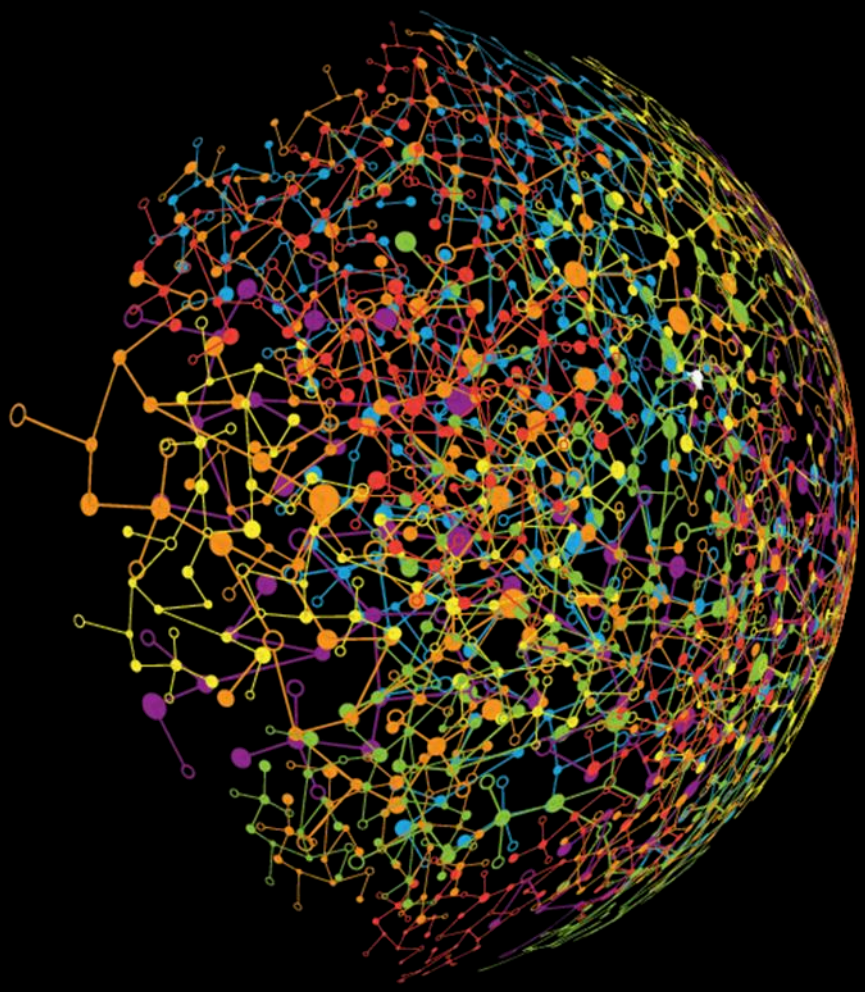
Deloitte.
Legal



Data Protection *Breaking news*

TRASFERIMENTI EXTRA-UE DI DATI

Ottobre 2021

TRASFERIMENTI EXTRA-UE DI DATI: IL NUOVO FRAMEWORK POST *SCHREMS II* E L'*ENFORCEMENT* DELL'AUTORITA'

Uno scenario in forte evoluzione quello delle tutele legali collegate al trasferimento di dati all'estero, post Schrems II: le nuove Standard Contractual Clauses (SCC) della Commissione, l'obbligo di effettuare Transfer Impact Assessment (TIA) e di adottare misure supplementari, le prime sanzioni da parte delle Autorità e il rischio della sospensione dei flussi di dati

Nuove Standard Contractual Clauses

Le nuove Standard Contractual Clauses (SCC) adottate dalla Commissione europea sono **efficaci dal 27 settembre 2021**. I **vecchi set di SCC** che sono stati utilizzati sino ad ora dalle società sono **abrogati**. Le aziende che, nello svolgimento della propria attività, necessitano di trasferire dati al di fuori dello Spazio Economico Europeo (SEE) in paesi non ritenuti adeguati dalla Commissione europea (cd. Paesi Terzi) devono quindi **fare riferimento, d'ora in avanti, solo al nuovo set di clausole**.

Le nuove SCC, oltre a regolamentare il rapporto tra titolari e tra titolari e responsabili, sono state predisposte per disciplinare anche i trasferimenti tra responsabili, nonché per gestire il rapporto inverso responsabile-titolare. **Tutti i possibili ruoli privacy sono quindi coperti, rendendole maggiormente fruibili rispetto a quelle precedenti**. Le nuove clausole sono state infatti aggiornate anche per fornire flessibilità nell'ambito di catene di trattamento complesse e per coprire una più ampia gamma di scenari di trasferimento. Per poter formalizzare le nuove SCC occorre effettuare un rilevante lavoro di adattamento, in base alle specificità dei trasferimenti.

La recente sanzione del Garante

Lo scorso mese di settembre il Garante per la protezione dei dati personali (Garante) ha sanzionato una società che ha **trasferito dati personali ad un fornitore statunitense in assenza di tutti i necessari requisiti**.

L'Autorità, nel proprio provvedimento, ha ribadito che i trasferimenti extra UE sono consentiti **solo ove il titolare del trattamento fornisca garanzie adeguate** che prevedano diritti azionabili e mezzi di ricorso effettivi per gli interessati, tra cui le SCC adottate dalla Commissione europea.

L'obbligo del Transfer Impact Assessment (TIA)

Il Garante ha precisato (richiamando la sentenza Schrems II della CGUE) che le SCC, viste le loro caratteristiche, **non forniscono di per sé garanzie che vadano al di là di un obbligo contrattuale** di rispettare il livello di protezione richiesto dal diritto dell'Unione europea, pertanto **può essere necessaria**, in funzione della situazione esistente nell'uno o nell'altro Paese terzo, **l'adozione di misure supplementari** al fine di garantire un livello di protezione adeguato. Incombe quindi sul titolare del trattamento l'**obbligo svolgere un Transfer Impact Assessment (TIA)** volto ad accertare caso per caso, anche in collaborazione con il destinatario del trasferimento (cd. *data importer*), se il diritto del Paese di destinazione garantisca effettivamente una protezione adeguata.

L'individuazione delle misure di sicurezza

Nel caso di specie, la società in questione aveva sin dal principio formalizzato un *data processing agreement* (DPA) ai sensi dell'art. 28 del GDPR con il proprio fornitore US, stipulando poi anche un atto aggiuntivo con SCC allegate, con la previsione aggiuntiva che l'importatore dovesse aver messo in atto misure amministrative, fisiche e tecniche per la protezione della sicurezza, la confidenzialità e l'integrità dei Dati Personali caricati per l'utilizzo dei prodotti concessi in licenza e che i dettagli relativi a tali misure fossero disponibili su un modulo consultabile su richiesta.

Il Garante ha però osservato che una simile configurazione del rapporto non risulta idonea: **le misure di sicurezza non sono chiaramente individuate né allegate al contratto e non vi è quindi certezza in merito al tipo di misure effettivamente adottate dall'importatore**. Le SCC prevedono invece espressamente che le misure di sicurezza debbano essere indicate in allegato, che costituisce parte integrante del contratto e deve essere compilato e sottoscritto dalle parti.

Inoltre, **la società sanzionata non aveva effettuato una valutazione circa l'effettiva capacità delle misure adottate di garantire il rispetto degli obblighi assunti dall'importatore con la sottoscrizione delle SCC**, alla luce della legislazione del Paese terzo in cui i dati devono essere trasferiti.

La sospensione del trasferimento dei dati

Sulla base di quanto previsto nella Raccomandazione 01/2020 dello *European Data protection Board* (EDPB), nel caso in cui il diritto del Paese in cui è stabilito l'importatore imponga a quest'ultimo degli obblighi che sono in contrasto con quelli previsti a suo carico dalle SCC e non sia possibile porre in essere misure supplementari capaci di assicurare il rispetto di tali obblighi, **il titolare è tenuto a sospendere il trasferimento dei dati personali verso il Paese terzo**.

Cifratura e pseudonimizzazione

Il Garante, nel proprio provvedimento, ha anche evidenziato una falla nella modalità di cifratura dei dati che sarebbe avvenuta **solo "in transito" e poi anche dal fornitore, una volta terminato il trattamento**. La cifratura con la chiave dell'esportatore di dati è quindi avvenuta soltanto dopo **l'elaborazione dei dati da parte del fornitore**, il quale ha **avuto quindi accesso ai dati in chiaro.**

L'Autorità di controllo **non ha ritenuto sufficiente neanche la pseudonimizzazione** dei dati oggetto di trasferimento all'estero, in quanto, anche ove questa sia avvenuta in modo efficace, non è in ogni caso una misura equivalente all'anonimizzazione.

Il Garante non solo ha comminato una sanzione pecuniaria nel provvedimento in oggetto ma ha anche **vietato ogni ulteriore trasferimento di dati personali negli Stati Uniti**, in assenza di adeguate garanzie.

WARNING!

- Il **Garante ha iniziato ad applicare importanti sanzioni** alle società che trasferiscono dati personali in Paesi terzi in modo non conforme al nuovo framework normativo.

- L'imposizione del **blocco dei trasferimenti dei dati**, che può essere imposto dall'Autorità, potrebbe determinare un rallentamento o un'interruzione del business.

Gli *step* operativi

Alla luce del nuovo framework normativo e delle indicazioni delle Autorità europee (EDPB) e italiane (Garante), per trasferire in modo legittimo dati personali al di fuori dell'UE nei cosiddetti Paesi terzi, evitando possibili sanzioni e il rischio "business" collegato all'interruzione del flusso di dati, occorre:

- **mappare i propri fornitori / partner commerciali;**
- **aggiornare i contratti, adottando le nuove SCC, personalizzandole in base ai ruoli privacy ricoperti dalle parti;**
- **effettuare transfer impact assessment (TIA);**
- **adottare misure supplementari tecniche, legali e organizzative, in base alle esigenze specifiche collegate ai diversi trasferimenti;**
- **adeguare alcuni rilevanti documenti che fanno parte dell'impianto privacy di ogni titolare del trattamento, come le informative (che devono essere molto trasparenti sul tema dei trasferimenti) e il registro dei trattamenti;**
- **dotarsi di procedure efficaci e documentare le attività svolte.**

Anche in presenza di un nuovo accordo tra l'UE e gli USA (a cui si sta lavorando) per legittimare il trasferimento dei dati oltre-oceano, il nuovo framework introdotto dalla sentenza Schrems II **impone di dotarsi di un impianto di conformità adeguato** per gestire i trasferimenti di dati, nel rispetto anche dei principi di *accountability* e di *risk based approach*, fondamentali nel sistema normativo europeo in materia di protezione dei dati personali.

Experience the future of law, today

Today, you need smart lawyers who bring even more to the table than legal advice and memorandums. You need to work better, faster and with lower total cost. That takes someone who knows your business and your industry, yet thinks and works in new ways. A steady hand at the center of the transformation all around us. An expert in law, commerce and technology, who is able to serve you globally.

To make an impact that matters, you need an accomplished confidante who is both pragmatic and pioneering.

Deloitte Legal invites you to experience the future of law, today. Meet current obligations more effectively while anticipating future opportunities.

Automate complicated and time-consuming legal activities. Benefit from a commercial mindset that integrates legal, business and industry expertise. Draw upon our experience with business operating model transformation.

As you lead your enterprise through unprecedented complexity and change, we'll work with you not just for you. Working together, you're empowered to make confident decisions, guide your business and take advantage of possibilities.

Experience the future of law, today.

Key contacts

Ida Palombella
Partner - IP, IT and Privacy Data Protection
ipalombella@deloitte.it

Pietro Boccaccini
Director - IP, IT and Privacy Data Protection
pboccaccini*@deloitte.it*

Francesca Gili
Federico Vota
Simone Prelati
Martina Liverani

Deloitte.
Legal