali società statunitensi possiedono i requisiti per aderire al *Privacy Shield*?

Hanno il diritto di presentare un'autocertificazione ai sensi del *Privacy Shield* le società stabilite negli USA che sono soggette ai poteri di controllo e di accertamento della *Federal Trade Commission* (FTC, Commissione federale per il commercio) o del *Department of Transportation* (DoT, Ministero dei trasporti). Non è escluso che in futuro questa possibilità sia estesa a imprese soggette al controllo di altri organismi federali. Per esempio, allo stato, organismi no-profit, banche, assicurazioni e fornitori di servizi di telecomunicazione (per quanto riguarda le loro attività di *common carrier*, ossia di vettori di comunicazioni

[1] La decisione relativa all'adeguatezza dello schema denominato *Privacy Shield* Ue-USA ("Privacy Shield" ovvero "Schema") è stata adottata dalla Commissione europea il 12 luglio 2016. Con essa la Commissione e il Ministero del commercio USA hanno inteso sostituire la decisione di adeguatezza sul *Safe Harbor* (2000/520/CE), che era stata invalidata dalla Corte di giustizia dell'Ue il 6 ottobre 2015.

conto terzi) non sono soggetti alla giurisdizione della FTC o del DoT e, pertanto, non possono presentare autocertificazioni ai sensi del *Privacy Shield.*

Il *Privacy Shield* è applicabile a tutte le categorie di dati personali trasferiti dall'UE agli USA, compresi informazioni commerciali, dati sanitari o relativi alle risorse umane, purché la società USA destinataria di tali dati abbia autocertificato la propria adesione allo schema.

Per maggiori informazioni, si può consultare il sito https://www.privacyshield.gov/.

3. Cosa occorre fare prima di trasferire dati personali a una società con sede negli USA che risulti certificata ai sensi del *Privacy Shield*, ovvero affermi di esserlo?

Prima di trasferire dati personali a una società stabilita negli USA che affermi di essere certificata ai sensi del *Privacy Shield*, una società europea deve accertarsi che la società USA disponga di una certificazione ancora attiva (la certificazione è soggetta a rinnovo annuale) e che tale certificazione copra i dati in questione (in particolare: dati relativi alle risorse umane, ovvero dati non relativi alle risorse umane).

Per verificare se una certificazione sia attiva e applicabile, occorre consultare la *Privacy Shield List*, ossia l'elenco delle società certificate ai sensi del *Privacy Shield*, pubblicato sul sito del Ministero del commercio USA (https://www.privacyshield.gov/welcome).

L'elenco comprende tutte le società stabilite negli USA che hanno completato la procedura di autocertificazione con esito positivo. L'elenco fornisce, inoltre, informazioni sulle categorie di dati personali alle quali si applica la certificazione fornita dalla singola società (dati relativi alle risorse umane o altri dati), nonché sui servizi offerti da quest'ultima.

L'elenco gestito dal Ministero del commercio USA comprende, in una diversa sezione, anche società che non sono più coperte dal *Privacy Shield*. Queste società non possono ricevere dati personali relativi a soggetti dell'UE nell'ambito della decisione di adeguatezza, essendo cessata la loro adesione allo schema, ma sono tenute a continuare ad applicare i principi stabiliti nello *Shield* ai dati che siano stati loro trasferiti durante il precedente periodo di adesione.

Ai fini del trasferimento di dati personali a società stabilite negli USA che non aderiscono o hanno cessato di aderire al *Privacy Shield* si possono utilizzare altri strumenti ritenuti validi nell'UE, come le norme vincolanti d'impresa o le clausole contrattuali tipo adottate dalla Commissione europea.

L'adesione al *Privacy Shield* da parte della società destinataria dei dati stabilita negli USA permetterà alle società europee di rispettare le norme di diritto nazionale che recepiscono l'articolo 25 della direttiva 95/46/CE (art. 44 del Codice in materia di protezione dei dati personali - d. lgs. n. 196/2003; nel prosieguo "Codice"); tuttavia, restano pienamente vigenti in capo alle società esportatrici di dati tutti gli altri obblighi fissati dalla legislazione nazionale in materia di protezione dei dati.

- Trasferimenti di dati a società stabilite negli USA operanti in qualità di titolari di trattamento

Prima di trasferire dati personali, una società europea operante in qualità di titolare del trattamento deve assicurarsi che il trasferimento sia conforme alla legislazione applicabile in materia di protezione dei dati. In

primo luogo, una società europea può trasferire dati personali a una società stabilita negli USA esclusivamente se, a monte, il trattamento alla base del trasferimento trova una base giuridica nelle disposizioni del diritto nazionale che recepiscono gli articoli 7 e 8 della direttiva 95/46/CE (cfr. artt. 23, 24 e 26 e 27 del Codice). Inoltre, anche con riferimento ai dati che si intende trasferire, sarà necessario rispettare tutti gli altri obblighi derivanti, in via generale, dalla legislazione UE in materia di protezione dei dati: principio di limitazione della finalità, proporzionalità, qualità dei dati, obblighi di trasparenza nei confronti degli interessati. In particolare, in caso di trasferimento dei dati a una società stabilita negli USA e munita di idonea certificazione, la società europea dovrà informare gli interessati dell'identità dei soggetti destinatari dei loro dati nonché della circostanza che i dati in questione beneficiano della tutela offerta dal *Privacy Shield*.

E' opportuno ricordare che il trasferimento di dati personali da parte di una società europea verso altre società extra-UE o extra-SEE potrebbe comunque incontrare limitazioni laddove previste da specifiche clausole contrattuali commerciali inserite negli accordi con le rispettive controparti.

- Trasferimenti di dati a società stabilite negli USA operanti in qualità di responsabili del trattamento

Nel caso di una società stabilita nell'UE che, in qualità di titolare del trattamento, trasferisca dati a un responsabile stabilito negli USA incaricato di trattare tali dati per suo conto, l'art. 17 della direttiva 95/46/CE (recepito nell'ordinamento italiano attraverso l'art. 29 del Codice) prescrive che i rapporti fra le due società siano disciplinati da un contratto per quanto riguarda le operazioni di trattamento dati, indipendentemente dall'adesione al *Privacy Shield* da parte della società USA (responsabile del trattamento).

La stipula di un contratto è necessaria allo scopo di garantire che il responsabile stabilito negli USA assuma una serie di impegni:

- agire esclusivamente sulla base delle istruzioni del titolare;
- prevedere idonee misure tecniche e organizzative a tutela dei dati personali dalla distruzione accidentale o illecita ovvero dalla perdita o alterazione accidentali e dalla comunicazione o dall'accesso non autorizzati, e avere contezza dell'ammissibilità di eventuali trasferimenti ulteriori.[2] Tenendo conto dello stato dell'arte e dei costi di attuazione, le suddette misure di sicurezza garantiscono un livello di sicurezza adeguato al rischio che il trattamento comporta nonché alla natura dei dati oggetto di tutela; e
- assistere il titolare nel dare riscontro alle richieste di accesso ai propri dati personali presentate dai singoli interessati, tenendo conto della natura del trattamento.

Si osservi che, in base alla direttiva 95/46/CE, il diritto nazionale dei diversi Stati membri può prevedere ulteriori requisiti come, per esempio, l'obbligo per l'impresa UE di inserire informazioni aggiuntive nei contratti relativi alle attività di trattamento dati. Ai sensi dell'art. 29, commi 4 e 5, del Codice, il titolare del trattamento stabilito in Italia deve specificare analiticamente e per iscritto i compiti affidati al responsabile e, anche tramite verifiche periodiche, lo stesso è tenuto a vigilare sulla puntuale osservanza delle disposizioni in materia di trattamento dei dati e delle proprie istruzioni.

[2] Per maggiori informazioni relativamente ai trasferimenti ulteriori effettuati da responsabili stabiliti negli USA, si veda il paragrafo "Contratti obbligatori per i trasferimenti ulteriori" nel testo del *Privacy Shield* e la risposta alla domanda n. 4.

Per esempio, è opportuno che la società europea specifichi se sia ammessa la nomina di sub-incaricati del trattamento da parte del responsabile negli USA e, in caso affermativo, a quali condizioni (in termini di trasparenza e riparto di responsabilità). Inoltre, potrebbe essere utile per la società europea ottenere rassicurazioni in merito alla notifica di violazioni della sicurezza oltre alla sottoscrizione di specifici impegni sulla cancellazione dei dati una volta risolto il contratto di servizi.

4. **Dove si possono reperire informazioni sull'adesione al *Privacy Shield* da parte di società stabilite negli USA che sono controllate di aziende europee?**

Per maggiori informazioni sull'adesione al *Privacy Shield* da parte di società stabilite negli USA che sono controllate di aziende europee, si può consultare la pagina relativa sul sito del DoC degli USA: https://www.privacyshield.gov/article?id=U-S-Subsidiaries-of-European-Businesses-Participation-in-Privacy-Shield .

L'elenco delle società che aderiscono al *Privacy Shield* è disponibile sul sito del DoC degli USA: https://www.privacyshield.gov/welcome. Il DoC ha pubblicato anche una Guida alla procedura di autocertificazione: https://www.privacyshield.gov/article?id=How-to-Join-Privacy-Shield-part-1.