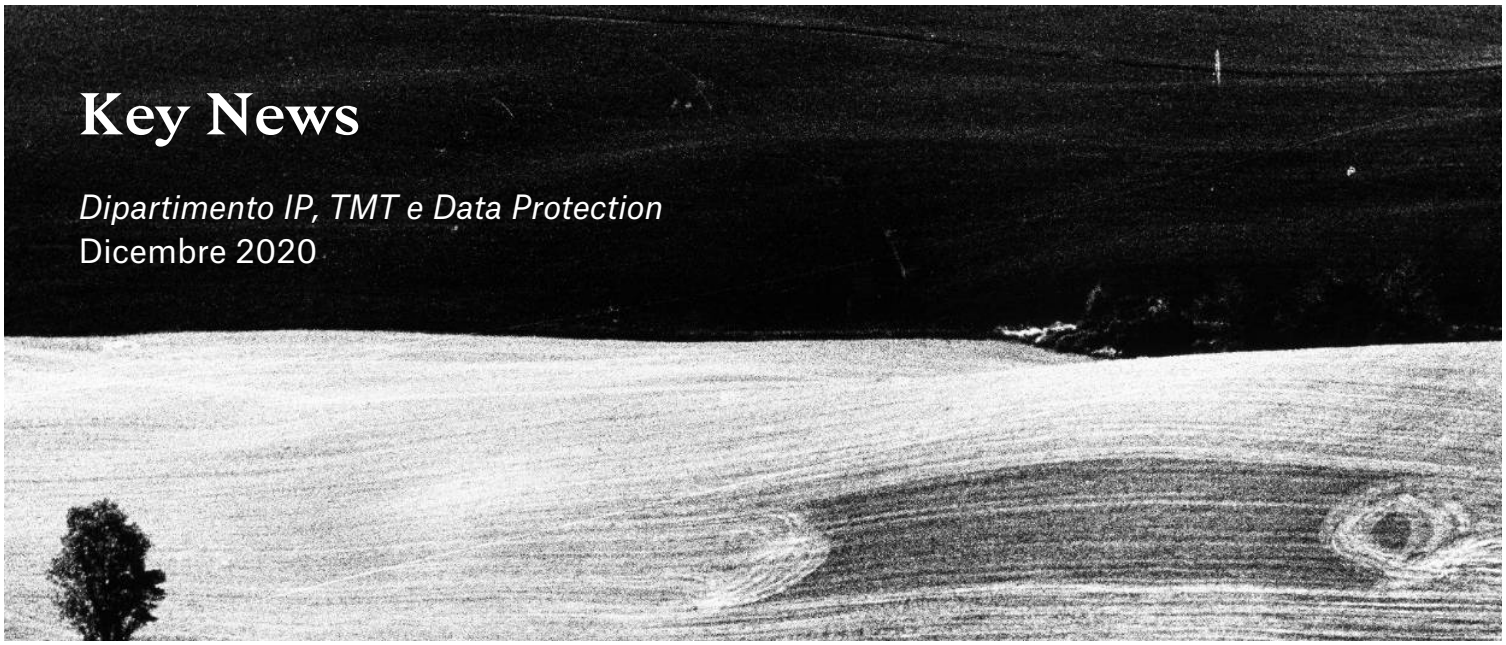
CHIOMENTI



Key News

Dipartimento IP, TMT e Data Protection
Dicembre 2020

Indice

I Raccomandazioni EDPB sulle "misure supplementari" in materia di trasferimenti di dati personali all'estero

II Raccomandazioni EDPB sulle garanzie essenziali europee relativamente alle misure di sorveglianza

III Strategia EDPS per l'Unione, le istituzioni, gli uffici, gli organi e le agenzie per adeguarsi alla sentenza *Schrems II*

IV Decisione della Commissione Europea – Clausole contrattuali standard per i trasferimenti di dati personali all'estero

V La prima decisione "post-*Schrems II*" relativa ai trasferimenti di dati personali emanata dall'Autorità di controllo svedese.

Definizioni

CGUE	Corte di Giustizia dell'Unione Europea
EDPB	European Data Protection Board ("Comitato Europeo per la Protezione dei Dati")
EDPS	European Data Protection Supervisor ("Garante Europeo della Protezione dei Dati")
GDPR	Regolamento (UE) 2016/679
SEE	Spazio Economico Europeo
DPA Svedese	Autorità di controllo svedese – *Datainspektionen*

Il trasferimento dei dati personali all'indomani della sentenza *Schrems II*: alcune considerazioni preliminari

Con la pronuncia del 16 luglio 2020 nel caso *Schrems II* (causa C-311/18) – ne avevamo parlato approfonditamente qui – la CGUE è ritornata sul tema dei trasferimenti dei dati personali all'estero, dichiarando l'invalidità del c.d. Privacy Shield UE-USA (istituito con la Decisione di esecuzione (UE) 2016/1250 della CE). Quest'ultimo non avrebbe garantito

il rispetto da parte degli Stati Uniti del principio di adeguatezza del livello di protezione dei dati personali trasferiti dallo SEE, come sancito dal GDPR. In particolare, la decisione si fonda su due ordini di motivi:

i. la prevalenza data nel sistema giuridico statunitense alle esigenze di sicurezza nazionale e all'interesse pubblico, rispetto ai diritti fondamentali dei cittadini, che giustifica la possibilità di ingerenze da parte delle autorità statunitensi nell'ambito di controlli pubblici e programmi di sorveglianza dei servizi di intelligence; e

ii. la mancanza di un adeguato livello di protezione rispetto ai cittadini UE interessati, ai quali non si riconoscono diritti azionabili e mezzi di ricorso effettivi.

Oltre a rendere illegittimo qualsiasi trasferimento di dati personali verso gli USA basato sul Privacy Shield UE-USA, nella medesima decisione la CGUE ha avuto modo di soffermarsi sul funzionamento del meccanismo delle clausole contrattuali standard, rendendo effettivo il rischio di generare incertezza giuridica in merito al giudizio di adeguatezza, alla luce del GDPR, necessario ai fini dei trasferimenti di dati personali verso i paesi al di fuori dello SEE.

Recentemente, le Autorità europee hanno cercato di fornire risposta con una serie di interventi illustrati nel prosieguo:

- l'adozione di linee guida, raccomandazioni e proposte che mirano a fornire agli operatori, intenzionati a proseguire con trasferimenti di dati personali extra-SEE, supporto nell'individuazione ed implementazione delle necessarie azioni e misure supplementari di garanzia da adottare (**v. paragrafi I, II e III della presente Newsletter**);
- la predisposizione di un nuovo set di clausole contrattuali standard per i trasferimenti extra-SEE (**v. paragrafo IV della presente Newsletter**).

Se il quadro risultante risponde a numerosi interrogativi sorti a valle della decisione *Schrems II*, esso sancisce un aggravio per gli operatori – economici e istituzionali – chiamati, nell'esercizio della propria *accountability*, non solo a mettere in atto una serie di misure in relazione ai trasferimenti extra-SEE, ma anche a svolgere un vero e proprio *assessment* sulla legge o la prassi del paese terzo di riferimento.

Anche l'eventuale stipula del nuovo set di clausole contrattuali *standard* – che sarà obbligatoria in seguito al periodo transitorio o, nel corso del medesimo, al di fuori di talune circostanze "esimenti" (**v. paragrafo IV della presente Newsletter**) – non solleverebbe gli operatori dall'obbligo di condurre il suddetto *assessment*. Tale set configura, piuttosto, un quadro generale di obblighi e step necessari per la conduzione dell'*assessment*, nonché per la gestione di scenari critici (e.g. richieste provenienti dalle forze dell'ordine straniere or agenzie di *intelligence*).

In sintesi, prima di effettuare trasferimenti extra-SEE gli operatori dovranno assicurarsi, da un lato, che legge o la prassi del paese terzo di riferimento non mettano a repentaglio le garanzie della protezione dei dati e, dall'altro lato, implementare le opportune misure di sicurezza. In secondo luogo, nel corso dei trasferimenti, gli operatori – nel quadro del principio di *accountability* – dovranno monitorare su base costante l'evoluzione di tali leggi e prassi, nonché l'adeguatezza le misure implementate di destinazione, al fine di individuare e gestire potenziali cambiamenti pregiudizievoli nel livello di protezione dei dati personali oggetto di trasferimento.

Quale prima decisione concernente i trasferimenti di dati personali all'estero in seguito alla sentenza *Schrems II* – ancorché "non applicabile" al momento degli eventi in considerazione – quella della DPA svedese è sicuramente degna di nota (**v. paragrafo V della presente Newsletter**).

I RACCOMANDAZIONI EDPB SULLE "MISURE SUPPLEMENTARI" IN MATERIA DI TRASFERIMENTI DI DATI PERSONALI ALL'ESTERO

L'EDPB ha adottato, in data 10 novembre 2020, le "*Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*" (le "**Raccomandazioni**"), attualmente sottoposte a consultazione pubblica.

Con le proprie Raccomandazioni, l'EDPB intende fare luce sulle "salvaguardie supplementari" o "misure supplementari" agli strumenti di trasferimento elencati all'articolo 46.2 del GDPR, di cui alla sentenza *Schrems II*, che gli esportatori di dati sono chiamati ad adottare per garantire il rispetto del livello di protezione in un determinato paese terzo richiesto dalla legislazione dell'UE, fornendo una metodologia per determinare se e quali misure supplementari devono essere poste in essere per i loro trasferimenti in base al principio di *accountability* su cui si basa il GDPR.

A tal fine, le Raccomandazioni prevedono una *road map* delle misure che i *data exporters* (siano essi titolari del trattamento o responsabili del trattamento) devono adottare per stabilire se sia necessaria l'adozione di tali misure supplementari. Detta *road map* consiste nelle sei fasi seguenti, che sono esaminate e trattate più in dettaglio nel testo delle Raccomandazioni:

I. Identificazione dei trasferimenti: quale fase preliminare rispetto a qualsiasi trasferimento, si consiglia agli esportatori di dati di registrare e mappare (ad esempio, nel registro dei trattamenti) tutti i trasferimenti, ivi inclusi quelli da un importatore di dati situato in un paese terzo verso un altro paese terzo, nonché di verificare il rispetto degli obblighi di informazione nei confronti degli interessati e del principio di minimizzazione dei dati. L'EDPB chiarisce che anche l'accesso remoto da un paese terzo e/o la memorizzazione in un *cloud* situato al di fuori del SEE devono considerarsi quali trasferimenti.

II. Identificazione dei meccanismi di trasferimento: a seguito dell'identificazione dei trasferimenti in questione, i *data exporters* devono identificare i relativi meccanismi di trasferimento dei dati su cui si basa il trasferimento, tra quelli previsti dal capitolo V del GDPR (*e.g.* decisioni di adeguatezza, clausole contrattuali tipo, norme vincolanti d'impresa, deroghe, ecc.).

III. Valutazione della legge del paese terzo: se un trasferimento si basa su uno dei meccanismi previsti dall'articolo 46 del GDPR (comprese le clausole contrattuali tipo e le norme vincolanti d'impresa), gli esportatori di dati devono valutare se la legge o la prassi del paese terzo può impedire all'importatore di adempiere agli obblighi previsti dal meccanismo su cui il trasferimento si fonda. Tale valutazione – che deve tenere in considerazione anche la natura, l'ambito di applicazione e il contesto del trasferimento – può essere effettuata con la collaborazione dell'importatore, ovvero facendo altresì riferimento ad altre fonti di informazione che sono elencate in modo non esaustivo nell'Allegato 3 alle Raccomandazioni (*e.g.*, la giurisprudenza della CGUE, risoluzioni e relazioni di organizzazioni intergovernative, relazioni di istituzioni accademiche e ONG, ecc.).

IV. Adozione di misure supplementari: qualora, dalla valutazione di cui *supra*, risulti che il meccanismo di cui all'articolo 46 del GDPR su cui il trasferimento di dati è basato non è efficace nel caso specifico, i *data exporters* devono adottare le misure supplementari necessarie per garantire che il livello di protezione dei dati trasferiti nel paese terzo sia sostanzialmente equivalente a quello previsto dalla legislazione dell'UE. Esempi di possibili misure supplementari, le quali vanno comunque individuate caso per caso, sono elencati in modo non tassativo nell'Allegato 2 alle Raccomandazioni e comprendono (i) misure tecniche; (ii) misure contrattuali; e (iii) misure organizzative.

V. Fasi procedurali dopo l'identificazione delle misure supplementari: a seconda di quale meccanismo di trasferimento di dati di cui all'articolo 46 del GDPR è stato adottato nel caso di specie, i *data exporters* devono mettere in atto tutte le misure procedurali formali che possono essere necessarie per l'efficace attuazione delle protezioni necessarie.

VI. Rivalutazione a intervalli adeguati: i *data exporters* devono monitorare su base costante l'evoluzione delle leggi del paese terzo di destinazione (anche, se del caso, con la collaborazione dei *data importers*), in modo da individuare e affrontare – alla luce del principio di *accountability* – potenziali cambiamenti pregiudizievoli nel livello di protezione dei dati personali offerto da tale paese terzo.

Si noti che, secondo l'EDPB, le anzidette valutazioni e attività devono essere adeguatamente documentate per poter essere prontamente rese disponibili in caso di richiesta da parte dell'autorità di controllo competente.

I soggetti interessati sono invitati a trasmettere eventuali commenti entro il 21 dicembre 2020.

Qui il *link* dove poter visionare il testo delle Raccomandazioni.

II RACCOMANDAZIONI EDPB SULLE GARANZIE ESSENZIALI EUROPEE RELATIVAMENTE ALLE MISURE DI SORVEGLIANZA

Il 10 novembre 2020, l'EDPB ha altresì adottato le "*Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*" (le "**Raccomandazioni EEG**"), complementari alle Raccomandazioni. Infatti, nell'ambito della Fase 3 di cui alle Raccomandazioni, un ruolo significativo è dato alle leggi che consentono l'accesso ai dati personali da parte delle autorità pubbliche nei settori dell'*enforcement* penale, del controllo regolatorio e della sicurezza nazionale.

Le Raccomandazioni EEG intendono fornire agli esportatori di dati, elementi utili al fine di valutare l'adeguatezza del livello di protezione offerto nel paese terzo dal quadro giuridico che disciplina l'accesso delle autorità pubbliche ai dati per fini di sorveglianza.

Si tratta di standard di riferimento, elaborati sulla base del diritto dell'Unione Europea, della giurisprudenza della CGUE e della Corte Europea dei Diritti dell'Uomo, da tenere in considerazione nel valutare se l'accesso ai dati personali da parte delle autorità pubbliche nei settori dell'*enforcement* penale e della sicurezza nazionale, possa ritenersi un'interferenza giustificabile, non contraria ai diritti fondamentali alla *privacy* e alla protezione dei dati personali sanciti dagli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea.

L'EPDB ha individuato quattro differenti garanzie europee essenziali (*European Essential Guarantees* - "**EEG**"), la cui sussistenza rende giustificabili le misure di sorveglianza adottate dallo stato terzo, in quanto ritenute coerenti con gli standard europei:

I. Il trattamento dei dati deve basarsi su regole chiare, precise e accessibili. Ogni ingerenza nei diritti dell'interessato deve essere prevista dalla legge, la quale dovrà definire la portata di ogni limitazione ai diritti fondamentali e prevedere la possibilità di azionare tali diritti in caso di ingerenza arbitraria e abusiva. La legge dovrà prevedere, *inter alia*, una definizione delle categorie di soggetti che potrebbero essere soggetti a sorveglianza, un limite di durata a tale misura, le procedure da seguire nell'esaminare, usare e conservare i dati ottenuti e le cautele necessarie per comunicare i dati a terze parti.

II. La necessità e la proporzionalità delle finalità perseguite devono essere dimostrate. Per poter essere considerata conforme al principio di proporzionalità, la legge stessa dovrà individuare i limiti al potere delle autorità pubbliche di interferire con i diritti degli interessati nell'ambito dei programmi di sorveglianza e i limiti imposti alle autorità pubbliche nell'aver accesso e all'uso dei dati raccolti, nel rispetto del principio di necessità.

III. Previsione di un meccanismo di controllo indipendente ed imparziale, condotto da un giudice o altro organo indipendente in relazione a tutte le fasi della attività di sorveglianza al fine di individuare eventuali violazioni dei diritti degli interessati.

IV. Previsione di rimedi efficaci a disposizione dei soggetti interessati al fine di garantire loro la possibilità di azionare i propri diritti qualora ritengano questi siano stati violati, al fine di avere accesso ai propri dati, di ottenerne la rettifica o la cancellazione degli stessi. L'EDPB rileva come l'efficacia di un tale rimedio sia intrinsecamente collegata ad una preventiva notificazione al soggetto interessato della misura di sorveglianza, una volta che tale attività sia terminata. In ogni

caso, anche in assenza di preventiva notificazione, dovrà essere previsto un effettivo rimedio legale. In altri termini, dovrà essere possibile rivolgersi a un tribunale o altro organo imparziale ed indipendente autorizzato ad assumere decisioni in grado di vincolare i servizi di *intelligence*.

Nei suoi commenti finali, l'EDPB evidenza come le suddette EEG dovranno valutarsi congiuntamente e non in modo indipendente l'una dall'altra, al fine di determinare un'eventuale ingerenza rispetto ai diritti fondamentali alla privacy e alla protezione dei dati personali. A seguito di tale valutazione, sarà, pertanto, possibile stabilire se la legislazione dello Stato terzo garantisca o meno un livello di protezione essenzialmente equivalente a quello garantito dalla normativa dell'UE.

Le Raccomandazioni EEG sono accessibili a questo *link.*

III STRATEGIA EDPS PER L'UNIONE, LE ISTITUZIONI, GLI UFFICI, GLI ORGANI E LE AGENZIE PER ADEGUARSI ALLA SENTENZA "*SCHREMS II*"

Lo European Data Protection Supervisor (o Garante europeo della protezione dei dati) è l'autorità di controllo indipendente istituita dall'articolo 56 del Regolamento (UE) 2018/1725 ("**Regolamento**"). È compito dell'EDPS, ai sensi dell'art. 57, par. 1, lett. a) ed f), del Regolamento, monitorare e garantirne l'applicazione per quanto riguarda il trattamento dei dati personali da parte di istituzioni, organi, uffici e agenzie ("**IUE**"), anche utilizzando i propri poteri investigativi e correttivi ai sensi dell'art. 58, par. 1 e 2.

Il 29 ottobre 2020, l'EDPS ha pubblicato un documento strategico volto a monitorare la conformità delle IUE alla sentenza *Schrems II* in relazione ai trasferimenti di dati personali verso paesi terzi, in particolare verso gli Stati Uniti. L'obiettivo è che i trasferimenti internazionali in corso e quelli futuri siano effettuati in conformità alla normativa sulla protezione dei dati dell'UE.

Sebbene la strategia in questione miri a rendere tutti i trasferimenti conformi alla sentenza *Schrems II* a medio termine, l'EDPS ha identificato due priorità da affrontare a breve termine: i contratti tra titolare e responsabile del trattamento e / o i contratti tra responsabile e sub-responsabile che comportano trasferimenti di dati a paesi terzi, con un'attenzione particolare rispetto a quelli effettuati verso negli Stati Uniti.

È in questo contesto che l'EDPS ha sviluppato un piano d'azione, distinguendo tra azioni di conformità a breve e medio termine.

Come azione di conformità a **breve termine**, il 5 ottobre 2020 l'EDPS ha ordinato alle EUI di completare una mappatura al fine di identificare quali contratti in corso, procedure di appalto e altri tipi di cooperazione comportano trasferimenti di dati. Le IUE dovrebbero riferire all'EDPS su alcuni tipi di trasferimenti. Si tratta di trasferimenti che non hanno una base giuridica, trasferimenti che si basano su deroghe e trasferimenti a soggetti privati verso gli Stati Uniti che presentano rischi elevati per gli interessati. Per quanto riguarda le nuove operazioni di trattamento o i nuovi contratti con i fornitori di servizi, l'EDPS incoraggia fortemente le IUE a evitare attività di trattamento che comportano trasferimenti di dati personali verso gli Stati Uniti.

Relativamente alle azioni di conformità a **medio termine**, il l'EDPS promuove l'adozione di azioni di conformità affinché ci sia una valutazione, caso per caso, dei trasferimenti verso gli Stati Uniti o verso altri paesi terzi. Le IUE saranno invitate a eseguire, di volta in volta, puntuali valutazioni sull'impatto del trasferimento (TIA) per verificare se il paese di destinazione sia in grado di garantire un livello di protezione sostanzialmente equivalente a quello previsto nell'Unione Europea. Sulla base di queste valutazioni che devono essere effettuate con l'aiuto dei soggetti c.d. "importatori di dati", le IUE dovrebbero decidere se sia possibile continuare i trasferimenti identificati in fase di mappatura. Le IUE saranno invitate a riferire all'EDPS sull'uso delle deroghe - come previste dall'art. 50 del Regolamento - sui trasferimenti che vengono proseguiti verso un paese terzo che non ha un livello di protezione sostanzialmente equivalente, e sui

trasferimenti che sono sospesi o cessati per l'assenza di un livello di protezione sostanzialmente equivalente nel paese di destinazione. Sulla base di questo primo esercizio di analisi e reportistica, l'EDPS si riserva il diritto di intraprendere azioni esecutive per rendere tali trasferimenti conformi al Regolamento o per sospenderli, se del caso.

L'EDPS intende, inoltre, esplorare la possibilità di **valutazioni congiunte** del livello di protezione dei dati personali offerto nei paesi terzi al fine di fornire orientamenti ai titolari del trattamento.

Infine, si noti che nel contesto dell'EDPB, l'EDPS sta lavorando – con le altre autorità per la protezione dei dati europee – allo sviluppo di ulteriori orientamenti e raccomandazioni per assistere i titolari e i responsabili del trattamento nei loro doveri per identificare e attuare misure supplementari appropriate per garantire un livello adeguato di protezione durante il trasferimento di dati verso paesi terzi.

IV DECISIONE DELLA COMMISSIONE EUROPEA – CLAUSOLE CONTRATTUALI STANDARD PER I TRASFERIMENTI DI DATI PERSONALI ALL'ESTERO

Non è una coincidenza il fatto che la CE abbia pubblicato la propria bozza di Decisione di esecuzione[1] ("**Decisione**") insieme a un nuovo *set* – ivi allegato – di clausole contrattuali standard per i trasferimenti di dati personali all'estero ("**Draft SCCs**"), facendo immediato seguito alle Raccomandazioni dell'EDPB **(v. paragrafo I della presente Newsletter)**.

Qui sotto abbiamo elencato alcuni punti chiave della Decisione e delle Draft SCCs, alla cui fase di consultazione pubblica (conclusasi il 10 dicembre 2020) farà seguito la procedura di approvazione da parte degli Stati membri UE con il parere dell'EDPB e dell'EDPS (c.d. "comitatologia")[2].

FINALITÀ – La Decisione risponde alle seguenti finalità:

- Fornire un modello di clausole contrattuali standard in linea con il GDPR e coerente con i principi sanciti nel quadro del caso *Schrems II* (con ciò superando i modelli esistenti, ancorati alla Direttiva 95/46/EC[3]);
- ammodernare i modelli esistenti *vis-à-vis* gli sviluppi nell'economia digitale, l'uso diffuso di nuove e più complesse operazioni e catene di trattamento così come le evolute relazioni commerciali;
- impiegare un approccio più flessibile *vis-à-vis* i molteplici scenari e ruoli di esportatori e importatori di dati personali, nonché le ulteriori parti che si uniscano ai rapporti contrattuali esistenti.

PERIMETRO – Le Draft SCCs abbinano clausole generali a un'impostazione modulare, per soddisfare i diversi scenari nei quali è necessaria una legittimazione dei trasferimenti di dati all'estero. In particolare, esse possono essere concluse tra le seguenti 4 coppie:

	(A)	(B)	(C)	(D)
Esportatore	**Titolare**	**Titolare**	**Responsabile**	**Responsabile**
Importatore	**Titolare**	**Responsabile**	**(Sub)Responsabile**	**Titolare**

È opportuno notare che le Draft SCCs:

[1] *Commission Implementing Decision (EU) on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.*

[2] V. art. 93 del GDPR e il Regolamento (UE) 182/2011 (qui il link alla pagina descrittiva del sito della CE).

[3] Si fa riferimento alle clausole contrattuali definite dalla Decisone 2001/497/CE, come successivamente modificata, e la Decisione 2010/87/UE.

- possono essere impiegate anche là dove l'esportatore stesso non abbia sede in UE, ma il trattamento rientri nell'ambito di applicazione del GDPR[4];
- permettono alle parti di soddisfare, al tempo stesso, gli obblighi (di cui all'art. 28 del GPDR) relativi agli accordi sul trattamento di dati personali: ove un importatore (responsabile del trattamento) accettasse le Draft SCCs – non negoziabili e intrinsecamente sfavorevoli per i responsabili del trattamento – ciò eliminerebbe la necessità di un separato accordo sul trattamento di dati personali e abbatterebbe i costi negoziali;
- possono essere oggetto di adesione da parte di ulteriori titolare e responsabili – con il consenso delle parti iniziali – mediante la compilazione e sottoscrizione degli appositi *Annexes* ivi acclusi (v. *infra*);

CLAUSOLE – Il corpo delle Draft SCCs è suddiviso in diversi moduli, a seconda delle coppie (A), (B), (C) e (D) illustrate nella tabella suesposta. Ad ogni modo, nei vari moduli rimane inalterato il nucleo essenziale di obblighi e principi (*e.g.* le disposizioni relative alla trasparenza, sicurezza, limitazione della conservazione, minimizzazione, ai diritti azionabili e agli strumenti legali cui possono ricorrere i soggetti interessati etc.) che rispecchiano quelli del GDPR i quali, pertanto, diventano contrattualmente vincolanti in capo agli importatori che non vi siano soggetti. A questo riguardo:

- le parti restano libere di includere le Draft SCCs all'interno di un accordo più ampio, nonché di aggiungere ulteriori clausole o salvaguardie, purché queste ultime siano supplementari e compatibili con quelle delineate nelle Draft SCCs (la stessa CE incoraggia le parti ad adottarle);
- oltre a fare affidamento sulle SCCs, gli esportatori dovranno comunque adempiere agli obblighi generalmente incombenti sui medesimi in qualità di titolari ovvero di responsabili ai sensi del GDPR (*e.g.* fornendo idonea informativa ai soggetti interessati);
- le parti dovrebbero essere in grado di dimostrare la conformità alle Draft SCCs, in particolare: (i) l'importatore dovrà conservare idonea documentazione relativa alle attività di trattamento sotto la propria responsabilità e informare tempestivamente l'esportatore nel caso in cui non sia in grado di garantire tale conformità; (ii) l'esportatore dovrà sospendere il trasferimento e, in casi particolarmente gravi, avrà il diritto di risolvere il relativo accordo contrattuale con l'importatore che sia in violazione delle o incapace di assicurare la propria conformità alle Draft SCCs.

ANNEXES – Le Draft SCCs includono i seguenti *Annexes* per opportuna compilazione e sottoscrizione delle parti:

- *Annex I.A – List of Parties* – per l'inserimento dei dati identificativi delle parti alle Draft SCCs.
- *Annex I.B – Description of the transfer(s)* – per l'indicazione dei dettagli delle attività di trattamento relative ai trasferimenti (*e.g.* categorie di dati personali, finalità del trasferimento, periodo di conservazione etc.).
- *Annex II – Technical and organizational measures* – per l'elencazione delle misure di sicurezza tecniche e organizzative che l'importatore dovrà implementare. Le prescrizioni in materia di sicurezza sono cruciali nell'ambito delle Draft SCCs, come emerge anche dalla lista dettagliata di misure esemplificative fornita dalla CE (la quale ha così indicato, implicitamente, le proprie aspettative).
- *Annex III – List of Sub-Processors* – per l'indicazione dei sub-responsabili – vuoi già autorizzati dall'esportatore (in virtù di specifica autorizzazione preventiva fornita all'importatore) vuoi previsti per essere ingaggiati dall'importatore (ove l'esportatore gli abbia concesso un'autorizzazione generale) – in ogni caso da mantenere aggiornata.

[4] Ossia quando le attività di trattamento riguardano *(a)* l'offerta di beni o la prestazione di servizi ai suddetti interessati in UE, oppure *(b)* il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'UE (art. 3, par. 2 del GDPR).

LEGGE STRANIERA – Da notare che la stipula delle Draft SCCs non solleverebbe l'esportatore dall'obbligo di condurre il proprio *assessment* relativo alla legge e alle prassi del paese terzo cui è soggetto l'importatore – come evidenziato anche nelle Raccomandazioni **(v. paragrafo I della presente Newsletter)** – le Draft SCCs configurando, piuttosto, un quadro generale di obblighi e *step* necessari per l'effettuazione di tale *assessment* e per la gestione di scenari critici (*e.g.* richieste provenienti dalle forze dell'ordine straniere or agenzie di *intelligence*).

Al momento dell'accordo relativo alle Draft SCCs, le parti dovrebbero assicurarsi di non avere ragioni per ritenere che la legge o la prassi del paese terzo cui è soggetto l'importatore non siano in linea con le prescrizioni delle Draft SCCs.

PERIODO TRANSITORIO – Durante un periodo transitorio di 1 anno – dalla data di entrata in vigore delle SCCs – gli esportatori e gli importatori potranno continuare ad avvalersi dei modelli esistenti di clausole contrattuali standard, nella misura in cui:

- ciò sia legato all'esecuzione di un contratto concluso tra di loro prima della suddetta data;
- durante il periodo transitorio tale contratto non subisca modifiche, fatta eccezione per le misure supplementari **(v. paragrafo I della presente Newsletter)**.

La necessità di adottare le nuove SCCs durante il periodo transitorio, ove determinatasi sul piano del rapporto titolare/responsabile, avrà un effetto a cascata su quello responsabile/sub-responsabile.

In seguito al periodo transitorio o al di fuori delle circostanze "esimenti" sopra evidenziate, per poter essere conformi alla normativa di *data protection*, le parti interessati dovranno *inter alia* revisionare la propria documentazione contrattuale esistente e adottare le nuove Draft SCCs.

V LA PRIMA DECISIONE "POST-*SCHREMS II*" RELATIVA AI TRASFERIMENTI DI DATI PERSONALI EMANATA DALL'AUTORITÀ DI CONTROLLO SVEDESE.

In data 11 dicembre 2020 la DPA svedese ha irrogato una sanzione amministrativa nei confronti dell'Università di Umeå per aver violato varie previsioni del GDPR in ragione delle seguenti carenze:

I. mancanza di adeguate misure di sicurezza per la protezione di categorie particolari di dati personali e di altre informazioni sensibili (anche in relazione alla salute e alla vita sessuale degli interessati) contenuti in oltre un centinaio di relazioni di indagini preliminari relative a casi di stupri maschili. Tali relazioni – precedentemente richieste alla polizia da un gruppo di ricerca dell'Università – sono state scannerizzate digitalmente e salvate in un serviio ***cloud*** **negli USA** (nonostante indicazione contraria dell'Università, pubblicata sul proprio portale *intranet*);

II. ripetuto invio di e-mail non criptate con le relazioni ivi allegate (nonostante esplicita indicazione contraria della polizia);

III. omessa notifica alla DPA svedese di alcuni *data breach* occorsi, così come omessa evidenziazione delle misure configurate, da un lato, per la mitigazione dei relativi effetti e, dall'altro lato, per prevenire il verificarsi di simili incidenti in futuro.

La decisione è degna di nota in quanto la prima concernente i trasferimenti di dati personali all'estero a seguito della sentenza *Schrems II* e facendovi esplicito riferimento (ancorché "non applicabile" al momento degli eventi in considerazione, quando era ancora in vigore il *Privacy Shield UE-USA*).

In particolare:

- l'Università di Umeå ha conservato i dati utilizzando un servizio *cloud* fornito da una società con sede negli Stati Uniti la quale, all'epoca (primavera 2019), aveva dichiarato di uniformarsi al *Privacy*

Shield UE-USA. Sebbene il trasferimento in quanto tale dovesse ritenersi permesso sulla base del *Privacy Shield UE-USA*, la DPA svedese ha osservato come il trattamento e la conservazione di siffatti dati sensibili non dovrebbero essere effettuati utilizzando un servizio *cloud* di tal guisa e come le misure adottate dall'Università di Umeå – *inter alia,* l'implementazione di un processo di autenticazione a fattore unico per accedere alla rete – non potessero essere considerate adeguate a impedire l'accesso ai dati da parte di terzi.

- la DPA svedese ha rilevato come il trasferimento di dati verso paesi terzi *extra*-SEE aumenti i rischi per la protezione dei dati personali, poiché gli interessati potrebbero non essere in grado di esercitare i propri diritti o di impedire qualsiasi divulgazione o accesso non autorizzato ai dati trasferiti, imponendo così oneri aggiuntivi per i titolari e i responsabili in rispetto alle misure da adottare in compliance al GDPR.

Considerato l'attuale "stato dell'arte" a seguito della sentenza *Schrems II*, è cruciale che i titolari e i responsabili del trattamento dei dati siano in grado di comprovare l'adozione di misure adeguate per effettuare trasferimenti di dati in conformità al GDPR, tenendo in debita considerazione l'intero insieme di linee guida e previsioni recentemente adottate dalle varie Autorità UE competenti (riassunte nei paragrafi che precedono).

Contatti

Gilberto Nava
Partner – Chiomenti
Dipartimento IP, TMT, Data Protection
T. +39.06.46622.719
gilberto.nava@chiomenti.net

Giulio Vecchi
Counsel – Chiomenti
Dipartimento IP, TMT, Data Protection
T. +39.02.72157.658
giulio.vecchi@chiomenti.net