CONSULENTI DI DIREZIONE ASSOCIATI

Multinazionali e GDPR: attenzione a gestire il trasferimento dei dati all'estero

In nome di una reale ed effettiva tutela degli interessati, il GDPR prevede che i dati possono essere trasferiti solo verso Paesi terzi che garantiscano un livello di sicurezza equivalente a quello previsto nell'Unione europea. In particolare, alle multinazionali viene richiesto di prevedere delle norme vincolanti per le imprese, autorizzate da un'autorità di controllo, per i trasferimenti internazionali dall'Unione agli organismi del gruppo, che contemplino i principi fondamentali di tutela della privacy e le opportune garanzie per il trasferimento di dati personali. Quali sono le clausole vincolanti?

Uno dei primi problemi che IL **GDPR** pone, e che non è nuovo (ma già era preso in considerazione nel Codice Privacy del 2003), riguarda il **controllo del dato** mentre circola, e soprattutto mentre circola **oltre i confini**.

Nella società dell'informazione attuale, grazie anche all'uso intensivo delle reti e del cloud, il concetto di confine (inteso come "barriera") viene a cadere, e le informazioni, soprattutto nelle **multinazionali**, attraversano il mondo passando da una business unit a un'altra o da sedi centrali e clienti in tutto il mondo.

Il fine (di protezione) che la normativa vuole raggiungere, allora, è quello di **garantire** lo **stesso livello di protezione** in ogni luogo che il dato attraversa o dove l'informazione è custodita. In altre parole: il dato può essere trasferito solo verso Paesi che garantiscano, in vari modi, un livello di sicurezza equivalente a quello previsto in Unione Europea e dal GDPR.

Estensione dell'ambito di applicazione del GDPR

Il GDPR tende ad estendere il proprio ambito di applicazione anche oltre i confini europei, in nome di una reale ed effettiva tutela degli interessati, prevedendo che tutti i fornitori di servizi che promuovono la propria attività anche in Stati europei debbano rispettare, nelle operazioni di trattamento dei dati personali, il Regolamento stesso.

La **globalizzazione** e l'espansione delle cooperazioni internazionali hanno reso sempre più comuni e frequenti i **trasferimenti di dati all'estero** e i flussi transfrontalieri.

Per tale ragione, il legislatore europeo, per garantire comunque un livello di sicurezza adeguato, ha imposto, con gli articoli 44 e seguenti del GDPR, determinate condizioni affinché sia possibile effettuare un trasferimento di dati verso Paesi terzi.

Innanzitutto, ai sensi dell'articolo 45, può essere la Commissione stessa a "decidere", con effetto nell'intera Unione, che un Paese terzo, un territorio, un settore specifico o un'organizzazione internazionale offrano un **livello adeguato di protezione** dei dati, garantendo in tal modo la certezza del diritto e l'uniformità in tutta l'Unione.

In tali casi, i trasferimenti di dati personali possono avere luogo **senza ulteriori autorizzazioni**. La Commissione può, inoltre, decidere, dopo aver fornito una dichiarazione completa che illustri le motivazioni al Paese terzo o all'organizzazione internazionale, di revocare tale decisione.

In particolare, com'è precisato nel Considerando n. 104, la Commissione UE, nella sua valutazione, dovrebbe tenere conto, nel momento in cui va a qualificare dei Paesi come "sicuri", di alcuni **elementi suggeriti dalla legge**.

Tra questi, vi sono il modo in cui il Paese terzo rispetta l'idea di Stato di diritto, la situazione della giustizia, le norme internazionali in tema di diritti umani e di libertà fondamentali, nonché la legislazione generale e settoriale riguardante la sicurezza pubblica, la difesa nazionale, l'ordine pubblico e il diritto penale. In altre parole, la Commissione verifica anche la "civiltà" giuridica di quel Paese in base a parametri presi in considerazione da Stati democratici.

Inoltre, l'adozione di una **decisione di adeguatezza** nei confronti di un territorio o di un settore specifico all'interno di un Paese terzo dovrebbe basarsi su criteri chiari e obiettivi, come specifiche attività di trattamento o come l'ambito di applicazione delle norme giuridiche e degli atti legislativi in vigore nel Paese stesso.

Da parte sua, il Paese terzo dovrebbe offrire garanzie di un **livello di protezione equivalente** a quello dell'Unione, assicurando un effettivo controllo indipendente della protezione dei dati, prevedendo meccanismi di cooperazione con autorità di protezione dei dati degli Stati membri e riconoscendo agli interessati diritti effettivi e azionabili, congiuntamente a mezzi di ricorso effettivo in sede amministrativa e giudiziale.

È opportuno che la Commissione controlli il funzionamento delle decisioni sul livello di protezione in un Paese terzo, prevedendo un meccanismo di **riesame** e **monitoraggio periodico**.

Come anticipato, infatti, essa può altresì riconoscere che un Paese terzo, un territorio, un settore specifico o un'organizzazione internazionale non garantiscano più un livello adeguato di protezione dei dati.

Di conseguenza, il trasferimento di dati personali verso tale Paese terzo od organizzazione internazionale dovrebbe essere vietato, fatta eccezione per deroghe previste in situazioni particolari. La Commissione dovrebbe informare tempestivamente il Paese terzo o l'organizzazione internazionale dei motivi e avviare consultazioni con questi al fine di risolvere la situazione.

Clausole di protezione dei dati

Ai sensi dell'articolo 46 del GDPR, poi, in mancanza di una decisione di adeguatezza, il titolare del trattamento o il responsabile del trattamento dovrebbe provvedere a **compensare la carenza di protezione** dei dati in un Paese terzo con adeguate garanzie a tutela dell'interessato.

Queste ultime possono consistere, ad esempio, nell'applicazione di **norme vincolanti d'impresa**, clausole-tipo di protezione dei dati adottate dalla Commissione o da un'autorità di controllo, o clausole contrattuali autorizzate da un'autorità di controllo. Tali garanzie dovrebbero assicurare un rispetto dei requisiti in materia di protezione dei dati e dei diritti degli interessati adeguato ai trattamenti all'interno dell'Unione.

Esse dovrebbero riguardare, in particolare, la conformità **rispetto ai principi generali** in materia di trattamento e protezione dei dati personali fin dalla progettazione. I trasferimenti possono essere effettuati anche da autorità od organismi pubblici ad autorità od organismi pubblici di Paesi terzi, o organizzazioni internazionali con analoghi compiti o funzioni.

In ogni caso, la facoltà per il titolare del trattamento o il responsabile del trattamento di utilizzare clausole-tipo di protezione dei dati adottate dalla Commissione o da un'autorità di controllo non dovrebbe precludere loro la possibilità di includere tali clausole in un contratto più ampio; al contrario, essi dovrebbero essere incoraggiati a fornire garanzie supplementari attraverso impegni contrattuali che integrino le suddette clausole.

Per quanto riguarda, nello specifico, la **situazione delle multinazionali**, l'articolo 47 del GDPR prevede che un gruppo imprenditoriale o un gruppo di imprese che svolge un'attività economica comune dovrebbe poter applicare le norme vincolanti d'impresa approvate per i trasferimenti internazionali dall'Unione agli organismi del gruppo stesso, purché tali norme contemplino tutti i principi fondamentali e i diritti azionabili che costituiscono adeguate garanzie per il trasferimento di dati personali.

Le **norme vincolanti** d'impresa dovrebbero specificare:

- la struttura e le coordinate di contatto del gruppo imprenditoriale e di ciascuno dei suoi membri;
- i trasferimenti di dati (categorie di dati personali, tipo di trattamento e finalità);
- la loro natura giuridicamente vincolante, sia a livello interno che a livello esterno;
- l'applicazione dei principi generali di protezione dei dati (limitazione della finalità, minimizzazione dei dati, limitazione del periodo di conservazione, etc.);
- i diritti dell'interessato e i relativi mezzi per esercitarli;
- le modalità in base alle quali sono fornite informazioni all'interessato;
- i compiti dei responsabili della protezione dei dati;
- le procedure di reclamo;
- i meccanismi per garantire la verifica della conformità alle norme vincolanti d'impresa;
- i meccanismi relativi alla modifica delle norme;
- il meccanismo di cooperazione con l'autorità di controllo e l'appropriata formazione in materia di protezione dei dati al personale che ha accesso regolare ai dati stessi.

Deroghe

Infine, l'articolo 49 del GDPR prevede una serie di deroghe che ammettono il trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale anche in **mancanza** di una **decisione di adeguatezza** ai sensi dell'articolo 45 o di garanzie adeguate ex articolo 46 del GDPR.

È, infatti, opportuno prevedere comunque la possibilità di trasferire dati nei casi in cui l'interessato abbia esplicitamente acconsentito, se il trasferimento è occasionale e necessario in relazione a un contratto o un'azione legale, se sussistono motivi di rilevante interesse pubblico previsti dal diritto dell'Unione o degli Stati membri o se i dati sono trasferiti da un registro stabilito per legge e destinato a essere consultato dal pubblico o dalle persone aventi un legittimo interesse.

In quest'ultimo caso, come precisato dal Considerando n. 111, il trasferimento non dovrebbe riguardare la totalità dei dati personali o delle categorie di dati contenuti nel registro. Inoltre, quando il registro è destinato a essere consultato dalle persone aventi un legittimo interesse, i dati possono essere trasferiti soltanto se tali persone lo richiedono o ne sono destinatarie, tenendo pienamente conto degli interessi e dei diritti fondamentali dell'interessato.

In ogni caso, se la Commissione non ha adottato alcuna decisione circa il livello adeguato di protezione dei dati di un Paese terzo, il titolare o il responsabile del trattamento dovrebbero ricorrere a soluzioni che diano all'interessato diritti effettivi e azionabili in relazione al trattamento dei suoi dati personali nell'Unione, dopo il trasferimento, così da continuare a beneficiare dei diritti fondamentali e delle garanzie.

Il quadro che abbiamo descritto può apparire complesso, ma ha la finalità di proteggere il dato nel suo momento più delicato e vulnerabile, ossia quando è in transito e "viaggia" verso altri Stati che non possiedono una cultura della data protection simile a quella europea.

Nella pratica, una buona combinazione di **indicazioni dell'Unione**, **clausole contrattuali vincolanti** e **rapporti chiari tra le società** dovrebbe aiutare a garantire un quadro più rispettoso dei diritti dell'interessato.