STEFANELLI & STEFANELLI STUDIO LEGALE

TRASFERIMENTO DEI DATI IN PAESI EXTRA SEE POST SCHREMS II

- a cura della dott.ssa Federica Pucarelli -

COSA SI INTENDE PER "TRASFERIMENTO DEI DATI"?

Trasferimento materiale dei dati verso un soggetto che si trova in un Paese extra SEE

Accessibilità ai dati da remoto da parte di un soggetto che si trova in un Paese extra SEE

IL CASO SCHREMS

Come inizia

L'austriaco Maximillian Schrems presenta richiesta al Garante irlandese per bloccare il trasferimento di dati effettuato da Facebook Ireland verso la società madre statunitense.
La critica ruota intorno alla tesi che, negli Stati Uniti, il controllo dell'utente sui propri dati venga perso, dal momento che la legislazione americana consentirebbe "invasioni" della privacy da parte delle istituzioni, carenti sia sul piano della trasparenza sia su quello degli strumenti giuridici a disposizione del cittadino europeo per l'esercizio dei propri diritti.

Sentenza "Schrems I" del 2015 DELLA CJEU

All'esito della vicenda, la Corte di Giustizia dell'Unione Europea invalidava il Safe Harbour in quanto non forniva un livello di protezione dei dati sufficiente ed equivalente a quello previsto dall'UE.

Luglio 2016 - Nasce il Privacy Shield

Il Privacy Shield è un meccanismo di autocertificazione per le società stabilite negli USA: 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 da parte del Dipartimento del Commercio statunitense e possibili sanzioni da parte della Federal Trade Commission.

Sentenza "Schrems II" DELLA CJEU

La sentenza infatti dichiara che:

il Privacy Shield è invalido poiché non è in grado di garantire un livello di protezione "sostanzialmente equivalente" a quello garantito dall'Unione europea, specie in relazione agli strumenti legislativi americani di sorveglianza pubblica, che risultano invece eccessivi e sproporzionati rispetto ai criteri del diritto europeo.
La Decisione della Commissione UE 2010/87 resta valida.

Questo anche se le Clausole Contrattuali Standard (di seguito "CCS") in essa contenute non possono vincolare le Autorità pubbliche a quanto in esse stabilite per il loro carattere contrattuale. Esse,

pur rimaste **valide**, possono però essere utilizzate **solo previa valutazione, caso per caso, circa la sussistenza di idonee garanzie a protezione dei dati personali** nel Paese del destinatario, al fine di **determinare se le garanzie previste dalle CCS possano essere rispettate nella pratica**. In caso contrario, occorre verificare se sia possibile prevedere **misure supplementari** atte a garantire un livello di protezione sostanzialmente equivalente a quello vigente nel SEE.

LE PRIME INDICAZIONI DELL'EDPB SUL TEMA

L'European Data Protection Board ha pubblicato in data 23 luglio 2020 le FAQ sul Caso Schrems con l'obiettivo di fare chiarezza sui contenuti della decisione e sulle conseguenze prodotte dalla medesima. Vediamo in sintesi.

- **La sentenza della Corte ha implicazioni sugli strumenti di trasferimento diversi dal Privacy Shield?**
  La normativa statunitense cui fa riferimento la Corte (vale a dire **l'articolo 702 della FISA e l'Executive Order (EO) 12333) si applica a qualsiasi trasferimento verso gli Stati Uniti per via elettronica che** rientra nell'ambito di applicazione della suddetta normativa, indipendentemente dallo strumento utilizzato per il trasferimento.

- **È previsto un periodo di grazia durante il quale continuare a trasferire i dati verso gli USA senza valutare la base giuridica per il trasferimento.**
  No, la Corte ha annullato la decisione relativa allo scudo per la privacy senza preservarne gli effetti.

- **Un'Azienda trasferisce i dati a un importatore di dati statunitense aderente privacy shield, cosa deve fare adesso?**
  I trasferimenti sulla base di tale quadro giuridico sono illegali. Qualora l'azienda desideri continuare a trasferire i dati verso gli Stati Uniti, dovrà verificare se ciò sia possibile alle condizioni di seguito indicate.

- **Cosa deve fare una azienda che trasferisce i dati in USA in forza alle Clausole Contrattuali Standard (CCS)?**
  L'azienda europea potrà trasferire i dati personali sulla base delle CCS solo dopo aver effettuato, **caso per caso, una valutazione della disciplina del paese di destinazione e del livello di tutela della disciplina stessa.**
  Se dall'analisi risulta che il livello di protezione è inferiore a quello europeo, l'azienda potrà

introdurre **misure di garanzia supplementari**.
Se il Titolare giunge alla conclusione che, in ragione delle circostanze e nonostante l'adozione di eventuali misure supplementari, non vi siano in ogni caso adeguate garanzie per il trasferimento dei dati all'estero, dovrà **sospenderlo o porvi fine**.

- **Cosa deve fare una azienda che trasferisce i dati in USA in forza delle Norme Vincolanti d'Impresa ("Binding Corporate Rules")?**
  Anche per le Norme Vincolanti d'Impresa occorrerà effettuare una **valutazione caso per caso** circa la possibilità di trasferire i dati, tenuto conto delle circostanze del trasferimento e delle misure supplementari eventualmente messe in atto.
  Se, a seguito della valutazione di fatto, non risultano esserci adeguate garanzie, occorre sospendere o porre fine al trasferimento di dati personali.

- **Può una azienda trasferire i dati utilizzando le regole dell'art. 49 GDPR?**
  È ancora possibile trasferire dati dal SEE agli Stati Uniti sulla base delle **deroghe** previste dall'articolo 49 del GDPR, purché siano soddisfatte le condizioni di cui a tale articolo.

- **Quali sono le misure supplementari che le aziende possono utilizzare?**
  Le misure supplementari dovrebbero essere stabilite caso per caso, in relazione alla natura del trattamento e alle circostanze del trasferimento dei dati personali.

- **Se l'azienda si avvale di un Responsabile del trattamento, come fa a sapere se tale Responsabile trasferisce dati negli USA?**
  Il contratto stipulato con il Responsabile in conformità dell'articolo 28, paragrafo 3, del GDPR deve stabilire se i trasferimenti dei dati siano o meno autorizzati.
  Si tenga presente che **anche l'accesso ai dati effettuato da un paese terzo costituisce un trasferimento di dati.**
  Occorre inoltre verificare quali sono i **sub-responsabili** e se nella firma dei contratti gli stessi sono stati autorizzati. L'EDPB su questo punto richiama l'attenzione sul fatto che molti servizi informatici utilizzati dalle aziende potrebbero comportare il trasferimento di dati personali verso un paese terzo (ad esempio, servizi di archiviazione dei dati o manutenzione dei sistemi).

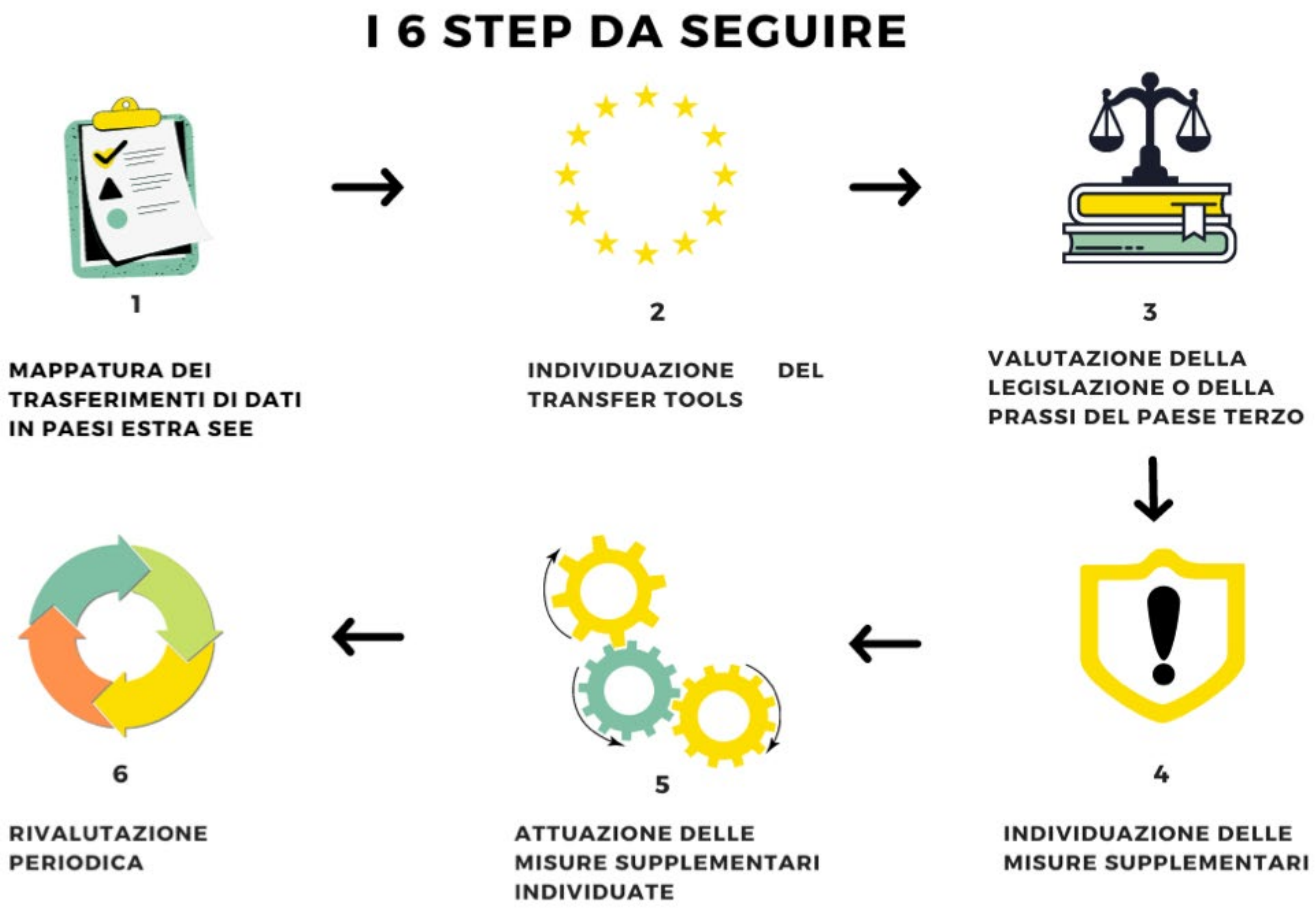
- **Nell'ipotesi in cui il contratto ex art. 28 GDPR preveda il trasferimento in USA o in altro paese terzo, cosa deve fare l'azienda?**
  Se è previsto che i dati siano trasferiti verso gli Stati Uniti e non possono essere introdotte misure supplementari agli strumenti per il trasferimento, così da garantire che la normativa statunitense non incida sul livello di protezione sostanzialmente equivalente a quello offerto nel SEE, né si applicano le deroghe di cui all'articolo 49 del RGPD, **l'unica soluzione è negoziare un emendamento o**

una clausola aggiuntiva al contratto per vietare il trasferimento di dati verso gli USA. Analogamente se i dati vengono trasferiti in un altro paese terzo, occorre verificare l'adeguatezza del livello di protezione dei dati garantito dal paese terzo e, se tale livello non può dirsi adeguato nemmeno con l'adozione delle misure supplementari e non ricorre una delle deroghe di cui all'art. 49 GDPR, occorrerà interrompere il trasferimento.

Quindi cosa devono fare le Aziende che trasferiscono i dati in Paesi extra SEE?

EDPB - RACCOMANDAZIONI 01/2020 RELATIVE ALLE MISURE CHE INTEGRANO GLI STRUMENTI DI TRASFERIMENTO DEI DATI

EDPB - Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE



1. Mappatura dei trasferimenti

Occorre innanzitutto conoscere i trasferimenti di dati in Paesi extra SEE che avvengono nell'ambito della propria organizzazione. Nel mappare i trasferimenti, dovrà tenersi conto anche dei trasferimenti successivi, valutando se i responsabili del trattamento al di fuori del SEE trasferiscono i dati personali a sub-responsabili in un altro paese terzo o nello stesso paese terzo.

2. Individuazione del transfer tool

Verificare lo strumento su cui si basa il trasferimento dei dati tra quelli previsti dal Capo V del GDPR.
Se il trasferimento non ha base giuridica né in una decisione di adeguatezza, né in una deroga di cui all'articolo 49, occorrerà passare al terzo step.

3. Valutazione della legislazione o della prassi del paese terzo

Valutare se nel Paese terzo siano adottate leggi o prassi che possono incidere sull'efficacia delle garanzie su cui si basano i trasferimenti. L'esportatore dovrà farsi assistere dall'importatore.

EDPB - Raccomandazioni 02/2020 relative alle garanzie essenziali europee per le misure di sorveglianza

Nel valutare l'ordinamento del Paese Terzo, occorre innanzitutto **verificare se le misure di sorveglianza** che consentono alle Autorità di accedere ai dati trasferiti **costituiscano o meno un'interferenza ingiustificata sui diritti degli interessati.**

Si potrà quindi tenere conto di quanto indicato dall'EDPB nelle **Raccomandazioni 02/2020 relative alle garanzie essenziali europee per le misure di sorveglianza** che costituiscono uno standard di riferimento:

- Il trattamento di dati personali per deve basarsi su **regole chiare, precise e accessibili.**
- Le eventuali limitazioni dei diritti al rispetto della vita privata e alla protezione dei dati devono essere **necessarie e proporzionali rispetto agli obiettivi legittimi perseguiti.**
- Dovrebbe esistere un **meccanismo di controllo indipendente.**
- **La persona deve poter accedere a mezzi di ricorso efficaci** per soddisfare i suoi diritti quando ritiene che essi non siano o non siano stati rispettati.

Ecco alcuni quesiti che possono assistere l'esportatore a valutare l'ordinamento del Paese terzo:

- **Le Autorità** del Paese estero **possono accedere ai dati?**
- Se sì, esistono norme di legge che consentono l'accesso ai dati?
- Se sì, **l'importatore è tenuto a rispettare queste leggi?**
- **Le leggi sono chiare?** I poteri di accesso sono precisamente delineati?
- La natura dei possibili accessi rispecchia il **principio di necessità e la proporzionalità** rispetto agli obiettivi legittimi perseguiti?
- Gli interessati godono di strumenti di tutela, ad esempio **mezzi di ricorso?**
- Il Paese Terzo ha adottato **leggi di protezione dei dati personali?**

4. Misure supplementari

Quando il transfer tool individuato per il trasferimento dei dati è uno degli strumenti di cui all'art. 46 GDPR e al contempo risulta anche che tale meccanismo **non garantisce un livello di protezione sostanzialmente equivalente**, occorrerà individuare e adottare adeguate **misure supplementari**, come individuate nel successivo **punto E**

5. Attuazione delle misure supplementari individuate

I passaggi procedurali da adottare nel caso in cui siano state individuate misure supplementari efficaci da mettere in atto possono essere diversi a seconda dello strumento di trasferimento di cui all'articolo 46 del RGPD che state utilizzando o che prevedete di utilizzare.

6. Rivalutazione periodica

Occorre monitorare costantemente gli eventuali sviluppi normativi del Paese terzo, anche in collaborazione con gli importatori di dati, in quanto gli eventuali cambiamenti potrebbero influenzare l'iniziale valutazione del livello di protezione dei dati. Bisogno sempre tenere a mente che l'accountability è un obbligo permanente.

ESEMPI DI MISURE SUPPLEMENTARI

Le Autorità pubbliche dei Paesi terzi potrebbero godere di poteri di controllo che gli consentono di accedere ai dati trasferiti:

- **in transito** accedendo alle linee di comunicazione utilizzate per trasmettere i dati al paese destinatario.
- **durante la custodia** da parte di un destinatario dei dati, accedendo personalmente alle strutture di trattamento o chiedendo al destinatario dei dati di localizzarli, estrarre i dati di interesse e consegnarli alle Autorità.

ATTENZIONE !

Gli importatori di dati statunitensi che rientrano nel campo di applicazione del titolo 50 U.S.C. § 1881 bis (sezione 702 della FISA) hanno l'obbligo diretto di concedere l'accesso a dati personali importati che sono in loro possesso, custodia o controllo, o di consegnarli.
Ciò può estendersi a qualsiasi chiave crittografica necessaria per rendere i dati intelligibili.
Se all'importatore non si applicano le norme di cui sopra, potrebbero non esserci particolari problemi per il trasferimento dei dati.

MISURE TECNICHE

L'EDPB riporta esempi non esaustivi di misure tecniche, che possono essere adottate ad integrazione delle garanzie previste dagli strumenti di trasferimento di cui all'articolo 46 del GDPR, affinché sia garantito il rispetto del livello di protezione richiesto dal diritto dell'Unione nel contesto di un trasferimento di dati personali verso un paese terzo. Tali misure si rendono particolarmente necessarie qualora la legislazione di tale paese imponga all'importatore di dati obblighi che sono in contrasto con le garanzie previste dagli strumenti di trasferimento di cui all'articolo 46 del GDPR e che sono, in particolare, in grado di **pregiudicare che sia contrattualmente garantito** un livello di protezione **sostanzialmente equivalente** a quello europeo.

Esempio Positivo – CIFRATURA

Un esportatore di dati utilizza un fornitore di servizi di hosting in un paese terzo per conservare dati personali, ad esempio a scopo di backup.

Se

1. I dati personali sono trattati con una **forte cifratura** prima della trasmissione,
2. L'algoritmo di cifratura e la sua parametrizzazione sono conformi allo stato dell'arte
3. La forza della cifratura tiene conto del periodo di tempo specifico durante il quale la riservatezza dei dati personali cifrati deve essere preservata
4. L'algoritmo di cifratura è applicato in modo impeccabile da un software correttamente aggiornato
5. **Le chiavi sono conservate esclusivamente sotto il controllo dell'esportatore di dati, o di altri soggetti incaricati di tale compito che risiedono nel SEE** o in un paese terzo adeguato ex art. 45 GDPR

L'EDPB ritiene che la cifratura fornisca un'efficace misura supplementare.

Esempio Positivo – PSEUDONIMIZZAZIONE

Un esportatore di dati pseudonimizza, in primo luogo, i dati in suo possesso e poi li trasferisce verso un paese terzo per analizzarli, ad esempio a scopo di ricerca.

Se

1. Un esportatore di dati **trasferisce i dati personali trattati in modo tale che non possano più essere attribuiti a un determinato interessato**, né essere utilizzati per individuare l'interessato in un gruppo più ampio, senza l'uso di informazioni aggiuntive
2. Tali **informazioni aggiuntive sono detenute esclusivamente dall'esportatore** di dati e conservate separatamente in uno **Stato membro** o in un paese terzo adeguato
3. La **divulgazione o l'uso non autorizzato di tali informazioni aggiuntive sono impediti da adeguate misure di sicurezza tecniche e organizzative**, si garantisce che l'esportatore di dati mantiene il controllo esclusivo dell'algoritmo o del repository che consente la re-identificazione utilizzando le informazioni aggiuntive
4. Il **titolare del trattamento ha stabilito**, mediante un'analisi approfondita dei dati in questione, tenendo conto di ogni informazione in possesso delle autorità pubbliche del paese destinatario, **che i dati personali pseudonimizzati non possono essere attribuiti a una persona fisica identificata identificabile**, anche se incrociati con tali informazioni

L'EDPB ritiene che la **pseudonimizzazione eseguita può costituire un'efficace misura supplementare**.

Esempio Negativo - TRASFERIMENTO A FORNITORI DI SERVIZI CLOUD O AD ALTRI RESPONSABILI DEL TRATTAMENTO CHE RICHIEDONO L'ACCESSO AI DATI IN CHIARO

Un esportatore di dati ricorre ad un fornitore di servizi cloud o ad un altro responsabile del trattamento per far trattare i dati personali secondo le sue istruzioni in un paese terzo.

Se

1. Un titolare del trattamento **trasferisce i dati a un fornitore di servizi cloud** o a un altro responsabile del trattamento,
2. **Il fornitore di servizi cloud** o altro responsabile del trattamento **deve accedere ai dati in chiaro** per eseguire il compito assegnato
3. Il **potere concesso alle autorità pubbliche del paese destinatario di accedere ai dati trasferiti va oltre quanto necessario e proporzionato in una società democratica**

l'EDPB, considerato **l'attuale stato dell'arte**, non è in grado di prevedere una misura tecnica efficace per impedire che tale accesso violi i diritti degli interessati.

Esempio Negativo - ACCESSO REMOTO AI DATI PER SCOPI COMMERCIALI

Un esportatore di dati consente ad enti di un paese terzo l'accesso da remoto ai dati personali per scopi commerciali condivisi. Un classico esempio può essere costituito da un titolare del trattamento o da un responsabile del trattamento stabilito nel territorio di uno Stato **membro che trasferisce dati personali a un titolare o a un responsabile in un paese terzo appartenente allo stesso gruppo di imprese o a un gruppo di imprese che esercita un'attività economica comune.**
L'importatore di dati può, ad esempio, utilizzare i dati ricevuti per fornire all'esportatore di dati servizi di gestione del personale. Per la fornitura del servizio, quindi l'importatore avrà bisogno di accedere ai dati personali dei dipendenti e dei collaboratori o ai dati di contatto dei clienti dell'esportatore che si trovano nell'UE.

Se

1. **Un esportatore di dati trasferisce dati personali a un importatore di dati in un paese terzo rendendoli disponibili in un sistema informatico di uso comune** in modo da consentire all'importatore l'accesso diretto ai dati di sua scelta, oppure trasferendoli direttamente, singolarmente o in blocco, mediante l'uso di un servizio di comunicazione,
2. **L'importatore utilizza i dati in chiaro per i propri scopi**,
3. Il **potere concesso** alle autorità pubbliche del paese destinatario di accedere ai dati trasferiti **va oltre quanto necessario e proporzionato** in una società democratica

l'EDPB non è in grado di prevedere una misura tecnica efficace per impedire che tale accesso violi i diritti degli interessati.

MISURE CONTRATTUALI

Queste misure consentono di prevedere impegni contrattuali unilaterali, bilaterali o multilaterali volti a rafforzare le garanzie poste a tutela dei dati personali.
Se il trasferimento si basa su uno strumento di cui all'articolo 46 del GDPR, nella maggior parte dei casi esso conterrà già una serie di impegni (per lo più contrattuali) per l'esportatore e l'importatore dei dati, volti a tutelare i dati personali.
Occorre sempre tenere in considerazione che le misure contrattuali non vincolano i poteri di controllo delle Autorità estere: esse dovrebbero essere "combinate" con altre misure tecniche e organizzative affinchè sia assicurato un livello di protezione dei dati sostanzialmente equivalente a quello garantito dall'UE.
Ad esempio, l'esportatore potrà:

- prevedere l'obbligo contrattuale di utilizzare **misure tecniche specifiche** di cui al punto precedente
- prevedere **specifici obblighi di trasparenza**
  1. elencare le leggi e i regolamenti del paese di destinazione applicabili all'importatore o ai relativi responsabili del trattamento che consentirebbero alle autorità pubbliche di accedere ai dati personali
  2. in assenza di leggi che disciplinano l'accesso ai dati da parte delle autorità pubbliche, **fornire informazioni e statistiche** basate sull'esperienza dell'importatore o su relazioni provenienti da varie fonti sull'accesso ai dati da parte delle autorità pubbliche
  3. indicare **quali misure sono adottate per impedire l'accesso** ai dati trasferiti
  4. fornire informazioni sufficientemente dettagliate su tutte le richieste di accesso ai dati personali da parte delle autorità pubbliche che l'importatore ha ricevuto in un determinato periodo di tempo
  5. specificare se e in quale misura all'importatore è legalmente vietato fornire le informazioni.

L'esportatore potrebbe rafforzare il suo potere di effettuare verifiche o ispezioni delle strutture di trattamento dei dati dell'importatore, in loco e/o da remoto, al fine di verificare se i dati sono stati divulgati alle autorità pubbliche e a quali condizioni (accesso non oltre quanto necessario e proporzionato in una società democratica), ad esempio prevedendo un breve preavviso e meccanismi che garantiscano il rapido intervento degli organismi di controllo e rafforzino l'autonomia dell'esportatore nella scelta degli stessi.

- prevedere **l'obbligo di intraprendere azioni specifiche**
  L'importatore dovrebbe impegnarsi a verificare che l'eventuale ordine dell'Autorità di accedere o comunicare i dati personali sia legittimo, ossia conforme alla normativa del paese di destinazione. Se, dopo un'attenta valutazione, l'importatore conclude che esso non rientri tra i poteri di controllo

concessi all'Autorità richiedente, dovrebbe impegnarsi a contestare l'ordine dell'Autorità e chiedere misure provvisorie che ne sospendano gli effetti sino ad un'eventuale pronuncia del tribunale nel merito. L'importatore dovrebbe inoltre impegnarsi a fornire solo i dati personali strettamente necessari a ad adempiere all'ordine delle Autorità.

- **consentire agli interessati di esercitare i loro diritti**

    1. Il contratto potrebbe prevedere che si possa accedere ai dati personali trasmessi in chiaro nel corso della normale attività commerciale (anche in casi di supporto) solo con il consenso espresso o implicito dell'esportatore e/o dell'interessato.
    2. Il contratto potrebbe obbligare l'importatore e/o l'esportatore a comunicare tempestivamente all'interessato la richiesta o l'ordine ricevuto dalle autorità pubbliche del paese terzo, o l'impossibilità da parte dell'importatore di rispettare gli impegni contrattuali, per consentire all'interessato di ottenere informazioni e ricorrere ad un mezzo di ricorso effettivo (ad esempio presentando un reclamo all'autorità di controllo competente e/o all'autorità giudiziaria e dimostrando la sua posizione dinanzi ai tribunali del paese terzo).

MISURE ORGANIZZATIVE

Le misure organizzative possono consistere in politiche interne, metodi organizzativi e standard che i titolari del trattamento e i responsabili del trattamento potrebbero applicare a se stessi e imporre agli importatori di dati in paesi terzi.

Esse possono contribuire a garantire la coerenza della protezione dei dati personali durante l'intero ciclo del trattamento.

La selezione e l'attuazione di una o più di queste misure non garantirà necessariamente e sistematicamente che il trasferimento soddisfi gli standard di sostanziale equivalenza richiesti dal diritto dell'Unione.

A seconda delle circostanze specifiche del trasferimento e della valutazione effettuata sulla legislazione del paese terzo, saranno necessarie misure organizzative che avdano ad integrare le misure contrattuali e/o tecniche, così da garantire un livello di protezione dei dati personali sostanzialmente equivalente a quello garantito all'interno dell'UE.
Esempi di misure organizzative possono essere:

- prevedere **politiche interne per la governance dei trasferimenti, in particolare con i gruppi di imprese,** come l'adozione di adeguate politiche interne con

    a. una **chiara attribuzione delle responsabilità per il trasferimento dei dati**,

b. **canali di segnalazione e procedure operative standard** per i casi di richieste di accesso ai dati da parte di autorità pubbliche, occulte o ufficiali.

Soprattutto in caso di trasferimenti tra gruppi di imprese, tali politiche possono includere, tra l'altro

a. la nomina di un **team specifico**, che dovrebbe avere **sede all'interno del SEE**, composto da esperti in materia di informatica, protezione dei dati e leggi sulla privacy, per trattare le richieste che riguardano dati personali trasferiti dall'UE;

b. la **comunicazione** alla direzione legale e aziendale e all'esportatore di dati **al ricevimento di tali richieste**;

c. i **passaggi procedurali per contestare richieste** sproporzionate o illegali e la fornitura di informazioni trasparenti agli interessati.

- prevedere **misure per la trasparenza e la responsabilizzazione**

  Documentare e registrare le richieste di accesso ricevute dalle autorità pubbliche e la risposta fornita, insieme alla motivazione giuridica e ai soggetti coinvolti (ad esempio se l'esportatore è stato informato e la sua risposta, la valutazione del team incaricato di trattare tali richieste, ecc.). Tali registrazioni dovrebbero essere messe a disposizione dell'esportatore, che dovrebbe a sua volta fornirle agli interessati, se necessario.

- prevedere l'adozione di tecniche di minimizzazione dei dati

  Applicare la **minimizzazione dei dati, al fine di limitare l'esposizione dei dati personali ad accessi non autorizzati**. Ad esempio, in alcuni casi **potrebbe non essere necessario trasferire determinati dati** (ad esempio, in caso di accesso remoto ai dati SEE, come nei casi di supporto, quando è concesso l'accesso limitato invece di un accesso completo; oppure quando la fornitura di un servizio richiede solo il trasferimento di un set di dati limitato e non di un'intera banca dati).

ATTENZIONE !

Le misure contrattuali non hanno efficacia vincolante nei confronti delle autorità pubbliche.

Quindi, affinché siano efficaci, dovrebbero sempre essere accompagnate da misure tecniche ed organizzative.

Di fatto le **misure tecniche potrebbero essere le uniche a fare la differenza.**

Qualora non sia possibile adottare misure tecniche, i trasferimenti dei dati dovrebbero essere sospesi oppure, se si ritiene di procedere, gli esportatori potrebbero limitarsi a mappare tutti i trasferimenti di dati, tenendo però conto che questà attività non copre in ogni caso l'Azienda dai rischi connessi ad un illegittimo trasferimento.

LE NUOVE STANDARD CONTRACTUAL CLAUSES

Il 12 novembre 2020 la Commissione europea ha pubblicato la **bozza delle nuove Calusole Contrattuali Standard (SCC).**

Quali novità?

Le SCC non prevedono più la dicotomia:

titolare ⟶ titolare

titolare ⟶ responsabile

Saranno invece previsti 4 moduli:

titolare ⟶ titolare

titolare ⟶ responsabile

responsabile ⟶ responsabile

responsabile ⟶ sub-responsabile

Il nuovo documento allinea il nuovo modello di SCC al GDPR. Esso si propone di disciplinare meglio i "trasferimenti più complessi" che vedono coinvolti più esportatori e/o più importatori.
Vi si prevedono garanzie specifiche per affrontare le implicazioni concrete delle legislazioni dei paesi terzi e in particolare come gestire le richieste vincolanti delle autorità pubbliche del paese terzo per la divulgazione delle informazioni trasferite.

Il 14 gennaio 2021

l'European Data Protection Supervisor e l'European Data Protection Board hanno reso un parere congiunto sulla bozza delle nuove SCC.

Nel Parere, l'EDPS e l'EDPB hanno invitato la Commissione europea a chiarire, tra vari aspetti:

- che **le nuove clausole potrebbero non essere sufficienti da sole** a garantire un livello di protezione sostanzialmente equivalente a quello europeo e che, in tal caso, esse dovranno essere adottate congiuntamente alle "misure supplementari" di cui alla raccomandazione 01/2020;
- se e come i progetti di SCC si applicano ai **rapporti di contitolarità**;
- che la **combinazione di diversi moduli** nello stesso documento non dovrebbe portare all'**offuscamento dei ruoli privacy e delle responsabilità** dei soggetti coinvolti nel trasferimento.

La finalizzazione del documento è prevista per questa primavera.

L'AUTRICE

dott.ssa Federica Pucarelli

Laureata in Giurisprudenza all'Alma Mater di Bologna, ha successivamente ottenuto il Master di Specializzazione di I livello in Trattamento dei dati personali e Privacy Officer presso CIRSFID - Alma Mater Studiorum Università di Bologna.

Fin dal suo ingresso nello Studio Legale Stefanelli&Stefanelli si occupa di privacy e in particolare degli aspetti legati alla protezione dei dati in sanità, mappatura di processi aziendali, redazione e verifica di procedure organizzative.

Studio legale Stefanelli&Stefanelli

Sedi
Bologna: Via Azzo Gardino 8/A - 40122
Milano: Via Nino Bixio, 31 - 20129
Roma: Palazzo Marignoli - Piazza di San Silvestro, 8 - 00187
Venezia: Sestiere Castello 2388 - 30122

E-mail: info@studiolegalestefanelli.it

Edizione: aprile 2021