lexant
STUDIO LEGALE

FOCUS ON

GDPR: l'impatto sulle multinazionali

L'applicazione del Regolamento Privacy UE 679/2016 nelle realtà multinazionali

GDPR (Regolamento Privacy UE 679/2016): l'impatto sulle Società multinazionali

Il nuovo "Regolamento generale per la tutela dei dati personali" (GDPR) è entrato in vigore in tutta Europa il 25 maggio e con questo l'onere per le aziende di metter mano alla propria organizzazione per adeguarsi ai nuovi adempimenti, che riguardano, non solo la necessità di gestire i nuovi diritti degli utenti (diritto di accesso, portabilità, cancellazione e rettifica dei dati e obbligo di richiesta del consenso esplicito per il loro utilizzo), ma comprendono anche questioni più tecniche, quali la valutazione dei rischi di compromissione dei dati da parte di hacker e virus, l'istituzione di un "Responsabile della protezione dei dati" (DPO) nelle aziende, la compilazione di un Registro e così via.

Il Regolamento ha un impatto particolare sulle aziende multinazionali che devono confrontarsi con la necessità di gestire il flusso di dati oltre i confini nazionali e devono coordinare le realtà dei singoli Paesi nei quali operano.

1. **gli adempimenti connessi al trasferimento dei dati all'estero, soprattutto Extra UE;**
2. **Il coordinamento tra il DPO e gli uffici privacy dei diversi Stati;**
3. **La tenuta del registro dei trattamenti;**
4. **Il quadro sanzionatorio.**

***** *** *****

1. Gli adempimenti connessi al trasferimento dei dati all'estero, soprattutto Extra UE:

Il GDPR prevede, agli articoli 44 e seguenti, che i dati possano essere trasferiti verso Paesi terzi, purché questi garantiscano un livello di sicurezza equivalente a quello previsto nell'Unione Europea.

Innanzitutto, ai sensi dell'articolo 45, vi possono essere Paesi terzi, territori, settori specifici o organizzazioni internazionali in relazione ai quali la Commissione, con effetto nell'intera Unione, può ritenere sussistente un livello adeguato di protezione dei dati, autorizzando i trasferimenti di dati personali verso questi Paesi senza necessità di ulteriori autorizzazioni.

In mancanza di tale parere di adeguatezza, ai sensi dell'articolo 46 del GDPR, il *Titolare* o il *Responsabile* del trattamento dovrebbero provvedere a compensare la carenza di protezione dei dati in un Paese terzo con adeguate garanzie a tutela dell'*interessato*. Queste garanzie 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.

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, un gruppo imprenditoriale o un gruppo di imprese che svolge un'attività economica comune può gestire i flussi intra-gruppo di dati personali attraverso il meccanismo del c.d. BCR (*Binding Corporate Rules*), ovvero chiedendo la concessione di una autorizzazione del Garante al trasferimento dei dati personali verso Paesi terzi, con riferimento a trasferimenti di dati personali dall'Italia verso Paesi terzi che si svolgano nel rispetto di quanto stabilito all'interno del testo di Bcr e per le sole finalità ivi indicate.

Il rilascio di un'autorizzazione al trasferimento di dati personali tramite Bcr consente alle filiali della multinazionale che ne abbia fatto richiesta, anche se stabilite in diversi Paesi, di trasferire, all'interno del gruppo d'impresa, i dati personali oggetto delle Bcr, senza ulteriori adempimenti.

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 verso altri Stati che non possiedono una cultura della *data protection* simile a quella europea.

2. Il coordinamento tra il DPO e gli uffici privacy dei diversi Stati:

Il *Data Protection Officer* (DPO) nel settore privato deve essere nominato obbligatoriamente per i trattamenti effettuati da un *titolare* le cui attività principali consistono in trattamenti che richiedono un monitoraggio regolare e sistematico degli interessati su larga scala, con riferimento a categorie particolari di dati personali e di dati relativi alle condanne penali e ai reati, ha una serie di compiti specifici e ben definiti e, ai sensi dell'Articolo 37 del GDPR deve avere una adeguata conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati e deve poter agire con indipendenza.

Nel caso di gruppi imprenditoriali, è possibile nominare un unico DPO, a condizione che vi sia un efficiente coordinamento tra questo e i diversi Uffici Privacy nazionali, che sia adeguatamente coinvolto in tutte le questioni che

riguardano la protezione dei dati personali e che gli siano fornite le risorse necessarie per lo svolgimento delle sue funzioni in maniera del tutto indipendente. Inoltre deve essere facilmente raggiungibile da ciascuno stabilimento.

A tal fine, il *titolare* o il *responsabile del trattamento* sono tenuti a pubblicare i suoi dati di contatto ed a comunicarli all'autorità di controllo.

Il *responsabile della protezione dei dati* (DPO) può assolvere i suoi compiti in base ad un apposito contratto di servizi oppure essere scelto tra i dipendenti del titolare o del responsabile del trattamento. In ogni caso, è fondamentale che egli riesca ad adempiere alle funzioni e ai compiti assegnatigli in maniera indipendente.

D'altro lato, però, il DPO, se necessario con il supporto di un team di collaboratori, deve essere in grado di comunicare con gli *interessati* in modo efficiente e di collaborare con le autorità di controllo coinvolte. Egli, infatti, oltre a rivestire il ruolo di "supervisore" interno per dimostrare la conformità dell'impianto aziendale ai dettami del GDPR, svolge anche la funzione di comunicatore verso l'esterno, con riferimento sia al vertice dell'organizzazione, sia alle sedi distaccate.

In alcune multinazionali che hanno la sede "madre" all'estero è stata fatta la scelta di mantenere un solo DPO nel Paese di origine e di prevedere degli uffici ad hoc nei singoli Paesi, dei veri e propri uffici (*Privacy Office*) che gestiscono le questioni relative alla protezione dei dati e si relazionano con il DPO "centrale".

Si tratta di una strategia che può garantire efficienza, anche se molto spesso la conoscenza della normativa specifica nel singolo Paese (si pensi, ad esempio, ai temi del diritto del lavoro) o la necessità di dialogare con l'autorità di controllo locale possono suggerire l'opportunità di nominare anche un DPO "locale" nel paese della *business unit*.

Ciò comporterà una necessità di coordinamento soprattutto in caso di adempimenti che richiedano una reazione rapida, che potrebbe essere viziata dalle distanze o dalle comunicazioni tra Paese e Paese. Si pensi a due casi tipici previsti dal Regolamento: la denuncia di un *data breach* o la risposta a un interessato che eserciti i suoi diritti.

Nel primo caso, un *data breach* in un Paese dove non sia nominato un DPO richiede un coordinamento rapidissimo per permettere al DPO centrale di non solo venire a conoscenza dell'incidente, ma anche di denunciarlo in tempo e di iniziare a dialogare col Garante per comprendere quali possano essere i rimedi da adottare nell'immediato.

Nel secondo caso, il rischio è che la richiesta dell'interessato – ad esempio di cancellazione dei propri dati – non sia evasa in tempo per mancanza di coordinazione tra i vari punti di contatto.

3. La tenuta del registro dei trattamenti:

Il Registro dei Trattamenti (art 30 GDPR) consiste in un documento che attesta la conformità della propria organizzazione alle prescrizioni della legge ed esplicita la *Privacy policy* adottata al fine della pianificazione e controllo della sicurezza dei dati trattati.

Nelle multinazionali la tenuta del registro è prevista al duplice fine di consentire all'Autorità di controllo di avere un quadro completo di tutti i trattamenti e delle misure in tal senso adottate e di disporre fin dall'inizio di un sistema di sicurezza funzionale, che permetta di tenere sotto controllo ogni aspetto relativo al dato trattato.

La buona tenuta di un registro delle attività di trattamento dei dati ricopre un ruolo fondamentale, si tratta infatti della mappa dei trattamenti dell'azienda che permette di comprendere la strategia di *compliance* che l'azienda ha scelto di adottare, di mantenere sotto controllo le attività svolte e gestire opportunamente le aree di rischio.

4. Il quadro sanzionatorio:

Con la piena operatività del GDPR le sanzioni applicabili in ambito UE in caso di violazione dei dati acquistano particolare peso per le multinazionali. Le sanzioni amministrative pecuniarie possono arrivare ad un valore di 10 o 20 milioni di euro a seconda dei casi, o possono essere pari al 2% o al 4% del fatturato mondiale totale annuo dell'esercizio precedente.

Il GDPR prevede, tuttavia, casi di mitigazione della gravità delle sanzioni se viene riscontrata la volontà, da parte dei gruppi di imprese, di cercare di rimediare al danno, o di contenerlo, e se l'azienda dimostra di aver affrontato gli adempimenti necessari per garantire la maggio sicurezza possibile e la protezione dei dati.

Ecco allora che un approccio serio e strutturato alla normativa può essere determinante anche nella gestione di tale rischio.

Avv. Simona Cardillo