TLS Newsletter

Mercoledì 24 agosto 2016

Per maggiori informazioni: info.tls@it.pwc.com

Privacy: dai Porti agli Scudi

di Michele Giuliani e Chiara Verri

La Commissione Europea (la "Commissione") e il Governo degli Stati Uniti hanno raggiunto, il 2 febbraio 2016, un nuovo accordo che consentirà il trasferimento dei dati personali a fini commerciali tra i rispettivi territori.

Solo il 12 luglio 2016, a seguito al parere favorevole reso del Gruppo dell'Articolo 29, la Commissione ha completato la procedura di adozione del nuovo accordo denominato EU – US Privacy Shield (il "Nuovo Accordo" o l' "Accordo" o "Privacy Shield").

Da sempre le due aree geografiche, quella americana e quella europea, hanno condiviso l'obiettivo di rafforzare la tutela della privacy adottando tuttavia diversi meccanismi e approcci a difesa degli stessi.

Al fine di colmare queste divergenze, rendere il contesto normativo più chiaro e facilitare lo scambio dei dati, la Commissione con Decisione 00/520/CE del 26 luglio 2000, (la "Decisione") aveva individuato un protocollo, denominato Safe Harbour, sviluppato dall'*US State Department*, in collaborazione con Parlamento e Consiglio Europeo.

Il Safe Harbour era destinato unicamente ad organizzazioni americane che ricevevano dati personali dall' Unione Europea, al fine di permettere loro di ottemperare al principio di "approdo sicuro" ed alla presunzione di "adeguatezza" che esso comportava a tutela degli interessati d'oltreoceano.

Infatti, le Autorità privacy dell'Unione Europea ritenevano le organizzazioni americane "adeguate" per la conservazione ed il trasferimento dei dati personali solo dietro apposita autocertificazione che ne attestasse il rispetto dei principi posti a base dell'accordo.

Privacy: from the Harbours to the Shields

As well know, on October 6, 2015, the European Court of Justice issued its judgment about the invalidity of the so called Safe Harbour, the protocol destined only to U.S. organizations receiving personal data from the European Union.

Until such a declaration, the EU Privacy Authorities considered "adequate", for the storage and the transfer of the personal data, exclusively the U.S. organizations that certified the compliance of the founding principles of the protocol with an appropriate self-certification.

However, in an economy increasingly characterized by the use of technology, the transfer of data appears as essential also for sectors different from the internet economy, such as insurance, pharmaceutical, manufacturing, hospitality and food service.

Also in light of the reasons mentioned above, on February 2, 2016, the European Commission and the U.S. Government reached an agreement on a new framework for transatlantic exchanges of personal data: the EU-U.S. Privacy Shield.

The Commission has finalized the adoption procedure of this agreement on the subsequent July 26.

The new self-certification system, on the one hand, reinforces the duties required by the previously protocol and, on the other hand, establishes additional limits and guarantees for the access of the US Authorities to the European personal data.

L'adesione a tali principi poteva essere limitata in presenza di: 1) esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia; 2) disposizioni legislative, regolamentari ovvero decisioni giurisdizionali purché l'organizzazione americana dimostrasse che il mancato rispetto dei principi da parte sua era limitata al soddisfacimento di interessi di ordine superiore; 3) eccezioni o deroghe previste dalle direttive o dalla legislazione degli Stati membri

D'altro canto, le società europee, prima di procedere alla conclusione di un contratto che comportasse il conseguente affidamento dei dati negli Stati Uniti, avevano l'onere di verificare che le loro interlocutrici americane rientrassero effettivamente nella *Safe Harbour List* e ne avessero recepito concretamente i principi.

Di conseguenza, l'organizzazione americana doveva essere in grado di fornire e garantire: 1) l'appartenenza volontaria alla *Safe Harbour List*; 2) livelli tecnologici adeguati al fine di sostenere appropriate misure di sicurezza dei dati; e 3) la disponibilità a dimostrare in qualunque momento i propri impianti di trattamento dei dati.

Lo scorso 6 ottobre l'equilibrio raggiunto con il *Safe Harbour* è venuto meno.

La Corte di Giustizia dell'Unione Europea (Grande Sezione) (la "Corte") con sentenza del 6 ottobre 2015 - Causa C-362-14 ha, infatti, invalidato tale meccanismo di tutela del trasferimento dei dati personali oltreoceano.

La Corte, tra l'altro, aveva a riguardo osservato come la *Federal Trade Commission* non avesse effettivamente proceduto ad una constatazione dell'adeguatezza dei dati personali garantiti dagli Stati Uniti come richiesto dalla Direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995 relativa alla "*tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*", ma si fosse limitata esclusivamente a valutare e considerare sufficiente il sistema del Safe Harbour.

L'invalidazione del *Safe Harbour* non ha comportato solo conseguenze giuridiche legate al rispetto o alla violazione della sfera privata degli individui, ma ha avuto anche un significativo impatto sull'economia digitale di migliaia di società, europee e americane.

Negli Stati Uniti il *Safe Harbour* ha, infatti, rappresentato, in termini di *digital industry*, un importante approdo per molti investitori esteri in Europa e nel nostro Paese.

Molto spesso, quando si parla di trasferimento e utilizzo di dati, si fa riferimento alle società della *Internet economy* e dell'*Information Technology*; tuttavia, in un'economia sempre più caratterizzata dall'utilizzo della tecnologia, il trasferimento e l'utilizzo di dati è diventato fondamentale anche per altri settori, quali quello assicurativo, farmaceutico, manifatturiero, dell'*hospitality* e della ristorazione.

Il rapporto commerciale transatlantico, il più consistente a livello mondiale, si basa anche sull'efficacia e la sicurezza dei dati, permettendo alle società europee di impiegare servizi disponibili solo nel "nuovo continente", rendendo più efficiente la propria struttura produttiva.

Per tali ragioni, vista l'importanza sia per l'Unione Europea che per gli Stati Uniti del libero trasferimento dei dati personali, la Commissione ed il Governo americano hanno raggiunto un nuovo accordo.

Il Privacy Shield impone maggiori obblighi alle società americane con il fine di garantire massima tutela ai dati personali europei.

Vera Jourova, Commissaria per la Giustizia, i consumatori e la parità di genere, ha definito il Nuovo Accordo "*un sistema nuovo e solido che offre agli europei la protezione dei dati personali e alle imprese la certezza del diritto. Rafforza le norme sulla protezione dei dati, che saranno fatte rispettare più rigorosamente, offre garanzie riguardo all'accesso da parte delle autorità pubbliche e semplifica per le singole persone le possibilità di ricorso in caso di reclamo (...)*".

Più precisamente, dal 1° agosto 2016 le aziende americane possono autocertificare al *US State Department* il rispetto del Nuovo Accordo.

Il Privacy Shield, analogamente al Safe Harbour, opera attraverso un sistema di autocertificazione.

Le organizzazioni americane, che intendono avvalersi dell'Accordo, devono attestare la loro *compliance* ai principi per la protezione dei dati personali stabiliti nell'ambito del Privacy Shield (i "Principi").

Molti di essi erano stati già precedentemente inseriti nel Safe Harbour, ma sono stati oggi notevolmente perfezionati, rendendo l'Accordo molto più solido di quanto precedentemente convenuto.

In particolare, i Principi riguardano:

1) "*Notice*". Gli obblighi informativi sono più severi rispetto a quelli in vigore per il Safe Harbour.

Mentre il Safe Harbour richiedeva alle imprese autocertificatrici di fornire informazioni generiche sul processo di acquisizione dei dati personali, *the notice principle* è molto più specifico e richiede informazioni dettagliate su 13 aspetti differenti. Le imprese, infatti, devono dichiarare e/o fornire:

- la loro partecipazione al Privacy Shield;
- il tipo di dati personali raccolti;
- l'impegno a trattare tutti i dati personali che ricevono dall'Unione Europea nel rispetto dei Principi;
- lo scopo del trattamento e le informazioni sul loro utilizzo;
- indicazioni sui contatti attraverso il quale è possibile richiedere informazioni o inviare reclami;
- terzi a cui si forniscono i dati personali e lo scopo per cui ciò è fatto;
- il diritto degli interessati di accedere ai propri dati personali;
- le alternative che l'impresa offre per limitare l'uso e la rivelazione dei loro dati personali;
- l'indicazione dell'organo indipendente predisposto alla risoluzione delle controversie, a cui si può ricorrere gratuitamente per proporre ricorsi;
- di essere soggetti ai poteri di indagine e di applicazione di un organo statutario autorizzato e prescritto dagli Stati Uniti;
- la possibilità, a certe condizioni, per gli interessati, di richiedere l'arbitrato obbligatorio;
- i requisiti per la trasmissione dei dati personali in risposta alle eventuali richieste legittime da parte delle autorità pubbliche;
- la propria responsabilità nel caso di trasferimenti successivi a terzi.

2) "*Choice* ". I "*Choice Principle*", che sono sostanzialmente rimasti invariati rispetto a prima, prevedono che la persona interessata ha il diritto di scegliere e, quindi, di manifestare il proprio consenso , tra i vari processi di trattamento dei dati in cui risulta coinvolto.

3) *"Accountability for Onward Transfer"*. È previsto che il trasferimento dei dati personali, da un'impresa americana verso terzi, possa avvenire solo per specifiche e limitate finalità, a condizione che sia garantito lo stesso livello di protezione previsto nel Privacy Shield.

4) "*Security* ". I requisiti in materia di sicurezza sono rimasti immutati. Le imprese autocertificatrici devo adottare misure appropriate per proteggere i dati da eventuali danni, smarrimenti e accessi non autorizzati, rivelazioni, alterazione e distruzione.

5) "*Data Integrity and Purpose Limitation* ". Sotto la vigenza del Safe Harbour l'obbligo era quello di dover limitare le attività sui dati allo stretto necessario per lo scopo preposto e di astenersi da porre in essere attività incompatibili con lo scopo per cui i dati personali erano stati inizialmente raccolti o per lo scopo per cui successivamente gli interessati ne avevano prestato il consenso.

Oggi, con il Privacy Shield, le imprese americane devono rispettare i Principi per tutto il tempo in cui trattano i dati personali e sono obbligati a rispettarli anche successivamente.

6) "*Access* ". I principi in materia di accesso ai dati restano essenzialmente gli stessi. I soggetti titolari dei dati trattati devono avere l'accesso alle informazioni che l'impresa possiede e devono poter correggere, rettificare o cancellare queste informazioni quando sono inaccurate, inesatte, o quando sono state acquisite in violazione dei Principi.

7) "*Recourse, Enforcement and Liability* ". Questi aspetti sono stati notevolmente rafforzati con il Privacy Shield che ha introdotto nuovi meccanismi di ricorso. In particolare, gli interessati avranno il diritto di presentare reclami:

- direttamente all'organizzazione americana, la quale deve garantire un meccanismo di risoluzione efficace. (la risposta, non solo dovrà pervenire entro un periodo di 45 giorni, ma dovrà contenere una valutazione della fondatezza della protesta e le informazioni sulle possibili modalità di risoluzione);
- agli organi indipendenti adibiti alla risoluzione delle controversie (ADR);
- all'Autorità Europea per la protezione dei dati personali;

- allo *US Department of Commerce*, impegnato a risolvere le controversie nascenti a causa di imprese americane che non rispetteranno i Principi imposti dal Privacy Shield; e
- ad un arbitrato vincolante del "*Privacy Shield Panel*" composto da almeno 20 arbitri designati dallo *US Department of Commerce* e dalla Commissione Europea.

Il Nuovo Accordo rivolge l'attenzione principalmente al settore commerciale e alle autorità pubbliche degli Stati Uniti.

Al fine di garantire maggiore trasparenza lo *US State Department* mette a disposizione un elenco pubblico delle organizzazioni (*Privacy Shield List*) che hanno certificato la loro adesione ai Principi. La certificazione dovrà essere aggiornata ogni anno; in caso contrario si procederà alla rimozione dalla lista del nominativo delle organizzazioni che non hanno proceduto in questo senso.

Per la prima volta, inoltre, l'accesso delle autorità americane ai dati personali europei è soggetto a stringenti limiti e maggiori garanzie.

A riguardo, i cittadini europei avranno la possibilità di interpellare un *Ombudsperson* (difensore civico), nel caso in cui ritengano che le organizzazioni americane in possesso dei loro dati non abbiamo gestito le loro richieste in modo appropriato.

Infine, è stati implementato un monitoraggio congiunto del funzionamento dell'Accordo tra la Commissione e il *Department of Commerce* USA con l'eventuale supporto dei servizi di *intelligence* americane e delle Autorità europee per la protezione dei dati.

Infatti, è previsto un *summit* annuale rivolto al contestuale aggiornamento degli sviluppi in materia di privacy in Europa e negli Stati Uniti, con la conseguente relazione pubblica della Commissione che dovrà essere trasmessa al Consiglio Europeo e al Parlamento in merito ai risultati raggiunti in sede di revisione.

Possiamo quindi concludere che ora i dati dei cittadini europei sono realmente al sicuro? Purtroppo, una risposta certa, al momento non può essere data.

Il Privacy Shield, infatti, è un accordo dalla struttura dinamica. Gli strumenti e le novità annunciate implicheranno ulteriori passaggi legislativi, ma soprattutto organizzativi che, con ogni probabilità, non saranno di facile e pronta approvazione e applicazione.

Attendiamo, comunque, le prime verifiche da parte degli organismi preposti già nel corso del 2017.