GattiPavesiBianchiLudovici

28 Giugno 2021

Dati personali e trasferimento fuori UE Vademecum per non perdere la bussola!

Nell'ultimo anno Corte di Giustizia, Commissione Europea e Garante europeo sono intervenuti con una serie di provvedimenti che hanno profondamente modificato il quadro applicativo delle regole che devono sovraintendere al trasferimento dei dati personali fuori dal territorio dell'UE.
La nostra sintesi, a primissima lettura delle novità dell'ultima settimana, si propone una interpretazione sistematica della Sentenza *Schrems II*; della Decisione della Commissione europea del 4 giugno 2021 n. 914/2021 e delle Raccomandazioni dello *European Data Protection Board* del 18 giugno 2021, pubblicate il 21 giugno 2021.

Il trasferimento di dati personali fuori dall'Unione europea

Che cosa significa trasferire i dati all'estero?
La risposta è solo apparentemente scontata e, spesso, l'importanza di qualificare esattamente questa fattispecie è sottostimata, con conseguenze che possono anche rilevanti in termini sanzionatori per imprese e professionisti.
La nozione di "trasferimento di dati all'estero, è infatti diffusamente equivocata, laddove si tende a limitarla alle sole attività di "spostamento fisico" di dati, con ciò intendendo operazioni di "trasmissione" e "invio" vero e proprio di dati, ed escludendo al contempo tutti quei casi – che sono la maggior parte – nei quali i dati personali raccolti siano *resi disponibili/accessibili in un altro Stato*.
Il tipico caso è quello dell'affidamento a un fornitore extracomunitario del servizio di *call center*: il fornitore viene incaricato di contattare i clienti europei utilizzando i dati identificativi e di contatto prelevati direttamente dal database del committente, al quale gli viene garantito l'accesso con un semplice log in; ebbene questo è, a tutti gli effetti, un trasferimento di dati extra SEE.

Tenendo questo a mente, costituisce un "trasferimento di dati", a titolo esemplificativo:

- Salvare i propri documenti, liste clienti, nominativi dei dipendenti, su una piattaforma *cloud* digitale, laddove il fornitore della piattaforma abbia i *server* al di fuori dell'Unione europea;
- Usufruire di piattaforme di automazione del marketing per l'invio di newsletter che abbiano sede al di fuori dell'Unione europea;
- Appaltare servizi di *customer care* a operatori siti fuori dall'Unione europea, anche nell'ipotesi in cui questi ultimi accedano ai database aziendali senza che vi sia un formale invio da parte della funzione aziendale dedicata;
- Fornirsi di un servizio di *recruiting* il cui fornitore sia sito fuori dall'Unione europea;
- Utilizzare una piattaforma gestionale interna (ad esempio, per la predisposizione di *timesheets*) che si basi su server ospitati fuori dall'Unione europea;
- Appaltare servizi di riscossione crediti tramite operatori che contattano i debitori europei chiamando al di fuori dell'Unione europea.

Questi esempi sono solo alcuni dei numerosi casi in cui le aziende si trovano ad effettuare un trasferimento di dati personali all'estero senza esserne consapevoli e che, se non regolamentati adeguatamente, presentano elevati livelli di rischio sia per le persone fisiche cui i dati si riferiscono, sia per l'azienda che opera in qualità di titolare del trattamento, la quale si espone a sanzioni non indifferenti per non aver informato gli interessati e, soprattutto, per non aver adottato un'idonea base giuridica che legittimasse il trasferimento.
A riprova dell'attualità del tema, si noti che, di recente, l'Autorità Garante per la Protezione dei Dati Personali, nel valutare l'adeguatezza dell'App IO a trattare i dati sensibili dei cittadini italiani, ha sollevato il tema dei trasferimenti all'estero, chiedendo espressamente che sia "*assicurata la legittimità del trasferimento dei dati personali verso Paesi terzi, considerato che, per la gestione della Piattaforma IO, PagoPA si avvale di alcuni fornitori (tra cui Microsoft, Google, Instabug e Mixpanel) che effettuano trattamenti al di fuori dell'Unione europea (punto 5.4 del provvedimento)*".
A seguito di questo avvertimento PagoPa ha dichiarato di essersi impegnata a sottoscrivere con i fornitori, entro il 18 giugno 2021, le nuove *Standard Contractual Clauses* del 4 giugno 2021 di cui diremo nel prosieguo, nonché ad adottare, se del caso, le misure supplementari suggerite dallo European Data Protection Board.

Le recentissime novità nel panorama dei trasferimenti di dati extra-SEE

Il panorama legislativo e applicativo dei trasferimenti di dati personali all'estero ha subito una (attesissima) svolta lo scorso 7 giugno 2021, quando è stato ufficialmente pubblicato sulla Gazzetta Ufficiale dell'Unione europea il testo definitivo delle nuove Clausole Contrattuali Standard ("**SCC**") ex art. 46 Regolamento (EU) per la Protezione dei Dati Personali ("**GDPR**"), approvate con Decisione di esecuzione della Commissione europea n. 914/2021 del 4 giugno 2021 che abrogano il vecchio *set* d clausole del 2001 e del 2010 (Decisioni della Commissione Europea n. 2001/497 e n. 2010/87). Le clausole sono state seguite, ad appena una settimana di distanza, dalla pubblicazione delle *Final Recommendations dello European Data Protection Board* ("**EDPB Final Recommendations**") pubblicate lo scorso lunedì 21 giugno 2021.
I testi, da leggere congiuntamente, hanno superato molti dei problemi che negli ultimi anni hanno influito sulla prassi applicativa dei trasferimenti all'estero, e in particolare:

- I dubbi sulla definizione di trasferimento di dati personali all'estero;
- La rigidità delle clausole del 2001 e 2010, che permettevano la sottoscrizione da parte del solo titolare del trattamento;
- L'incertezza sulle procedure da adottare per valutare la sicurezza del trasferimento di dati personali in un Paese terzo.

I due testi risolvono il clima di incertezza giuridica che si era creato nella materia, a partire dalla sentenza della Corte di Giustizia dell'Unione europea del 16 luglio 2020 *Schrems II* C-311/18, la quale non solo ha annullato la decisione di adeguatezza "*Privacy Shield*", così privando i titolari del trattamento europei della più utilizzata base legale per trasferire i dati negli Stati Uniti, ma ha contestualmente sancito una serie di principi generali in materia di trasferimenti dei dati al di fuori dell'Unione europea applicabili a tutte le operazioni di trattamento, in tutti i Paesi extra-europei, quali:

- La necessità di una verifica preliminare da parte dell'esportatore dei dati (c.d. "*data exporter*") dell'adeguatezza della legislazione del destinatario del trasferimento (c.d "*data importer*") a garantire la protezione dei dati personali degli interessati;
- Il *risk-based approach*, ovverosia l'adozione di misure supplementari per assicurare un'adeguata protezione dei dati personali, da valutare a seguito della verifica preliminare di cui al primo punto.

Le novità e i chiarimenti

A seguito di una prima lettura delle clausole standard e delle EDPB Final Recommendations, ne evidenziamo le maggiori novità:

- **A chi si rivolgono le nuove clausole**: le clausole si rivolgono a tutte le imprese che trasferiscono dati personali al di fuori del territorio dell'Unione Europea. **Le EDPB Final Recommendation hanno chiarito che il concetto di trasferimento include anche il *semplice accesso* da remoto ai dati personali e la mera *conservazione* di dati all'estero;**
- **Chi sottoscrive le nuove clausole**: le clausole possono essere sottoscritte tra il responsabile del trattamento e un altro responsabile del trattamento o sub-responsabile del trattamento, senza partecipazione del titolare (c.d. *Module Three – Transfer Processor to Processor*). È altresì previsto che più soggetti possano aderire alle clausole in qualità di più *data exporters* o *importers*.
- **Gli obblighi di trasparenza**: le clausole richiedono al *data exporter* di dettagliare, con grande precisione e trasparenza, quali siano esattamente i dati oggetto di trasferimento, le modalità con i quali saranno trattati, la ragione per cui sono trattati, il periodo di tempo per cui saranno conservati, le tipologie di trattamento a cui saranno sottoposti. Le clausole specificano infatti che "*Deve essere possibile distinguere chiaramente le informazioni applicabili a ciascun trasferimento o a ciascuna categoria di trasferimenti e, a tale riguardo, determinare i ruoli rispettivi delle parti quali esportatori e/o importatori*"
- **Chi è responsabile nei confronti degli interessati**: il *Module Three – Transfer Processor* to Processor stabilisce che il *data exporter* (che in questo caso saranno uno o più responsabili del trattamento) è responsabile per i danni causati alle persone fisiche dall'illecito trattamento dei dati personali, salvo attribuirgli azione di regresso verso il *data importer* o gli altri responsabili esportatori nel caso in cui la responsabilità per la violazione sia in tutto o in parte di questi ultimi.
- **I rapporti interni di responsabilità tra i soggetti partecipanti al trasferimento nei confronti dell'Autorità**: in attesa di chiarimenti da parte della Commissione europea su questo punto, in questa fase è possibile affermare che vi sia un accrescimento della responsabilità del responsabile del trattamento, che non elimina quella del titolare (che comunque dovrà sicuramente essere a conoscenza del trasferimento e partecipare nella scelta della base giuridica più adatta per legittimarlo), ma si somma a quest'ultima e riguarda gli aspetti "operativi" del trasferimento (i.e. la vigilanza sulla corretta applicazione delle clausole standard, la valutazione dei rischi del trasferimento nel Paese d'importazione)
- **Le misure supplementari**: le EDPB Recommendations prevedono che prima del trasferimento, il *data exporter* debba valutare se la legislazione del Paese di importazione può pregiudicare il livello di protezione sancito dal GDPR. Nel caso in cui questa valutazione individui effettivamente dei rischi, il *data exporter* dovrà valutare di adottare le misure supplementari tecniche e organizzative suggerite nelle EDPB Final Recommendations (ad esempio: l'anonimizzazione dei dati prima del trasferimento)

I nostri suggerimenti operativi

Alla luce del nuovo quadro così delineato consigliamo alle aziende che effettuano trasferimenti di dati all'estero di considerare che:

- I trasferimenti sono operazioni rischiose;
- I flussi di dati fuori dall'Unione europea vanno mappati, anche dal punto di vista tecnico, secondo il criterio sopra individuato, e cioè tenendo presente l'ampia accezione di "trasferimento";
- Le condizioni contrattuali imposte da fornitori esterni devono essere esaminate con attenzione per ricercare possibili circostanze che determinano un trasferimento all'estero (ad esempio la localizzazione dei server fuori dallo SEE);
- I fornitori esterni di servizi vanno valutati dal punto di vista strutturale (i.e. che tipo di garanzie offre un fornitore sulla sicurezza dei dati);
- I servizi affidati a fornitori esterni, se coinvolgono il trattamento di dati personali, devono essere regolati a livello contrattuale anche dal punto di vista della protezione dei dati;
- La *compliance* alla normativa sul trasferimento dei dati al di fuori dell'Unione europea è costosa: per questa ragione è necessario condurre un'analisi costi/benefici e, nel caso affidare il servizio a un fornitore europeo;
- Ad ausilio della valutazione sull'adeguatezza della legislazione del Paese terzo, è possibile predisporre una *check-list*, da compilare e firmare da parte del *data importer*. In questo modo sarà possibile per il *data exporter* dimostrare, in ossequio al principio di *accountability*, di aver condotto attente valutazioni preliminari al trasferimento;
- Per trasferimenti fuori dall'Unione europea ma all'interno del medesimo gruppo di imprese, potrebbero essere state adottate dalla capogruppo delle *Binding Corporate Rules*, approvate dall'Autorità di controllo competente, che costituiscono una valida base legale per questo tipo di trasferimenti.

Massimiliano Patrini e Francesca Ellena

Il presente contributo è stato pubblicato dalla testata "Diritto Bancario" in data 24 giugno 2021 – Link alla pubblicazione: LINK