STEFANELLI & STEFANELLI STUDIO LEGALE

AREA PRIVACY

APPROFONDIMENTO A CURA DELL' AVV. DELLI PONTI

I DATI POSSONO CIRCOLARE LIBERAMENTE PER IL MONDO?

Le regole previste dal GDPR per una circolazione sicura in ogni Paese e non solo nei Paesi dell'Unione Europea

Grazie allo sviluppo dell'economia e soprattutto delle tecnologie, oggi, quantità strabilianti di dati circolano da un paese all'altro.

Questo è stato uno dei motivi che ha spinto l'Unione Europea ad aggiornare i contenuti della Direttiva 95/46/CE sulla protezione dei dati. La circolazione sicura del dato all'interno dei paesi UE, ma anche in paesi extra UE è uno degli obiettivi del GDPR, fondamentale per consentire l'operatività del mercato e delle tecnologie.

Quello che molto spesso può capitare nelle aziende: un fornitore di cloud con server extra UE, un fornitore di un bene che ha sede extra UE che per produrre un certo bene ha bisogno dei dati dell'utilizzatore finale (un manufatto protesico per esempio), una applicazione web di un fornitore che salva dati in un Paese diverso dall'Unione Europea, ecc.

In tutti questi casi: come fare per trasferire il dato rispettando il GDPR?

La regola generale, prevista anche dalla Direttiva 95/46/CE, è che: il trasferimento transfrontaliero di dati personali è vietato (art. 44).

Tale regola è, ovviamente, mitigata da alcune circostanze al ricorrere delle quali il trasferimento diventa lecito.

Il trasferimento, infatti, è ammesso solo nei seguenti casi:

1. la Commissione abbia deciso che il paese terzo o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato (art. 45)

2. il titolare o il responsabile del trattamento possono effettuare il trasferimento in presenza di garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi (art. 46)

3. come ultimo criterio, che trova applicazione in mancanza di una decisione di adeguatezza della Commissione o della predisposizione di garanzie adeguate, l'articolo 49 del GDPR prevede una serie di deroghe e condizioni che, a prescindere dal livello di protezione dei dati personali apprestato, consentono il trasferimento extra UE di dati personali.

Vediamole nel dettaglio al fine di rispondere a quesito apparentemente semplice: ***come posso trasferire dei dati verso un'azienda di un Paese extra UE?***

1. TRASFERIMENTO SULLA BASE DI UNA DECISIONE DI ADEGUATEZZA

Il criterio principale previsto dal GDPR affinché possa effettuarsi un trasferimento "cross-border" è l'adozione da parte della Commissione di una decisione di adeguatezza, così come enunciato dall'articolo 45.

La Commissione, quindi, dovrà verificare se, nel contesto extra europeo, il livello di protezione dei dati è "adeguato", ovvero equivalente a quello previsto dalle disposizioni europee. Per compiere tale valutazione la Commissione dovrà tenere in considerazione una serie di criteri, elencati all'interno del Regolamento, come lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti, gli impegni internazionali che il paese terzo o l'organizzazione internazionale hanno assunto ecc.

Quello che si vuole garantire, tramite queste decisioni della Commissione, è la certezza del diritto e l'uniformità in tutta l'Unione dei rapporti nei confronti del paese terzo o dell'organizzazione internazionale.

La Commissione, inoltre, dovrebbe prevedere un riesame periodico del funzionamento delle decisioni di adeguatezza assunte, con una particolare attenzione rivolta a quelle adottate sulla base degli articoli 25 e 26 della direttiva 95/46/CE. Le decisioni di adeguatezza erano, infatti, una idonea base giuridica per il trasferimento dati in Paese extra UE già con la direttiva 95/46.

Nel caso in cui la Commissione decida che un paese terzo o un'organizzazione internazionale non garantiscono più un livello adeguato di protezione, il trasferimento di dati personali dovrà considerarsi vietato, a meno che non siano presenti garanzie adeguate. In questo particolare frangente di pervenuta "inadeguatezza", la Commissione deve avvisare tempestivamente il paese terzo o l'organizzazione internazionale per avviare delle consultazioni volte a risolvere la situazione.

Sul sito del Garante è possibile verificare se il Paese verso cui si intende trasferire il dato ha una legislazione "adeguata" in base ad una decisione della Commissione
Vai al sito

Il delicato caso del trasferimento dati in USA

E se devo trasferire i dati in USA?

Il 6 ottobre del 2015 la Corte di Giustizia dell'Unione Europea ha emesso sentenza sulla Causa C-362/14 (Maximillian Schrems vs Data Protection Commissioner), dichiarando invalida la decisione della Commissione Europea che stabiliva l'adeguatezza della legislazione europea il c.d. "Safe Harbour" (Decisione 520/2000/CE).

Il caso esaminato dalla Corte riguardava un reclamo di Maximillian Schrems, un utente austriaco di Facebook, presentato all'Autorità garante della privacy irlandese in cui affermava che, alla luce delle rivelazioni fatte da Edward Snowden in merito alle attività dei servizi di intelligence statunitensi, le leggi degli Stati Uniti non offrissero sufficiente protezione dalla sorveglianza attuata dalle pubbliche autorità sui dati trasferiti negli USA. L'autorità irlandese archiviò il reclamo, asserendo, in particolare, che con la Decisione Safe Harbour la Commissione Europea avesse già verificato che, nell'ambito del programma Safe Harbour, gli Stati Uniti assicurassero un adeguato livello di protezione.

Il caso fu rimesso alla Corte Suprema irlandese, la quale, in sede di rinvio pregiudiziale, chiese alla Corte di Giustizia se, a seguito di un reclamo presentato da un cittadino, la Decisione Safe Harbour della Commissione impedisse effettivamente all'Autorità garante irlandese di verificare autonomamente il livello di protezione dei dati offerto dagli Stati Uniti d'America.

La Corte di Giustizia rispose che l'esistenza di una decisione della Commissione, secondo la quale un paese terzo assicura un adeguato livello di protezione dei dati personali, non può né

escludere né ridurre i poteri delle Autorità garanti nazionali. Pertanto, anche se la Commissione ha adottato una propria decisione, le Autorità nazionali, allorquando ricevano un reclamo da parte di un cittadino, devono poter valutare in completa indipendenza se il trasferimento dei dati in un paese terzo soddisfi i requisiti previsti dalla Direttiva.

La decisione della Corte creò non pochi problemi visto l'enorme traffico di dati verso gli USA.

Per tale ragione "a tempo record" la Commissione europea ha adottato il 12 Luglio 2016 una nuova decisione che regolamenta il trasferimento di dati tra Unione europea e USA, il cosìdetto "Privacy Shield".

Il Privacy Shield, 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 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.

Il trasferimento dati verso un'azienda negli USA deve essere preceduto dalla verifica che la stessa azienda americana sia certificata.
Verifica sul sito del Privacy Shield
In caso negativo dovranno applicarsi le altre condizioni per il trasferimento

2. TRASFERIMENTO A SEGUITO DI GARANZIE ADEGUATE

Qualora il Paese in cui si intende trasferire il dato rientri in una decisione di adeguatezza della Commissione, il titolare del trattamento è tranquillo. Ma se il Paese non rientra in quelli per i quali è presente una decisione di adeguatezza?

La normativa offre altri strumenti, le così dette garanzie adeguate (art. 46 GDPR) ovvero dei meccanismi che garantiscono che il dato sarà trattato in conformità ai principi della normativa dell'Unione Europea.

Clausole contrattuali standard di protezione dei dati

Le Clausole contrattuali standard sono una sorta di "*model law*" da applicare per regolamentare il trasferimento dati da un Paese UE ad un Paese extra UE.

Già previste dalla Direttiva 95/46/CE, le clausole contrattuali standard non richiedono un'autorizzazione preventiva delle autorità di vigilanza. Le clausole contrattuali standard esistenti possono rimanere valide, ma il GDPR lascia aperta la possibilità di una loro abrogazione.

Clausole contrattuali redatte ad hoc possono essere utilizzate per garantire e rafforzare la conformità al GDPR. Tali clausole, però, dovranno ricevere un'approvazione preventiva dell'autorità di vigilanza.

Le clausole contrattuali standard da utilizzare per il trasferimento da titolare a responsabile sono visionabili qui

per il trasferimento da titolare a titolare si vedano i seguenti documenti
Document 32001D0497
Document 32004D0915

Codici di condotta e meccanismi di certificazione

L'articolo 49 del GDPR elenca due nuove opportune garanzie: i codici di comportamento e i meccanismi di certificazione.

I codici di comportamento sono programmi di autoregolamentazione usati per dimostrare che l'azienda aderisce a determinati standard sulla privacy.

Secondo il GDPR tali codici di comportamento possono essere creati da entità terze o da organismi che rappresentano gli interessi di titolari dei dati. Possono essere elaborati per affrontare molti aspetti del GDPR ivi compresi i trasferimenti internazionali di dati.

L'adesione a questi codici di comportamento da parte delle aziende che non sono soggette alla regolamentazione ma che sono coinvolte nel trasferimento dei dati personali al di fuori dell'UE, aiuterà quest'ultime a dimostrare che sono state adottate delle adeguate garanzie nella gestione delle informazioni.

I codici di comportamento formulati devono essere presentati all'autorità di vigilanza appropriata per l'approvazione ai sensi dell'articolo 38. Un organismo accreditato e competente può, a norma dell'articolo 41, controllare l'osservanza di un codice di condotta.

Possono essere sviluppate certificazioni di protezione dei dati, sigilli e marchi, registrati al livello dell'Unione, per dimostrare l'adesione ad alcuni standard. Come i codici di condotta, la certificazione è disponibile per un utilizzo da parte di soggetti esterni all'UE, a condizione che dimostrino, mediante contratti o altri strumenti legali, la loro volontà di aderire alle garanzie di protezione dei dati.

Come descritto negli articoli 42 e 43, i meccanismi di certificazione, i sigilli e i marchi richiedono un'ulteriore azione da parte del comitato europeo per la protezione dei dati. È in fase di studio la realizzazione di un marchio europeo comune che certificherà l'adesione agli standard fondanti della direttiva.

Attualmente non risultano certificazioni o codici in tal senso.

Disposizioni specifiche per le Binding Corporate Rules ("BCR")

Il GDPR, a differenza della "Direttiva sulla Protezione dei Dati 95/46/CE", elenca in modo esplicito le BCR e ne attribuisce una garanzia di adeguatezza all'articolo 46 e prevede le modalità dettagliate per i trasferimenti tramite BCR di cui all'articolo 47.

Tale disposizione precisa che le BCR richiedono l'approvazione di un'autorità di vigilanza in conformità al meccanismo di coerenza di cui all'articolo 63 e disciplinano le regole minime che devono essere incluse.

Le regole minime di condotta dovranno considerare le informazioni di contatto per il gruppo interessato, le informazioni sui processi di dati e di trasferimento, le norme che si applicano principi generali di protezione dei dati, le procedure di reclamo e i meccanismi di conformità.

L'articolo 4, paragrafo 20, definisce che anche un gruppo di imprese che svolgono un'attività economica congiunta può utilizzare la stessa struttura di regole per i trasferimenti internazionali di dati.

Se si intende utilizzare le BCR il documento base per la richiesta di approvazione di una BCR resta il WP 133 del Gruppo di lavoro articolo 29

Per conoscere i riferimenti di ulteriori documenti applicabili e i dettagli della procedura è possibile consultare questo link

3. LE ULTIME DEROGHE

E se con nessuno dei meccanismi sopra riportati si è riuscito ad avere la base giuridica necessaria per trasferire i dati nel Paese extra UE l'articolo 49 del GDPR prevede una "ultima" serie di deroghe e condizioni che, a prescindere dal livello di protezione dei Dati personali apprestato, consentono il trasferimento extra UE di Dati personali.

Le deroghe sono generalmente parallele a quelle della "Direttiva sulla Protezione dei Dati 95/46/CE" con l'inserimento di una nuova deroga per i trasferimenti considerati di "legittimo interesse".

Il trasferimento è ammesso se si verifica una delle seguenti condizioni :

- l'interessato ha espressamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di tali trasferimenti per l'interessato a causa dell'assenza di una decisione di adeguatezza e di adeguate misure di salvaguardia,
- il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato;
- il trasferimento sia necessario per importanti motivi di interesse pubblico;
- il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
- il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può essere consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri.

Naturalmente qualora si scelga di utilizzare una di queste deroghe si consiglia di dare evidenza di ciò nel registro dei trattamenti o in altro documento interno che dia atto della base giuridica utilizzata.

A conclusione della disamina sopra effettuata si precisa che se nessuna delle deroghe descritte può essere utilizzata è consigliabile non effettuare il trasferimento dati e utilizzare un altro fornitore.

Infatti, una delle implicazioni più significative del GDPR è che, a differenza di quanto disposto dalla "Direttiva sulla Protezione dei Dati 95/46/CE", il mancato rispetto delle disposizioni internazionali di trasferimento dei dati può comportare sanzioni fino a 20.000.000 di Euro, oppure, nel caso di un'impresa, fino al 4% del fatturato annuo globale all'anno precedente, a seconda di quale sia superiore.

I fattori considerati per infliggere un'ammenda comprendono: la natura, la gravità e la durata dell'infrazione o il carattere intenzionale della stessa, tutte le azioni adottate per mitigare il danno subito, il grado di responsabilità e il modo in cui tale infrazione è stata resa nota all'autorità di vigilanza.

Riferimenti Normativi

- REGOLAMENTO 679/2016: Articoli: da 44 a 50 (Capo V), 68, Considerando: 6, da 101 a 103, da 107 a 116, da 167 a 169
- Decisione di esecuzione (UE) 2016/1250 della commissione sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy
- Gruppo di lavoro Articolo 29 – WP245 del 13 dicembre 2016

Approfondimenti

- Comunicazione della Commissione al Parlamento Europeo e al Consiglio Scambio e protezione dei dati personali in un mondo globalizzato COM / 2017/07 finale
- Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali del Garante italiano

STEFANELLI & STEFANELLI STUDIO LEGALE

il valore del network
la forza dell'esperienza

www.studiolegalestefanelli.it

Professionisti dello Studio

AVV.	**ANDREA STEFANELLI**
AVV.	**SILVIA STEFANELLI**
AVV.	LAURA ASTI
AVV.	FABIO CARUSO
AVV.	ADRIANO COLOMBAN
AVV.	ALESSANDRA DELLI PONTI
AVV.	EDOARDO DI GIOIA
AVV.	ALESSIA DIOLI
AVV.	RAFFAELE GAMMAROTA
AVV.	ELEONORA LENZI
AVV.	ANDREA MARINELLI
AVV.	SILVIA PARI
DOTT.	FEDERICO BRESCHI
DOTT.	VALENTINA ANNA GAROFANO
DOTT.	GIORGIA VERLATO
PROF. AVV.	ALESSANDRA MAGLIARO *of counsel*

Qualità Certificata

Member of CISQ Federation

RINA CERTIFIED IQNet MANAGEMENT SYSTEM

CERTIFIED MANAGEMENT SYSTEM

Certificato n. 32945/15/S

Assistenza e consulenza legale giudiziaria e stragiudiziaria,
per privati e aziende, sia nazionale che internazionale

BOLOGNA - Via Azzo Gardino, 8/A - tel +39 051 520315
MILANO - Via Lepetit, 8 - tel. +39 02 0069 6504
mail info@studiolegalestefanelli.it