Relazione del Gruppo di Lavoro in tema di trasferimento di dati personali al di fuori dello SEE a fronte della sentenza "Schrems II" emessa dalla Corte di Giustizia dell'Unione Europea

Con i contributi di: Avv. Valentina Apruzzi, Dott. Giovanni Gobbi, Avv. Maria Grassetto, Avv. Martina Lonardi, Avv. Floriana Tagliaferro

Coordinatori del Gruppo di Lavoro: Dott. Ing. Manuela Sforza, Ing. Franco Sesona

Prefazione: dott. Rosario Mauro Catanzaro

Prefazione

La dichiarazione di invalidità del "Privacy Shield" da parte della Corte di Giustizia Europea ha creato un esteso vuoto normativo e giurisprudenziale.

Gli operatori si sono ritrovati, da un giorno all'altro, a dover fare i conti con una sentenza che, spesso, impatta fortemente con la normale operatività aziendale e professionale. Molte piattaforme, infatti, prevedono il trasferimento dei dati negli USA o, comunque, danno potenzialmente accesso alle autorità di intelligence USA, permettendogli di accedere ai dati e ai canali di comunicazione senza particolare garanzia di forme di tutela per gli interessati.

A questa situazione di incertezza normativa si aggiungono opinioni contrastanti non solo degli osservatori, ma anche degli Enti Governativi, Europei e sovranazionali.

L'Associazione Nazionale per la Protezione dei Dati, con lo scopo aiutare imprese e professionisti ad affrontare un argomento così complesso, ha quindi ritenuto opportuno promuovere un gruppo di lavoro per elaborare la presente relazione.

Ringrazio per l'abnegazione dimostrata tutti coloro che hanno dato il loro contributo e senza i quali non sarebbe stato possibile realizzare questo lavoro. Un ringraziamento particolare ai coordinatori del Gruppo: Manuela Sforza e Franco Sesona, ed a tutti i relatori che elenco in stretto ordine alfabetico: Valentina Apruzzi, Giovanni Gobbi, Maria Grassetto, Martina Lonardi, Floriana Tagliaferro.

Rosario Mauro Catanzaro
Presidente Associazione Nazionale per la Protezione dei Dati

1. Introduzione

Le aziende ed organizzazioni pubbliche e private, di qualsiasi dimensione, negli ultimi tempi, al fine di implementare il proprio sviluppo, stanno progressivamente affrontando un processo, noto come "digital transformation" con l'obiettivo di migliorare i propri prodotti e servizi, fidelizzare il cliente, ed esplorare nuovi canali e metodi di approccio al mercato. Nel settore pubblico si assiste ad una progressiva transizione dei servizi offerti verso le piattaforme digitali (es. SPID, app IO[1] – l'app dei servizi pubblici, ecc.)

L'ampia disponibilità di soluzioni a basso costo, le crescenti funzionalità offerte, insieme alla necessità di far fronte ad un mercato globale che ha imposto nuove regole, sono state vettori e stimoli all'utilizzo delle nuove tecnologie digitali. La crisi pandemica indotta dall'epidemia di Sars-CoV2 (COVID-19) è stata un fattore accelerante alla diffusione di tali strumenti, anche in contesti che avrebbero, in condizioni normali, richiesto maggiore tempo. Il massiccio ricorso allo SmartWorking[2], la enorme diffusione delle videoconferenze (pensiamo alla didattica a distanza), l'esplosione del commercio on-line[3], ma anche la nascita di app per il "contact tracing", sono solo alcuni esempi della penetrazione delle tecnologie nel mondo delle aziende e della popolazione.

In questo contesto, il 16 luglio scorso, la Corte di Giustizia Europea si è pronunciata dichiarando invalida la decisione della Commissione Europea del 2016, con la quale la stessa aveva espresso un giudizio di adeguatezza sul livello di protezione dei dati personali dei cittadini EU trasferiti negli USA nell'ambito dell'accordo UE-USA, meglio noto come "Privacy Shield". Vale la pena ricordare che tale decisione, il "Privacy Shield", è stata utilizzata come valida base giuridica per il trattamento dei dati personali dalla maggioranza dei fornitori di servizi digitali con base negli USA quali Microsoft, Google, Facebook, Salesforce, ecc. Data la grande diffusione di tali piattaforme, anche nell'ambito dei progetti di "digital transformation", si evince come la sentenza rivesta un'importanza fondamentale non solo per gli esperti di data protection, ma, ancor di più, per le aziende e le organizzazioni che trattano i dati personali e che hanno necessità di trasferirli negli USA.

Nelle pagine che seguono abbiamo cercato di approfondire il tema, analizzando i contenuti della sentenza, la giurisprudenza rilevante, il concetto di trasferimento, alcune criticità applicative derivanti dalla sentenza, fornendo un quadro che ci auguriamo il più possibile chiaro e completo, insieme ad alcune raccomandazioni e proposte, sviluppate tenendo conto delle informazioni più aggiornate.

2. La Sentenza della Corte Europea C-311/18 (c.d. "Schrems II") - Novità ed Effetti

La sentenza del 16 luglio 2020 nella causa C-311/18[4], emessa dalla Corte di giustizia dell'Unione europea (di seguito "CGUE" o "Corte"), ha dichiarato invalida la decisione 2016/1250 della Commissione europea sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la protezione dei dati personali, il cosiddetto "Privacy Shield".

[1] IO, https://io.italia.it/ è un servizio digitale che permette di interagire oggi con diverse Pubbliche Amministrazioni, locali o nazionali ed in prospettiva con la totalità degli uffici della PA, raccogliendo in un'unica app, i servizi ai cittadini quali comunicazioni, pagamenti e documenti.

Con l'app IO, alla quale si accede tramite Identità Digitale SPID o con la Carta d'Identità Elettronica (CIE), è possibile ricevere messaggi, avvisi, comunicazioni, da qualunque Ente pubblico. E' possibile inoltre eseguire operazioni relative al pagamento di servizi o tributi oltre che mettersi in contatto con gli enti pubblici tramite i canali di contatto disponibili nell'app.

[2] Dal 1,2 % al 8.8% della forza lavoro in pochi mesi, fonte: Osservatorio SmartWorking del Politecnico di Milano.
[3] 2M di nuovi consumatori nel 1° semestre 2020, fonte: NetComm Forum.
[4] http://curia.europa.eu/juris/liste.jsf?num=C-311/18

La sentenza riveste un'importanza fondamentale non solo per gli esperti e cultori della materia ma, ancor di più, per chi i dati personali li tratta e, soprattutto, per chi li ha trasferiti e/o necessita di trasferirli negli USA oppure, come avremo modo di considerare in seguito, anche in altri paesi fuori del SEE.

Fino al 16 luglio gli esportatori e gli importatori dei dati hanno fatto leva sul Privacy Shield – ovvero, il sistema di regolamentazione del trasferimento e dello scambio delle informazioni di carattere personale tra l'Unione europea e gli Stati Uniti – che la sentenza de quo ha dichiarato invalido, in quanto non compatibile con la normativa UE, primaria e secondaria, concernente la tutela del diritto alla protezione dei dati personali.

2.1 Il quadro normativo

Ai sensi degli articoli 25 e 26 della Direttiva 95/46/EC[5], poi abrogata con l'introduzione del GDPR e, in particolare, degli articoli da 44 a 50, il trasferimento di dati personali a paesi non ricompresi nello Spazio Economico Europeo ("SEE", ossia UE + Norvegia, Liechtenstein, Islanda) può essere effettuato solo se (i) tale paese terzo assicura un adeguato livello di protezione dei dati e (ii) gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.

Ai sensi dell'art. 45 del GDPR, la Commissione europea stabilisce se un paese terzo garantisce, in base alla propria legge e al suo impegno nei rapporti internazionali, un *adeguato* livello di protezione secondo gli standard del legislatore europeo.

In relazione agli USA, la Commissione ha stabilito in un primo momento, con la Decisione 2000/520/EC, che la protezione adeguata fosse garantita dall'adesione delle aziende al meccanismo del cosiddetto "approdo sicuro", il "Safe Harbour". Tale meccanismo, tuttavia, è stato poi invalidato dalla prima sentenza Schrems. Successivamente è intervenuta una nuova decisione di adeguatezza (Decisione 2016/1250[6]) che ha adottato il regime EU-US Privacy Shield.

In sintesi, al fine di proteggere i diritti fondamentali delle persone i cui dati vengono trasferiti negli USA, il "Privacy Shield" ha previsto:

- obblighi di protezione restrittivi per le imprese che trasferiscono dati negli USA;
- misure di sicurezza per l'accesso ai dati da parte del governo USA;
- strumenti specifici per la tutela degli interessati;
- la revisione annuale congiunta (UE-USA) dell'accordo per monitorarne l'attuazione.

In assenza di una decisione di adeguatezza, i trasferimenti di dati personali verso paesi terzi, fatte salve alcune specifiche deroghe di limitata utilizzabilità previste dall'art. 49 del GDPR, possono avvenire solo se l'esportatore di dati personali stabilito nell'UE ha fornito adeguate garanzie previste dall'art. 46 GDPR, quali ad esempio, l'adozione di norme vincolanti di impresa ai sensi dell'art. 47 GDPR da parte dei gruppi di imprese ("BCR").

Le garanzie ricomprese nell'art. 46 includono la sottoscrizione di clausole contrattuali standard ("SCC") approvate dalla Commissione europea con la decisione 2001/497/EC, modificata con la decisione 2004/915/EC – nei rapporti titolare-titolare - e la decisione 2010/87/CE – nei rapporti titolare-responsabile - (congiuntamente, nel prosieguo, la "Decisione SCC").

[5] *Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati* https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:31995L0046&from=it

[6] *Decisione di esecuzione (UE) 2016/1250 della Commissione*, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza *della protezione offerta dal regime dello scudo UE-USA per la privacy* [notificata con il numero C(2016) 4176] (https://eur-lex.europa.eu/legalcontent/IT/TXT/?uri=CELEX%3A32016D1250)

2.2 Il fatto

Maximillian Schrems, cittadino austriaco residente in Austria, è iscritto dal 2008 al social network Facebook, con sede europea in Irlanda. Come avviene per tutti gli utenti Facebook dell'Unione europea, i suoi dati personali sono trasferiti da Facebook Ireland verso server posizionati nel territorio degli USA, appartenenti alla casa-madre Facebook Inc. Schrems presenta all'Autorità di controllo irlandese una denuncia tesa a far vietare tali trasferimenti, sostenendo che il diritto e le prassi degli Stati Uniti non assicurerebbero una protezione adeguata contro l'accesso da parte delle autorità pubbliche ai dati trasferiti negli USA.

Pesano sul fatto le vicende di Edward Snowden, ex tecnico della CIA, e le denunce che nel 2013 rivelarono una serie di programmi di sorveglianza di massa delle comunicazioni, realizzati dai servizi di intelligence statunitensi e, in particolare, dalla National Security Agency (NSA), l'agenzia di sicurezza nazionale, con la quale lo stesso Snowden aveva collaborato. I programmi in questione - quali il PRISM[7] e l'UPSTREAM[8] - permettono, sostanzialmente, alle autorità di intelligence USA, di attingere ai dati e ai canali di comunicazione praticamente senza limiti e senza garanzia di forme di tutela per gli interessati.

La denuncia di Schrems viene respinta, principalmente perché la Commissione Europea, con precedente decisione 2000/520 (c.d. decisione "Safe Harbour", "approdo sicuro"), aveva stabilito che gli Stati Uniti garantivano un adeguato livello di protezione. Tale decisione, tuttavia, con la sentenza Schrems I, veniva dichiarata invalida dalla CGUE, investita di una questione pregiudiziale sottopostale dall'Alta Corte irlandese.

A seguito della sentenza Schrems I[9] e del successivo annullamento della decisione di rigetto della denuncia, ad opera del giudice irlandese, l'autorità di controllo irlandese invita il sig. Schrems a riformulare la sua denuncia, tenendo conto della intervenuta dichiarazione di invalidità della decisione 2000/520.

Nella sua riformulazione, il sig. Schrems può così:

- sostenere che gli Stati Uniti non offrissero una protezione sufficiente per i dati trasferiti dentro i propri confini;
- chiedere di sospendere o vietare, per il futuro, i trasferimenti dei suoi dati personali dall'UE verso gli USA, effettuati da Facebook Ireland, sul fondamento delle "clausole tipo di protezione" contenute nell'allegato della Decisione SCC.

Tenendo conto che il trattamento relativo alla denuncia del sig. Schrems dipendesse, in particolare, dalla validità della Decisione SCC, l'autorità di controllo irlandese avvia un procedimento dinanzi all'Alta Corte irlandese affinché quest'ultima presenti alla CGUE una domanda di pronuncia pregiudiziale, come di seguito meglio descritta.

Nel frattempo, la Commissione, con la decisione (UE) 2016/1250 (di seguito "Decisione Privacy Shield"), dichiara adeguata la protezione offerta dal regime dello scudo UE-USA per la privacy (il c.d. "Privacy Shield Ue-Usa").

2.3 Questioni pregiudiziali

Alla luce di quanto sopra e a seguito di una complessa vicenda giudiziaria, la CGUE viene quindi chiamata a pronunciarsi su undici questioni pregiudiziali. Ricordiamo che il rinvio pregiudiziale consente ai giudici degli Stati membri dell'UE, nell'ambito di una controversia della quale sono investiti, di interpellare la CGUE in merito all'interpretazione del diritto dell'Unione o alla validità di un atto dell'Unione. La Corte non è chiamata a risolvere la controversia domestica ma spetta ai giudici nazionali risolverla, conformemente alla decisione della Corte.

---

[7] *PRISM*: Programma di Sorveglianza usato per la gestione di informazioni raccolte attraverso Internet e altri fornitori di servizi elettronici e telematici adottato dalla NSA (National Security Agency) dal 2007 sulla base dell'art. 702 del FISA (Foreign Intelligence Surveillance Act, 1978) e dell'E.O.12333 (Executive Order 12333, 1981).

[8] *UPSTREAM*: Programma di Sorveglianza utilizzato per la raccolta di informazioni in transito nella rete internet, adottato dalla NSA (National Security Agency) dal 2007 sulla base dell'art. 702 del FISA e dell'E.O.12333.

[9] *CGUE, 6 ottobre 2015, nella causa C-362/14.*

Analizziamo, di seguito le questioni pregiudiziali sulla base dell'ordine di disamina compiuto dalla CGUE stessa:

a) Con la prima questione, il giudice del rinvio si chiede se l'art. 2, par. 1, e l'art. 2, par. 2, lett. a), b) e d), del GDPR, in combinato disposto con l'art. 4, par. 2 del Trattato dell'Unione europea ("TUE"), debbano essere interpretati nel senso che rientri nell'ambito del GDPR un trasferimento di dati personali effettuato da un operatore economico stabilito in uno Stato membro UE verso un altro operatore economico stabilito in un paese terzo, qualora, durante o in seguito a tale trasferimento, detti dati possano essere trattati dalle autorità del suddetto paese terzo a fini di sicurezza pubblica, di difesa e di sicurezza dello Stato.
b) Con le questioni seconda, terza e sesta, il giudice del rinvio interroga la CGUE sul livello di protezione richiesto dall'art. 46, par. 1, e dall'art. 46, par.2, lett. c), del GDPR nell'ambito di un trasferimento di dati personali verso un paese terzo effettuato sulla base di clausole tipo di protezione dei dati ("SCC"). In particolare, il giudice chiede di precisare gli elementi da tenere in considerazione per determinare se il livello di protezione sia garantito nel contesto di un trasferimento effettuato sulle SCC.
c) Con l'ottava questione, il giudice del rinvio chiede se l'art. 58, par. 2, lettere f) e j), del GDPR debba essere interpretato nel senso che l'autorità di controllo competente è tenuta a sospendere o a vietare un trasferimento di dati personali verso un paese terzo effettuato sulla base di SCC, allorché la suddetta autorità ritenga che le SCC non sono o non possono essere rispettate in detto paese terzo e che la protezione dei dati trasferiti richiesta dal diritto dell'Unione, in particolare dagli artt. 45 e 46 del GDPR nonché dalla Carta dei diritti fondamentali dell'Unione europea (di seguito la "Carta"), non possa essere garantita, oppure nel senso che l'esercizio di tali poteri è limitato ad ipotesi eccezionali.
d) Con la settima e l'undicesima questione, il giudice del rinvio interpella, in sostanza, la Corte sulla validità della Decisione SCC alla luce degli artt. 7, 8 e 47 della Carta. In particolare, il giudice del rinvio si chiede se la Decisione SCC sia idonea a garantire un livello di protezione adeguato dei dati personali trasferiti verso paesi terzi, *considerato che le SCC da essa previste non vincolano le autorità di tali paesi terzi*.
e) Con la nona questione, il giudice del rinvio chiede, in sostanza, se e in che limiti l'autorità di controllo di uno Stato membro sia vincolata dalle constatazioni contenute nella decisione sul Privacy Shield.
f) Con le questioni quarta, quinta e decima, detto giudice chiede se, tenuto conto delle sue constatazioni riguardo al diritto degli USA, il trasferimento di dati personali verso tale paese terzo sul fondamento delle SCC violi i diritti garantiti dagli articoli 7, 8 e 47 della Carta e chiede, segnatamente, alla Corte se l'aver istituito il Mediatore menzionato nell'allegato III della decisione sul Privacy Shield sia compatibile con il suddetto art. 47.

2.4 Nel merito della decisione della CGUE

La CGUE, una volta stabilita la ricevibilità della domanda - l'eccezione di irricevibilità veniva sollevata da Facebook, in virtù del fatto che la domanda verteva sull'interpretazione delle norme della direttiva 95/46/EC abrogata ad opera del GDPR - passa alla disamina di tutte le questioni pregiudiziali, traendo le seguenti conclusioni.

2.4.1 Riguardo l'applicabilità del GDPR ai trasferimenti di dati personali

La CGUE ha risposto positivamente alla prima questione pregiudiziale confermando che il GDPR trova applicazione nel caso di trasferimento di dati personali effettuato a fini commerciali da un operatore economico stabilito in uno Stato membro dell'UE verso un operatore economico stabilito in un paese terzo anche se, durante o dopo detto trasferimento, i dati possono essere soggetti a trattamento per finalità di sicurezza pubblica, di difesa e di sicurezza dello Stato ad opera delle autorità del paese terzo considerato.

2.4.2 In relazione al livello di protezione dei dati personali richiesto dal GDPR nel quadro dei trasferimenti verso Paesi terzi basati sulle SCC

In relazione al livello di protezione richiesto nell'ambito di un trasferimento basato sulle SCC, la CGUE dichiara che i requisiti previsti dal GDPR in materia di garanzie adeguate, diritti opponibili e mezzi di ricorso effettivi, devono essere interpretati nel senso che gli interessati i cui dati personali sono trasferiti verso un paese terzo mediante uso delle SCC, devono godere di un livello di protezione *sostanzialmente equivalente* a quello garantito all'interno dell'UE dal GDPR, letto alla luce della Carta.

A questa conclusione la CGUE arriva muovendo dall'analisi dei considerando 104[10] e 108[11] del GDPR che aiutano a individuare gli elementi da tenere in considerazione nella valutazione del livello di adeguatezza: (i) il livello di protezione deve essere sostanzialmente equivalente a quello applicato in UE e assicurare un effettivo controllo indipendente della protezione; (ii) le adeguate garanzie da adottarsi in assenza di una decisione di adeguatezza devono compensare la carenza di protezione dei dati nel paese terzo.

La valutazione del predetto livello di protezione, pertanto, deve prendere in considerazione sia quanto stipulato contrattualmente tra l'esportatore dei dati europeo e il destinatario del trasferimento stabilito nel paese terzo, sia – con particolare riferimento a eventuali accessi da parte delle pubbliche Autorità di tale paese terzo – gli aspetti del sistema giuridico ivi esistente alla luce dei principi di diritto applicati nell'UE e segnatamente della Carta.

2.4.3 Il potere di sospendere o vietare il trasferimento da parte delle Autorità di controllo

Riguardo all'obbligo delle Autorità di controllo nazionali di sospendere o vietare il trasferimento dei dati verso un paese terzo mediante l'uso delle SCC, ove l'autorità ritenga che tali clausole non possano essere rispettate e la protezione dei dati non garantita, la CGUE muove dal presupposto che alle autorità nazionali di controllo spetti la vigilanza del rispetto delle norme UE e che nell'ambito dei propri poteri e del proprio giudizio indipendente sia tenuta a sospendere o vietare il trattamento che non ritenga conforme alle SCC o in relazione al quale le SCC non possano essere rispettate.

2.4.4 Validità della Decisione SCC

La CGUE, pur ritenendo infine valida la Decisione sulle SCC, muove le proprie considerazioni dall'assunto che non spetti alla Commissione, nell'adottare le clausole tipo di protezione dei dati senza particolare riferimento ad un paese terzo o ad un settore determinato, "*procedere ad una valutazione dell'adeguatezza del livello di protezione garantito dai paesi terzi verso i quali potrebbero essere trasferiti dati personali in base a tali clausole*" e che spetti invece al titolare o al

[10] *"In linea con i valori fondamentali su cui è fondata l'Unione, in particolare la tutela dei diritti dell'uomo, è opportuno che la Commissione, nella sua valutazione del paese terzo, o di un territorio o di un settore specifico all'interno di un paese terzo, tenga conto del modo in cui tale paese rispetta lo stato di diritto, l'accesso alla giustizia e le norme e gli standard internazionali in materia di diritti dell'uomo, nonché la legislazione generale e settoriale riguardante segnatamente la sicurezza pubblica, la difesa e la sicurezza nazionale, come pure l'ordine pubblico e il diritto penale. L'adozione di una decisione di adeguatezza nei confronti di un territorio o di un settore specifico all'interno di un paese terzo dovrebbe prendere in considerazione criteri chiari e obiettivi come specifiche attività di trattamento e l'ambito di applicazione delle norme giuridiche e degli atti legislativi applicabili in vigore nel paese terzo. Il paese terzo dovrebbe offrire garanzie di un adeguato livello di protezione sostanzialmente equivalente a quello assicurato all'interno dell'Unione, segnatamente quando i dati personali sono trattati in uno o più settori specifici. In particolare, il paese terzo dovrebbe assicurare un effettivo controllo indipendente della protezione dei dati e dovrebbe prevedere meccanismi di cooperazione con autorità di protezione dei dati degli Stati membri e agli interessati dovrebbero essere riconosciuti diritti effettivi e azionabili e un mezzo di ricorso effettivo in sede amministrativa e giudiziale"* (Considerando 104 GDPR).

[11] *"In mancanza di una decisione di adeguatezza, il titolare del trattamento o il responsabile del trattamento dovrebbe provvedere a compensare la carenza di protezione dei dati in un paese terzo con adeguate garanzie a tutela dell'interessato. Tali adeguate garanzie possono consistere nell'applicazione di norme vincolanti d'impresa, clausole tipo di protezione dei dati adottate dalla Commissione, clausole tipo di protezione dei dati adottate 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, compresa la disponibilità di diritti azionabili degli interessati e di mezzi di ricorso effettivi, fra cui il ricorso effettivo in sede amministrativa o giudiziale e la richiesta di risarcimento, nell'Unione o in un paese terzo. Esse dovrebbero riguardare, in particolare, la conformità rispetto ai principi generali in materia di trattamento dei dati personali e ai principi di protezione dei dati fin dalla progettazione e di protezione dei dati di default. I trasferimenti possono essere effettuati anche da autorità pubbliche o organismi pubblici ad autorità pubbliche o organismi pubblici di paesi terzi, o organizzazioni internazionali con analoghi compiti o funzioni, anche sulla base di disposizioni da inserire in accordi amministrativi, quali un memorandum d'intesa, che prevedano per gli interessati diritti effettivi e azionabili. L'autorizzazione dell'autorità di controllo competente dovrebbe essere ottenuta quando le garanzie sono offerte nell'ambito di accordi amministrativi giuridicamente non vincolanti"* (Considerando 108 GDPR).

responsabile del trattamento "*provvedere a compensare la carenza di protezione dei dati in un paese terzo con adeguate garanzie a tutela dell'interessato*[12]" senza preclusione riguardo alla possibilità di aggiungere altre clausole o garanzie[13].

Esiste, inoltre, evidenzia la CGUE, ai sensi della clausola 5, lett. a) relativa alle clausole tipo contenute nell'allegato della Decisione sulle SCC, un obbligo informativo in capo al destinatario del trattamento verso il titolare stabilito nell'UE circa la sua eventuale impossibilità a rispettare gli obblighi derivanti dal contratto e il diritto per il titolare di ottenere la restituzione o la distruzione dei dati. Peraltro, aggiunge ancora la Corte, ove un'autorità di controllo ritenga che i trasferimenti verso un paese terzo debbano essere vietati, può adire l'EDPB (European Data Protection Board) per adottare una decisione vincolante. Il fatto che le SCC non vincolino le autorità del Paese destinatario non incide, a detta della Corte, sulla validità della Decisione SCC.

Alla luce di tutte le considerazioni esposte, la CGUE conclude ritenendo che la Decisione SCC prevede meccanismi efficaci che permettono di garantire che il trasferimento effettuato sulla base delle SCC sia sospeso o vietato in caso di mancato o impossibile rispetto da parte del destinatario delle predette clausole tipo e conclude rigettando ogni elemento di invalidità delle clausole stesse[14].

2.4.5 Invalidità della Decisione Privacy Shield

Riguardo alla Decisione Privacy Shield, la CGUE, accogliendo in parte le accuse mosse dal sig. Schrems nelle sue denunce, ha dichiarato invece la sua invalidità per motivi connessi principalmente alla violazione delle disposizioni della Carta, che garantiscono ai cittadini europei (i) il rispetto della vita privata e familiare (art. 7 della Carta), (ii) la protezione dei dati personali (art. 8 della Carta), nonché (iii) il diritto a una tutela giurisdizionale effettiva (art. 47 della Carta). In particolare, la Corte ha evidenziato che la possibile limitazione dei principi stabiliti dalla Decisione, prevista all'art. 1.5 dell'Allegato II, derivante dalla necessità di "*soddisfare esigenze di sicurezza nazionale*" rende possibili "*ingerenze fondate su esigenze connesse alla sicurezza nazionale e all'interesse pubblico o alla legislazione interna agli Stati Uniti, nei diritti fondamentali delle persone, i cui dati personali sono o potrebbero essere trasferiti dall'Unione verso gli Stati Uniti*".

Le ingerenze richiamate sono determinate dalla presenza negli USA dei programmi di controllo e sorveglianza (PRISM e UPSTREAM) adottati ai sensi dell'art. 702 del FISA e del PPD-28 nonché dell'Executive Order (EO) 12333, i quali non solo non limitano l'uso dei programmi da parte dell'intelligence ma nemmeno prevedono garanzie per i cittadini stranieri oggetto di tali programmi.

Tali ingerenze, conclude la Corte, non permettono strumenti di tutela da parte dell'interessato poiché anche la figura del "Mediatore" (cd. Mediatore o Ombudsman), prevista dalla Decisione Privacy Shield, risulta in qualche modo corrotta nella sua indipendenza – essendo designato dal Segretario di Stato e parte integrante del Dipartimento di Stato degli Stati Uniti – e, conseguentemente, non costituisce un efficace metodo di tutela per gli interessati ai sensi dell'art. 47 della Carta.

2.5 In breve

Nella sentenza del 16 luglio 2020, la CGUE dichiara che, dall'esame della Decisione SCC, alla luce della Carta, non è emerso alcun elemento idoneo ad inficiarne la validità. Infatti, la Decisione SCC impone un obbligo per l'esportatore e l'importatore dei dati personali di verificare, prima di effettuare il trasferimento, se il livello di protezione è adeguato nel paese di destinazione e, inoltre, precisa che sia il ricevente i dati a dover informare l'esportatore di una eventuale

[12] Considerando n.108 GDPR, in linea anche il considerando n. 114 GDPR.
[13] Considerando n.109 GDPR.
[14] *"[t]hat validity depends, however, on whether, in accordance with the requirement of Article 46(1) and Article 46(2)(c) of the GDPR, interpreted in the light of Articles 7, 8 and 47 of the Charter, such a standard clauses decision incorporates effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection required by EU law and that transfers of personal data pursuant to the clauses of such a decision are suspended or prohibited in the event of the breach of such clauses or it being impossible to honour them. (para. 137)"*

impossibilità ad adeguarsi alle SCC, essendo quest'ultimo tenuto a interrompere il trasferimento dei dai o risolvere il contratto con il ricevente.

Mentre, con effetto dirompente, ha dichiarato invalida la Decisione Privacy Shield in considerazione del fatto che, alla luce dalla Carta, essa sancisce il primato delle esigenze di sicurezza nazionale degli Stati Uniti a danno dei diritti dei cittadini stranieri i cui dati sono oggetto di trasferimento negli USA e ai quali non è concesso neanche un effettivo strumento di tutela.

La pronuncia si concretizza in una dura critica ai sistemi di tutela della protezione dei dati personali offerti tanto dal Privacy Shield quanto dagli operatori di internet, piattaforme social in testa, nonché dall'ordinamento giuridico statunitense nel suo complesso, attraverso una stretta comparazione tra gli stessi ed i principi adottati nell'Unione europea. La critica appare senz'altro fondata se solo si tiene conto del fatto che, diversamente dall'ordinamento UE in cui i diritti alla riservatezza e alla protezione dei dati sono considerati fondamentali e disciplinati dettagliatamente, il sistema giuridico statunitense non opera un simile riconoscimento e non prevede una disciplina precisa e uniforme tesa a tutelare adeguatamente detti diritti, ma una normativa frammentaria e settoriale.

3. La Giurisprudenza rilevante e le Raccomandazioni EDPB

Pochi giorni dopo la pubblicazione della sentenza della CGUE, l'EDPB realizza le prime FAQ sulla sentenza Schrems II, che il Garante Italiano ha provveduto a tradurre.

L'EDPB ha dato le proprie iniziali indicazioni operative, ribadendo che la CGUE ha ritenuto valide, per i trasferimenti verso i paesi terzi, le SCC. Queste ultime, avendo esse natura contrattuale, non sono vincolanti per le autorità dei paesi terzi. La validità delle SCC dipende dall'esistenza di meccanismi efficaci che consentano di garantire il rispetto di un livello di protezione sostanzialmente equivalente a quello garantito dal GDPR all'interno dell'Unione europea, e che prevedano la sospensione o il divieto dei trasferimenti di dati personali in caso di violazione delle clausole stesse o risulti impossibile garantirne l'osservanza.

La decisione, mentre da un lato impone all'esportatore e all'importatore dei dati l'obbligo di verificare, prima di qualsiasi trasferimento, se tale livello di protezione sia rispettato nel paese terzo in questione, dall'altro, impone, come ricordato nella sezione precedente, all'importatore di informare l'esportatore di qualsiasi impossibilità di rispettare le SCC, nel qual caso l'esportatore di dati è tenuto a sospendere, a sua volta, il trasferimento dei dati e/o a risolvere il contratto con l'importatore.

La CGUE ha ritenuto che i requisiti del diritto interno degli Stati Uniti, e in particolare taluni programmi di sorveglianza che consentono alle autorità pubbliche statunitensi di accedere ai dati personali trasferiti dall'UE agli Stati Uniti per motivi di sicurezza nazionale, non prevedono limitazioni al potere conferito alle autorità statunitensi, né garanzie per soggetti non statunitensi potenzialmente sottoposti a tale sorveglianza. Ne risultano limitazioni alla protezione dei dati personali, che non sono configurate in modo da soddisfare requisiti sostanzialmente equivalenti a quelli previsti dal diritto dell'UE. Tale legislazione non consente ai soggetti interessati diritti azionabili in sede giudiziaria nei confronti delle autorità statunitensi.

Alla luce di tale grado di ingerenza nei diritti fondamentali delle persone i cui dati sono trasferiti verso tale paese terzo, la CGUE, secondo quanto ricordato in precedenza, ha dichiarato invalida la decisione sull'adeguatezza del Privacy Shield, senza preservarne gli effetti; pertanto i trasferimenti verso importatori che aderiscono al Privacy Shield sono illeciti.

Per i paesi terzi, la soglia fissata dalla CGUE si applica anche a tutte le garanzie adeguate ai sensi dell'articolo 46 del GDPR delle quali ci si avvalga per trasferire dati dal SEE a qualsiasi paese terzo. La normativa statunitense cui fa riferimento la CGUE (art. 702 FISA e Executive Order 12333) si applica a qualsiasi trasferimento verso gli Stati Uniti per via elettronica che rientra nell'ambito di applicazione di tale normativa, indipendentemente dallo strumento utilizzato per il trasferimento.

La possibilità o meno di trasferire dati personali sulla base di SCC, ovvero di BCR, dipende dall'esito della valutazione che l'esportatore dovrà compiere, tenuto conto delle circostanze del trasferimento e delle misure supplementari eventualmente messe in atto. Le misure supplementari unitamente alle SCC, ovvero alle BCR, alla luce di un'analisi caso per caso delle circostanze del trasferimento, dovrebbero garantire che la normativa statunitense non interferisca con l'adeguato livello di protezione garantito dalle SCC e dalle misure supplementari stesse.

La metodologia della valutazione è illustrata dall'EDPB nelle recenti "*Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*"[15], come composta da 6 passi fondamentali:

1. La mappatura dei trasferimenti, sia quelli diretti, sia quelli indiretti, attuati dal responsabile o sub-responsabile;
2. L'identificazione degli strumenti del trasferimento cui si fa ricorso;
3. La valutazione dell'efficacia dello strumento, declinata nel caso specifico, nel garantire l'equivalenza sostanziale delle garanzie previste agli interessati dal Diritto dell'Unione;
4. Nel caso in cui l'esportatore giunga ad una valutazione sull'efficacia negativa, l'adozione di misure supplementari a suo carico[16];
5. Nel caso di adozione di misure supplementari, la realizzazione di un corredo documentale in grado di dimostrare l'adozione di procedure che le rendano effettive;
6. Il monitoraggio e la ri-valutazione continua della valutazione, anche come parte integrante del più generale processo di risk assessment e valutazione dei rischi in materia di Protezione dei Dati.

Pare ad ogni modo ineluttabile che:

- tenuto conto delle circostanze del trasferimento e delle eventuali misure supplementari, qualora non vi siano adeguate garanzie, occorra sospendere o porre fine al trasferimento di dati personali. Se nonostante ciò dovesse esserci la necessità o la volontà di trasferire i dati, occorrerebbe informarne l'Autorità nazionale competente.
- I ragionamenti sviluppati con riguardo a ai trasferimenti verso gli Stati Uniti si possano estendere a qualsiasi paese terzo.

L'EDPB si riserva inoltre di valutare le conseguenze della sentenza sugli strumenti di trasferimento diversi dalle SCC e dalle BCR, tenuto conto che il parametro per l'adeguatezza delle garanzie di cui all'Art. 46 GDPR rimane quello dalla "equivalenza sostanziale", al fine di garantire che non sia compromesso il livello di protezione delle persone fisiche.

È sicuramente ancora possibile trasferire dati sulla base delle deroghe previste dall'articolo 49 GDPR ma solo dopo aver verificato la sussistenza delle condizioni necessarie:

- quando i trasferimenti sono basati sul consenso dell'interessato, esso dovrebbe essere: - esplicito, - specifico, che avvenga prima del trasferimento, e - informato, in particolare sui possibili rischi del trasferimento (derivanti dal trasferimento dei dati verso un paese che non fornisce una protezione adeguata, e dell'assenza di misure di salvaguardia adeguate volte a proteggere i dati);
- per quanto riguarda i trasferimenti necessari all'esecuzione di un contratto tra l'interessato e il titolare del trattamento, i dati personali possono essere trasferiti solo su base occasionale. Tale deroga può essere invocata solo quando il trasferimento è oggettivamente necessario all'esecuzione del contratto;
- in relazione ai trasferimenti necessari per importanti motivi di interesse pubblico, il requisito essenziale per l'applicabilità di tale deroga è la constatazione della sussistenza di importanti motivi di interesse pubblico; non significa che possano configurarsi su larga scala e in modo sistematico;

[15] 10 novembre 2020
[16] Esempi di misure tecniche ed organizzative aggiuntive, e i relativi casi d'uso, sono contenuti nell'Annex 2 delle stesse Raccomandazioni 1/2020

- occorre inoltre rispettare il principio generale per cui le deroghe previste all'articolo 49 non dovrebbero trasformarsi di fatto in una regola, essendo necessario limitarne l'applicazione a situazioni specifiche e purché ogni esportatore di dati garantisca che il trasferimento soddisfi un rigoroso test di necessità, requisito che rende tale tipo di deroga di difficile applicazione.

L'EDPB rappresenta che, nell'ipotesi di contratto stipulato con il responsabile in conformità all'articolo 28, paragrafo 3, del GDPR, il titolare deve stabilire se i trasferimenti siano o meno autorizzati (costituisce un trasferimento anche l'accesso ai dati effettuato a partire da un paese terzo, ad esempio a fini amministrativi, come vedremo nel prosieguo della relazione). L'autorizzazione occorre anche per consentire a un responsabile di affidare a sub-responsabili il trasferimento di dati verso paesi terzi: numerose soluzioni informatiche possono comportare il trasferimento di dati personali verso un paese terzo, a fini di conservazione o manutenzione. Se è previsto che i dati siano trasferiti verso gli Stati Uniti e non possono essere introdotte misure supplementari per garantire che la normativa statunitense non incida sul livello di protezione sostanzialmente equivalente a quello offerto nel SEE, assicurato dagli strumenti di trasferimento, né si applicano le deroghe di cui all'articolo 49 del GDPR, l'unica soluzione è negoziare un emendamento o una clausola aggiuntiva al contratto per vietare il trasferimento di dati verso gli USA[17]. Non solo la conservazione, ma anche la gestione dei dati dovrebbero quindi avvenire in paesi diversi dagli USA.

Le autorità di controllo proseguiranno i lavori in seno all'EDPB al fine di garantire approcci coerenti, in particolare qualora debbano essere vietati determinati trasferimenti verso paesi terzi.

Il Garante dello Stato tedesco del Baden-Württemberg ha intanto pubblicato una guida sul trasferimento dei dati al di fuori dello Spazio economico europeo, individuando tra le misure supplementari idonee ad assicurare un livello di protezione adeguato dei dati personali:

- i sistemi di crittografia in cui solo l'esportatore possiede la chiave di decriptazione;
- i sistemi di anonimizzazione;
- i sistemi di pseudonimizzazione, in base a cui l'esportatore può ricollegare i dati ad una determinata persona fisica.

Il 06.10.2020 il Garante Privacy, commentando una sentenza in pari data della CGUE, che si è espressa escludendo che quella dei trattamenti di dati funzionali alle finalità di conservazione dei dati di traffico, da parte dei fornitori dei servizi di comunicazione elettronica, possa essere una 'zona franca', impermeabile alle esigenze di tutela della persona, ritiene come principio di assoluta rilevanza, sotto il profilo democratico, il rapporto tra libertà e sicurezza, richiamando espressamente la sentenza Schrems II, al fine di evitare che una dilatazione (nell'ordinamento statunitense particolarmente marcata) della nozione di sicurezza nazionale finisca di fatto per eludere l'effettività della tutela di un fondamentale diritto di libertà, quale appunto quello alla protezione dei dati.

In un intervento del 20.10.2020, l'Avv. Guido Scorza, Membro del Collegio del Garante per la protezione dei dati ha affermato che la Sentenza della CGUE del 16.7.2020, ha rilevato l'esistenza di una asimmetria delle norme e della giustizia USA rispetto alle norme ed ai regolamenti EU, che potrebbe essere risolta attraverso un adeguamento normativo tra i vari paesi, ad esempio allineando le norme USA ai requisiti del GDPR.

Sempre l'Avv. Guido Scorza, in suo recente articolo, auspica l'identificazione nella comunità internazionale di uno strumento pattizio capace di garantire la libera circolazione globale dei dati nel rispetto di poche, ma nel contempo insuperabili, garanzie a tutela degli interessati[18].

[17] Ulteriori indicazioni sulle clausole contrattuali aggiuntive sono contenute nell'Annex 2 delle Raccomandazioni 1/2020, in appendice al presente documento.

[18] Trasferimento dati extra-Ue, Scorza (Garante Privacy): "Abbiamo un problema, anzi tre" https://www.agendadigitale.eu/sicurezza/privacy/trasferimento-dati-extra-ue-abbiamo-un-problema-anzi-tre-e-non-riguarda-solo-gli-usa/

Andrea Jelinek, la presidente del Comitato Europeo per la Protezione dei Dati, ha dichiarato che il Comitato è ben consapevole del fatto che la sentenza Schrems II attribuisce ai titolari del trattamento una responsabilità importante. Oltre alla dichiarazione e alle FAQ pubblicate subito dopo la sentenza, l'EDPB ha elaborato le Raccomandazioni 1/2020 proprio per supportare titolari e responsabili del trattamento nel processo di valutazione del rischio, preliminare alla necessaria individuazione e attuazione di adeguate misure supplementari di natura giuridica, tecnica e organizzativa, al fine di soddisfare il requisito di «equivalenza sostanziale» nel trasferimento di dati personali verso paesi terzi. La presidente conferma che la sentenza ha implicazioni di ampia portata e i contesti dei trasferimenti di dati verso paesi terzi sono molto diversi, che non possibile pensare a una soluzione unica e di immediata applicazione, e che pertanto ciascun titolare o responsabile dovrà valutare i trattamenti svolti e i relativi trasferimenti, adottando le misure opportune.

4. Definizione di Trasferimento

4.1 Art. 44 GDPR

Il Regolamento del Parlamento Europeo e del Consiglio del 27 aprile 2016, n. 679 (di seguito, il "GDPR") non contiene una definizione di "trasferimento" dei dati personali, così come non la prevedeva la direttiva 95/46/CE.

Detta definizione sarebbe stata auspicabile alla luce dell'evoluzione tecnologica e del quotidiano utilizzo di Internet che comporta un continuo flusso transfrontaliero di informazioni e che può rendere difficile l'individuazione di uno spostamento fisico di un file.

Gli artt. 44 e seguenti del GDPR, infatti, determinano soltanto le regole in base alle quali "*qualunque trasferimento di dati personali oggetto di un trattamento o destinati ad essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale*" può avere luogo, ma non cosa debba intendersi per trasferimento di dati personali verso un paese terzo, ovvero situato al di fuori dello Spazio Economico Europeo (SEE).

È pacifico che nel concetto di "trasferimento" rientra tutto ciò che comporta uno spostamento materiale di dati personali da un punto ad un altro, mentre diventa più complesso individuare quali altre operazioni possano qualificare il trasferimento.

Si pensi, ad esempio, alla comunicazione. Nel caso di comunicazione "mediante trasmissione" può parlarsi di uno spostamento fisico del dato, mentre nel caso della comunicazione in forma orale si ha un transito immateriale del dato, ma anche in quest'ultimo caso si realizza un trasferimento.

Il trasferimento può dunque avvenire attraverso la comunicazione. Ma cosa si intende per "comunicazione"?

L'art. 4 del GDPR nell'ambito della definizione di trattamento prevede la "*comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione*".

Può essere utile quindi partire dal concetto di "comunicazione" per ampliare quello di "trasferimento".

4.2 Comunicazione

Prima di procedere oltre, è innanzitutto opportuno chiarire – anche se potrà sembrare banale ai più– che non vi è trasferimento laddove sia l'interessato a comunicare direttamente i propri dati al Titolare del trattamento che ha sede in un paese terzo.

Al Titolare del trattamento che offre beni e servizi all'interessato in UE si applicheranno certamente le disposizioni del GDPR (art. 3, par. 2) ma per il trattamento dei dati da parte sua non sono richieste le garanzie previste dagli artt. 45 e seguenti del GDPR (chiaramente, se questi poi si avvarrà di Responsabili che si trovano nel suo stesso paese o comunque al di fuori dello SEE sarà tenuto a rispettare le garanzie previste per il trasferimento dei dati al Responsabile).

La comunicazione dei dati personali, quindi, deve avvenire tra figure diverse dall'interessato (dall'interno dell'UE – Titolare o Responsabile – all'esterno della stessa – destinatario: Responsabile, dipendente autorizzato al trattamento, terzo soggetto).

Un ulteriore chiarimento in merito alla comunicazione che integra il trasferimento è stato fornito dalla Corte di Giustizia Europea con la sentenza del 6 novembre 2003 resa nella causa C-101/01 (caso Lindqvist). Il caso era quello della signora Lindqvist che aveva pubblicato nel proprio blog dati personali riguardanti alcune persone che lavoravano, come lei, in qualità di volontari presso una parrocchia della Chiesa protestante di Svezia.

La Corte di Giustizia ha stabilito che la semplice pubblicazione di dati personali su un sito web non può considerarsi un trasferimento verso un paese terzo (ai sensi dell'allora vigente art. 25 della Direttiva 95/46) in quanto, essendo i dati disponibili a chiunque, si tratterebbe di un trasferimento verso tutti i paesi esteri e il regime speciale stabilito per il trasferimento al di fuori del SEE diventerebbe un regime generale: se anche solo un Paese estero non dovesse garantire un livello di protezione adeguato, gli Stati membri dovrebbero bloccare l'immissione di tutti i dati in rete.

Ne consegue che soltanto la comunicazione diretta da un soggetto europeo a destinatari specifici in paesi terzi rientra nella nozione di trasferimento al di fuori dell'UE.

4.3 Comunicazione e trasferimento

Chiariti questi aspetti, occorre tornare sull'ampiezza del concetto di comunicazione ai fini della sua qualificazione come trasferimento.

Ricordiamo che il Legislatore italiano all'art. 2-ter del D.lgs. 196/2003 (Codice Privacy), introdotto dal D.lgs. n. 101/18 dettaglia maggiormente la nozione di "comunicazione" rispetto all'art. 4 del Regolamento, definendola come il "*dare conoscenza dei dati personali a uno o più soggetti determinati (..) in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione*".

La locuzione comunicazione, dunque, comprende anche l'ipotesi del rendere disponibili i dati per la mera consultazione, accesso, visualizzazione degli stessi.

La semplice messa a disposizione di dati, senza trasmissione, può allora comportare un trasferimento?

Una qualche conferma la si può trovare nella Direttiva 2016/680 del Parlamento Europeo e del Consiglio, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati (Direttiva Polizia).

Tale Direttiva, al paragrafo 1, lett. c), dell'art. 35 "Principi generali per il trasferimento di dati personali", prevede che "*qualora i dati personali siano trasmessi o resi disponibili da un altro Stato membro, tale Stato membro ha fornito la propria autorizzazione preliminare al trasferimento conformemente al proprio diritto nazionale*".

Ne consegue quindi che il "trasferire" comprende anche il "rendere disponibili" senza trasmissione, senza spostamento fisico.

Parte della dottrina è di questo avviso, ma tale ampia definizione di trasferimento è stata spesso avversata, soprattutto dalla frangia più tecnica degli interpreti, secondo i quali ai fini del trasferimento sarebbe necessario lo spostamento fisico del dato.

Sulla base di tale ultima interpretazione molti titolari hanno ritenuto che ad escludere il trasferimento, e dunque l'applicazione delle garanzie di cui agli artt. 45 e seguenti del GDPR, fosse sufficiente che il fornitore extra UE avesse i server in Europa e garantisse l'utilizzo di questi per la conservazione dei dati mediante l'inserimento di tale obbligo nei propri Data Processing Agreements di cui all'art. 28 del GDPR.

In moltissime informative sul trattamento dei dati personali si leggono frasi del tipo, "*il Titolare conserva i dati presso i server propri o dei propri fornitori situati in Unione Europea, sicché non si verifica alcun trasferimento*".

In realtà, per quanto appena ricordato, la circostanza che i dati fisicamente si trovino in UE non esclude che si possa realizzare un trasferimento.

4.4 Trasferimento

A seguito della sentenza Schrems II si è sentita ancora più forte l'esigenza di un chiarimento in merito alla nozione di trasferimento.

E la risposta, fortunatamente, è arrivata dall'European Data Protection Board (EDPB) che con le proprie FAQ sulla sentenza della Corte di Giustizia dell'UE (CGE) pubblicate il 23 luglio 2020 non lascia spazio a dubbi su cosa debba intendersi per "trasferimento" di dati.

Alla FAQ n. 11) "*mi avvalgo di un responsabile del trattamento che tratta dati per mio conto, essendo io il titolare del trattamento. Come posso sapere se il mio responsabile del trattamento trasferisce i dati verso gli Stati Uniti o un altro paese terzo*?" l'EDPB risponde: "*il contratto stipulato con il responsabile in conformità dell'art. 28, paragrafo 3, del GDPR deve stabilire se i trasferimenti siano o meno autorizzati (occorre tenere presente che costituisce un trasferimento anche l'accesso ai dati effettuato a partire da un paese terzo, ad esempio a fini amministrativi) (...) è necessaria particolare attenzione perché numerose soluzioni informatiche possono comportare il trasferimento di dati personali verso un paese terzo (ad esempio a fini di conservazione o manutenzione)*".

È chiaro, quindi, che anche la semplice consultazione di un database sito nell'Unione da parte di un Responsabile che si trova in un Paese terzo, per esempio per fini di assistenza tecnica, comporta trasferimento di dati e richiede il rispetto delle garanzie previste dal Regolamento.

Per escludere il trasferimento non è pertanto sufficiente che il fornitore-responsabile abbia i propri server all'interno dell'Unione Europea ma occorrerà anche che lo stesso garantisca di non effettuare accessi ai server da un paese esterno allo SEE.

Tutto ciò è stato da ultimo confermato dalle Raccomandazioni 1/2020 che esplicitamente richiamano il caso dell'accesso remoto da un paese terzo.

5. Le clausole tipo di protezione dei dati (Standard Contractual Clauses) - Criticità Applicative

5.1. Peso della "security" e "safety" nella normativa sulla privacy europea e statunitense

Sebbene la Commissione Europea, con la sentenza C311-18 del 16 luglio 2020 abbia dichiarato invalida la decisione 2016/1250 relativa al *Privacy Shield* ed, allo stesso tempo, abbia giudicato valida la decisione del 2010/87 relativa alle *Standard Contractual Clauses*, va comunque sottolineato che quest'ultima decisione era stata adottata sulla base della direttiva 95/46 e non ovviamente sulla base del più recente GDPR. Si deduce quindi che, considerando i termini temporali, una possibile criticità applicativa è da ritenersi collegata all'evoluzione della normativa europea in materia di protezione dei dati che ha progressivamente attribuito un peso maggiore ai diritti degli interessati.

Se al tempo della decisione 2010/87 il livello di protezione dei dati che doveva essere garantito nel Paese Terzo faceva riferimento soprattutto al concetto di "*security*" ora il livello di protezione si è adeguato primariamente al concetto di

"*safety*". Quando viene fatto riferimento alla "*safety*" ci si riferisce alla conformità del trattamento del dato in relazione al diritto: dal rispetto del più classico diritto alla riservatezza fino alla protezione del dato personale secondo i principi declinati nell'art.5 del GDPR. Quando, invece, viene fatto riferimento alla "*security*" ci si riferisce alla valutazione del dato come "*asset*" dell'organizzazione in grado di generare anche valore economico in quanto considerato come parte integrante del processo produttivo e gestionale. A tal proposito il GDPR disciplina sia la dimensione della "*safety*" che quella della "*security*" e per questo viene utilizzata come normativa di riferimento anche a livello internazionale per la predisposizione di normative sulla privacy locali.

La suddetta differenza appare evidente se per esempio consideriamo il "*Data processing amendment to Google workspace and/or complementary product agreement (Version 2.3)*". Google, nel documento fa un chiaro riferimento alla sicurezza dei dati personali – intesa soprattutto come protezione dall'eventuale danno economico derivante da un trattamento illecito di dati – ma non ai principi applicabili al trattamento dei dati. Pertanto, con riferimento a questo esempio pratico, anche considerando che le "*Standard Contractual Clauses*" possano valere solamente se i dati personali trasferiti in USA fossero protetti sostanzialmente in maniera equivalente a quello garantito all'interno dell'Unione dal GDPR già appare evidente la mancanza di un riferimento ai principi base declinati dallo stesso Regolamento (in primis la "limitazione della finalità" ex art. 5 co. 1 lett. b) GDPR).

7 Data Security.

7.1 Google's Security Measures, Controls and Assistance.

- *7.1.1 Google's Security Measures. Google will implement and maintain technical and organizational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 2 (the "Security Measures"). The Security Measures include measures to encrypt personal data; to help ensure ongoing confidentiality, integrity, availability and resilience of Google's systems and services; to help restore timely access to personal data following an incident; and for regular testing of effectiveness. Google may update the Security Measures from time to time provided that such updates do not result in the degradation of the overall security of the Services.*
- *7.1.2 Security Compliance by Google Staff. Google will: (a) take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance, and (b) ensure that all persons authorized to process Customer Personal Data are under an obligation of confidentiality.*
- *7.1.3 Additional Security Controls. Google will make Additional Security Controls available to: (a) allow Customer to take steps to secure Customer Data; and (b) provide Customer with information about securing, accessing and using Customer Data.*
- *7.1.4 Google's Security Assistance. Google will (taking into account the nature of the processing of Customer Personal Data and the information available to Google) assist Customer in ensuring compliance with its obligations pursuant to Articles 32 to 34 of the GDPR, by:*

a. implementing and maintaining the Security Measures in accordance with Section 7.1.1 (Google's Security Measures);

b. making Additional Security Controls available to Customer in accordance with Section 7.1.3 (Additional Security Controls);

c. complying with the terms of Section 7.2 (Data Incidents);

d. providing Customer with the Security Documentation in accordance with Section 7.5.1 (Reviews of Security Documentation) and the information contained in the applicable Agreement including this Data Processing Amendment; and

e. if subsections (a)-(d) above are insufficient for Customer to comply with such obligations, upon Customer's request, providing additional reasonable assistance.

Quindi il punto fondamentale che occorre sottolineare è come possano le "*Standard Contractual Clauses*" costituire una garanzia adeguata secondo quanto espresso dall'art.46 del GDPR se poi gli accordi attuativi (vedi l'esempio di Google) proteggono i dati solamente sulla base delle misure di sicurezza declinate nell'art.32 ma non secondo i principi espressi nell'art. 5, che invece nella nostra cultura della privacy europea sono considerati fondamentali. Infatti nel suddetto emendamento Google fa un chiaro riferimento alla crittografia come misura di protezione ma non fa invece alcun riferimento ai principi applicabili al trattamento dei dati personali.

Con riferimento alla crittografia essa viene definita dall'ENISA, l'Agenzia europea per la sicurezza delle reti e delle informazioni, come una forma di pseudonimizzazione. [19] Altre tecniche di pseudonimizzazione oltre la crittografia citate dall'ENISA sarebbero rappresentate dal contatore, dal generatore casuale di numeri (RNG), dalla funzione crittografica di Hash e dal "*Message authentication code*" (MAC). L'ENISA definisce la pseudonimizzazione come "*il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile*" (art.4 definizione di pseudonimizzazione). Le linee guida ENISA sulla pseudonimizzazione definiscono anche il concetto di pseudonimo altrimenti detto criptonimo o, semplicemente, nomio come "*il pezzo di informazione associata a un identificativo di un individuo o a un altro qualsiasi tipo di dato personale (quali, ad esempio, i dati di residenza)*". Le stesse linee guida chiariscono inoltre che cosa si intenda per ente di pseudonimizzazione e riportano delle casistiche circa i soggetti operanti come ente di pseudonimizzazione.

Ai fini dell'analisi condotta sulle criticità applicative delle SCC è opportuno mettere in evidenza che la pseudonimizzazione nel GDPR non è considerata solamente come una misura di conformità alla "*security*" ma anche alla "*safety*" in quanto strumento tecnico in grado di garantire il rispetto dei principi di proporzionalità, necessità e minimizzazione, sin dall'inizio della progettazione (art.25 GDPR).

5.2. Implicazioni della sentenza sul processo di analisi dei rischi dei Titolari

In presenza di un fattore esogeno (la Sentenza) che dichiara invalida una base giuridica precedentemente considerata utilizzabile (il trasferimento sulla base di una decisione di adeguatezza), viene imposta al Titolare una rielaborazione dei rischi del trattamento, probabilmente con la necessità di effettuare una DPIA, indagando e motivando l'implementazione delle effettive misure di "equivalenza sostanziale" che accanto alle SCC, dovrebbero consentire i trattamenti.

Con riferimento a questa considerazione, le recenti raccomandazioni dell'EDPB[20] evidenziano come la Corte di Giustizia dell'Unione Europea abbia stabilito che sia responsabilità del soggetto esportatore e del soggetto importatore valutare se il livello di protezione richiesto dal GDPR sia rispettato nel Paese Terzo interessato, al fine di determinare se le garanzie stabilite dalle SCC possano essere ritenute valide. Qualora a seguito della valutazione del rischio venga messo in evidenza che le garanzie stabilite dalle SCC non possano essere ritenute valide, il Titolare dovrebbe documentare la presa in carico formale e sostanziale delle "misure supplementari" per assicurare un livello di protezione equivalente a quello garantito all'interno del SEE.

Ci si troverebbe pertanto davanti a un caso di analisi dei rischi a responsabilità condivisa tra il soggetto esportatore e il soggetto importatore. Nelle valutazioni dell'impatto e della probabilità di occorrenza della minaccia, l'esportatore potrà contattare l'importatore per verifiche sulla legislazione del Paese del soggetto importatore e sulla validità delle SCC; per contro l'importatore oltre a collaborare nell'eventuale predisposizione di un piano di contenimento del rischio che preveda l'applicazione tra le altre di misure aggiuntive dovrà esprimersi circa la fattibilità stessa del trasferimento anche quando a trattamento effettuato si rendesse conto che non possa essere garantito nel suo Paese un livello di protezione equivalente a quello richiesto dal GDPR.

[19] Linee guida ENISA "Tecniche di pseudonimizzazione e buone pratiche" novembre 2019
[20] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, adopted on November 2020

Alla luce di queste considerazioni, il principio dell'"*accountability*" sembrerebbe quindi determinare un ruolo fondamentale anche nella questione del trasferimento dei dati all'estero e la valutazione dei rischi risulterebbe indispensabile per l'elaborazione di quelle garanzie supplementari alle SCC cui anche il considerando 109) del GDPR farebbe riferimento, purché tali garanzie non contraddicano le clausole stesse.

5.3 Un Caso Pratico: considerazioni sulle criticità applicative delle SCC nelle scuole

Le scuole sono state indirizzate dal Ministero dell'Istruzione, all'inizio dell'emergenza sanitaria e comunque prima della sentenza Schrems II, ad utilizzare per la didattica in digitale piattaforme quali "Office 365 education" e "G-SUITE for education" in quanto ritenute sicure.

Il trasferimento dei dati extra UE per le scuole riguarderebbe il nome e cognome degli alunni, anche minori di 14 anni, e dei docenti, gli indirizzi e-mail istituzionali degli alunni (qualora l'account sia stato creato per quest'ultimi) e dei docenti, e gli elaborati in digitale degli alunni svolti nelle classi virtuali.

Per le scuole dove è stata implementata la "*G-SUITE for education*", i Titolari del trattamento, anche in virtù della dimensione del contesto, difficilmente potrebbero valutare un'alternativa a quella proposta da Google circa il trasferimento dei dati per mezzo delle "*Model Contractual Clauses*". La strategia di Google, sebbene basata su una logica di accettazione dell'emendamento da parte della singola organizzazione, sta infatti rendendo altamente improbabili eventuali richieste delle scuole di trasferire i dati all'estero attraverso soluzioni alternative a quella delle SCC, anche se questa possibilità sarebbe contemplata nell'emendamento stesso.

> *b. if Customer does not enter into the Model Contract Clauses as described in Section 10.2(a), then:*
>
> *i. if an Alternative Transfer Solution is made available by Google: (A) Customer will be deemed to be using it and will take any action (which may include execution of documents) strictly required to give it full effect; and (B) Google will ensure that the transfers are made in accordance with such Alternative Transfer Solution; or*
>
> *ii. if an Alternative Transfer Solution is not made available by Google: (A) Customer (as data exporter) will be deemed to have entered into the Model Contract Clauses with Google LLC (as data importer); (B) the transfers will be subject to the Model Contract Clauses; and (C) Google will ensure Google LLC complies with its obligations under the Model Contract Clauses in respect of those transfers; and*

L'applicazione delle SCC, inoltre, non sembra rispettare completamente il bilanciamento delle responsabilità così come definito nel capo IV del GDPR che distingue i diversi soggetti coinvolti nelle attività di trattamento. Prendendo come riferimento l'art.28, comma 3 lett. a) GDPR, si prevede che il Responsabile del trattamento tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale. Con l'applicazione delle SCC questo rapporto di gerarchia delle responsabilità nell'organigramma privacy non verrebbe rispettato, a svantaggio soprattutto di piccole realtà, quali appunto le scuole, che non avrebbero la forza di dettare delle condizioni a grandi colossi come Google, senza il supporto delle Istituzioni.

Il problema del trasferimento dei dati in USA si porrebbe anche per l'utilizzo dei servizi aggiuntivi, quali estensioni o applicazioni di terze parti, cui sarebbe possibile accedere attraverso le stesse piattaforme attraverso per esempio meccanismi di *log in* con *Single-sign-on* o addirittura attraverso il *download* delle singole estensioni o delle applicazioni di terze parti dal *market place* di Google. Questi servizi esporrebbero le scuole ad ulteriori rischi per gli interessati, soprattutto per i minori, non solo connessi al trasferimento dei dati da parte di società terze all'estero, ma anche connessi all'utilizzo dei dati per finalità proprie del fornitore oltre il miglioramento del singolo servizio.

Viste le suddette criticità alcune scuole hanno inviato una breve lettera all'ufficio legale di "*Google Italy*" per provare a richiedere di mantenere i dati dell'organizzazione all'interno del SEE o di trasferire i dati verso un Paese coperto da una decisione di adeguatezza. Alla data di pubblicazione del presente documento le scuole che hanno presentato la richiesta non hanno ricevuto un riscontro. Questa misura ha in ogni caso sensibilizzato i Dirigenti Scolastici alla tematica del

trasferimento dei dati, in quanto in futuro potrebbe riproporsi in maniera diversa e per trattamenti specifici dell'organizzazione.

Ciò nonostante, facendo riferimento anche alle recenti raccomandazioni dell'EDPB relative all'implementazione di misure supplementari a tutela della protezione dei dati, la delicata questione del trasferimento dei dati extra UE avrebbe prodotto degli impatti positivi sulle scuole. In primis, gli Istituti Scolastici avrebbero iniziato a capire l'importanza della corretta gestione del registro dei trattamenti. Infatti il registro delle attività dei trattamenti non può più essere considerato semplicemente come un adempimento burocratico da mettersi in atto perché richiesto dalla normativa, ma deve essere visto soprattutto come uno strumento sempre più utile per mappare e sviluppare la consapevolezza di quali siano, tra i trattamenti effettuati, quelli che prevedono un trasferimento dei dati extra UE. Avere questa consapevolezza sta diventando per le scuole fondamentale vista anche la loro necessità di coinvolgere nelle attività di trattamento un numero sempre più crescente di responsabili del trattamento.

Inoltre, considerata la potenza di strumenti quali la "*G-SUITE for education*" soprattutto per l'erogazione della didattica in digitale, molti Istituti Scolastici hanno iniziato a comprendere la necessità di utilizzare per i trattamenti che comporterebbero un trasferimento dei dati misure supplementari effettive quali una corretta implementazione della pseudonimizzazione attraverso l'adozione di procedure contestualizzate.

Per contro, dal momento che la maggior parte dei trasferimenti dei dati avviene verso società con sede negli USA, risulterebbe allo stato attuale molto complesso per gli Istituti Scolastici valutare quali misure supplementari potrebbero assicurare un livello di protezione equivalente a quello garantito dal Regolamento europeo.

In ultima analisi, non può passare inosservato, soprattutto per quanto riguarda l'aspetto del trasferimento dei dati extra UE, che alcune informative, come ad esempio quella di Microsoft (https://privacy.microsoft.com/it-it/privacystatement), non siano state aggiornate. L'aspetto relativo all'obbligatorietà di rendere l'informativa trasparente agli interessati è considerato dall'Autorità Garante della Privacy italiana di fondamentale importanza ai fini di garantire la privacy compliance nel processo di adeguamento. Secondo l'art. 83 co. 5 del GDPR, la violazione dei principi di base del trattamento, che nel caso di omissione dell'informativa deriverebbe dalla mancanza di trasparenza del trattamento in corso, è soggetta a sanzioni fino al 4% del fatturato. Pertanto, se la nostra cultura giuridica ci impone di prestare un così elevato livello di importanza all'informativa, sarebbe auspicabile che importanti *player* tecnologici come Microsoft adottino informative aggiornate e trasparenti soprattutto su questioni oggigiorno così delicate quali il trasferimento dei dati all'estero. Considerando la realtà delle scuole, sulla base dell'informative disponibili, sembrerebbe che le caselle di posta messe a disposizione degli Istituti Scolastici da parte del Ministero stiano trasferendo i dati in USA ancora sulla base di una decisione di adeguatezza quale il "*Privacy Shield*". Questa prassi risulterebbe in contraddizione con il trasferimento dei dati secondo il meccanismo delle SCC.

7. Considerazioni conclusive

Alla luce di quanto esposto nelle pagine precedenti, tenuto conto delle informazioni raccolte ed in base alle pronunce e agli orientamenti emanati in questi mesi da parte delle Autorità, di seguito riportiamo alcune considerazioni:

1. Le clausole tipo di protezione dei dati o Standard Contractual Clauses (SCC), delle quali la Corte Europea di Giustizia ha riaffermato la validità, non rappresentano "tout court" una giustificazione per la conformità del trasferimento dati personali fuori del SEE, ma nella loro applicazione, il data controller (titolare) deve obbligatoriamente accertarsi che il data processor prescelto (il responsabile), tenuto conto delle misure di sicurezza adottate e dei vincoli del paese in cui opera e nel quale vengono trasferiti i dati, sia in grado di rispettare, dal punto di vista sostanziale, le disposizioni del GDPR in tema di protezione dei dati personali.
2. Occorre tenere conto che, alla luce dei recenti chiarimenti dell'European Data Protection Board, per "trasferimento" si intende non solo lo spostamento fisico dei dati da un paese all'altro o da un data center ad un

altro ma si considera trasferimento anche la semplice possibilità di accedere ai dati personali da parte di personale e/o organizzazioni situate al di fuori del SEE.

3. Nella progettazione di ogni tipo di trattamento è necessario rispettare i principi di Privacy by Design e di Privacy by Default ex art. 25 del GDPR; in questo senso il ricorso a tecniche / interventi di pseudonimizzazione (ad esempio alla crittografia dei dati) sono altresì raccomandabili per ridurre / mitigare il rischio relativo al trasferimento di dati fuori del SEE.
4. Sul piano operativo, alla luce della sentenza e della conseguente invalidità di una base giuridica in precedenza utilizzabile, a seguito anche delle Raccomandazioni fornite dall'EDPB e fino all'emanazione di linee guida ufficiali da parte delle Autorità di Controllo nazionali, risulta opportuno per i titolari (organizzazioni ed aziende), procedere ad una rivalutazione dei rischi, rivedendo la propria analisi ed attivando una fase di verifica che si potrebbe riassumere nei punti seguenti:
   a) Rivedere analiticamente il registro dei trattamenti al fine di identificare eventuali situazioni a rischio.
   b) Analizzare criticamente la tipologia di dati e il rispetto del principio di minimizzazione rispetto alle finalità, nonché l'elenco dei soggetti destinatari dei dati personali oggetto del trattamento ed i relativi contratti di servizio, rivedendo in particolare le finalità, le basi giuridiche e l'esistenza di circostanze (inclusa la legislazione del paese di esportazione dei dati) che prevedano l'accesso ai dati personali, magari mediante processi di manutenzione / supporto tecnico, che potrebbero presentare dei rischi. In quest'ottica sarà opportuno includere nell'analisi anche i trattamenti effettuati mediante repository di database in sistemi cloud aventi data center nel SEE ma accessibili da soggetti situati fuori del SEE.
   c) Per i trattamenti identificati che utilizzano come base giuridica il Privacy Shield, attivare un processo documentabile di adeguamento basato sull'adozione delle clausole tipo di protezione dei dati (Standard Contractual Clauses), opportunamente valutate ed eventualmente integrate nei termini illustrati in precedenza, valutare la possibilità di adottare le BCR o una delle deroghe previste dall'art. 49 GDPR nel rispetto dei requisiti dell'occasionalità e necessità o in alternativa, procedere alla rimozione del trasferimento al di fuori dello SEE in favore di una soluzione intraUE.
   d) Nel caso di trattamenti di categorie particolari di dati personali ex art. 9 GDPR, in ottica di risk mitigation, evitare il ricorso a trattamenti che richiedano un trasferimento degli stessi al di fuori del SEE.

APPENDICE

ANNEX II Raccomandazioni 01/2020 sulle misure supplementari agli strumenti di trasferimento che assicurino conformità con il livello di protezione dei dati personali dell'UE

69. Le seguenti misure sono esempi di misure supplementari che potreste prendere in considerazione quando affrontate la Fase 4 denominata "Adottare misure supplementari". Questo elenco non è esaustivo. La selezione e l'attuazione di una o più di queste misure non garantirà necessariamente e sistematicamente che il vostro trasferimento soddisfi gli standard essenziali di equivalenza richiesti dalla legislazione dell'UE. Infatti, dovranno essere selezionate quelle misure supplementari che sono in grado di garantire efficacemente tale livello di protezione per i vostri trasferimenti.

70. Qualsiasi misura supplementare può essere ritenuta efficace, ai sensi della sentenza della CGUE "Schrems II" , se e nella misura in cui affronta le carenze specifiche individuate nella vostra valutazione della normativa e del contesto giuridico vigente nel paese terzo. Se, in ultima analisi, non foste in grado di garantire un livello di protezione sostanzialmente equivalente, non dovete procedere al trasferimento dei dati personali.

71. In qualità di titolare del trattamento "data controller" o responsabile del trattamento "data processor" vi potrebbe essere già stato richiesto di implementare alcune delle misure descritte in questo allegato, anche nel caso in cui il vostro importatore di dati fosse coperto da una decisione di adeguatezza, così come può esservi richiesto di attuarle quando trattate i dati all'interno del SEE.[1]

Misure tecniche

72. Questa sezione descrive, in modo non esaustivo, esempi di misure tecniche che possono integrare le garanzie di cui all'articolo 46 GDPR in tema di strumenti per il trasferimento di dati personali, ai fini di assicurare il rispetto del livello di protezione richiesto dal diritto dell'UE nel contesto di un trasferimento di dati personali verso un paese terzo. Tali misure saranno particolarmente necessarie quando la legislazione di tale paese impone all'importatore di dati alcuni obblighi che sono contrari alle garanzie degli strumenti di trasferimento di cui all'articolo 46 GDPR e, in particolare, in grado di pregiudicare la garanzia contrattuale di un livello di protezione sostanzialmente equivalente contro l'accesso a tali dati da parte delle autorità pubbliche di tale paese terzo.[2]

73. Per maggiore chiarezza, questa sezione specifica innanzitutto le misure tecniche che potrebbero essere potenzialmente efficaci in determinati scenari/casi d'uso per garantire un livello di protezione sostanzialmente equivalente. La sezione prosegue con alcuni scenari/casi d'uso in cui non è stato possibile trovare misure tecniche per garantire questo livello di protezione.

[1] Articolo 5.2 GDPR, Articolo 32 GDPR
[2] C-311/18 (Schrems II), paragrafo 135.

Scenari per i quali è stato possibile trovare misure *efficaci*

74. Le misure elencate di seguito sono intese a garantire che l'accesso , da parte di autorità pubbliche di paesi terzi, ai dati trasferiti, non pregiudichi l'efficacia delle garanzie appropriate contenute negli strumenti di trasferimento di cui all'articolo 46 del GDPR. Tali misure si applicano anche nel caso in cui l'accesso delle autorità pubbliche è conforme alla legge del paese dell'importatore, quando tale accesso vada al di là di quanto stabilito come necessario e proporzionato in una società democratica [3] (68). Tali misure mirano a precludere l'accesso potenzialmente illecito impedendo alle autorità di identificare le persone interessate, di dedurre informazioni su di loro, di individuarle in un altro contesto o di associare i dati trasferiti con altri set di dati in loro possesso che possono contenere, tra l'altro, gli identificativi online forniti dai dispositivi, applicazioni, strumenti e protocolli utilizzati dagli interessati in altri contesti.

75. Le autorità pubbliche di paesi terzi possono tentare di accedere ai dati trasferiti:

a) Durante il loro trasferimento accedendo alle linee di comunicazione utilizzate per trasmettere i dati al paese destinatario. Questo accesso può essere passivo, nel qual caso il contenuto della comunicazione, eventualmente dopo un processo di selezione, viene semplicemente copiato. Tuttavia, l'accesso può essere attivo anche nel senso che le autorità pubbliche si interpongono nella comunicazione non solo leggendo il contenuto, ma anche manipolando o sopprimendo parti di esso.

b) Durante la custodia dei dati presso il destinatario dei dati trasferiti, accedendo alle strutture di elaborazione o chiedendo al destinatario dei dati di localizzarli, di estrarre i dati di interesse e di consegnarli alle autorità.

76. In questa sezione vengono presi in considerazione gli scenari in cui le misure applicate sono efficaci in entrambi i casi. Misure supplementari diverse possono essere applicate ed essere sufficienti nella data circostanza di un trasferimento concreto qualora la legge del paese destinatario prevede un solo tipo di accesso. È pertanto necessario che l'esportatore di dati analizzi attentamente, con il sostegno dell'importatore di dati, gli obblighi che incombono a quest'ultimo.

A titolo di esempio, gli importatori di dati statunitensi che rientrano nel campo di applicazione del 50 USC § 1881a (FISA 702) sono sottoposti all'obbligo diretto di concedere l'accesso o di consegnare i dati personali importati che sono in loro possesso, custodia o controllo. Ciò può estendersi a qualsiasi chiave crittografica necessaria per rendere i dati intelligibili.

77. Gli scenari descrivono circostanze specifiche e misure adottate. Eventuali modifiche agli scenari possono danno luogo a conclusioni diverse.

[3] Vedi Articoli 47 e 52 della Carta dei Diritti Fondamentali della EU, Articoli 23.1 GDPR e le Raccomandazioni EDPB sulle garanzie essenziali europee per le misure di sorveglianza.

78. I titolari del trattamento potrebbero dover applicare alcune o tutte le misure qui descritte, indipendentemente dal livello di protezione previsto dalle leggi applicabili all'importatore di dati, in quanto necessarie per conformarsi agli articoli 25 e 32 del GDPR nelle circostanze concrete del trasferimento. In altre parole, gli esportatori possono essere tenuti ad attuare le misure descritte nel presente documento anche se i loro importatori di dati sono coperti da una decisione di adeguatezza, così come i titolari del trattamento ed i responsabili del trattamento possono essere tenuti ad attuarle quando i dati sono trattati all'interno del SEE.

Caso 1: Memorizzazione dei dati per il backup e/o altri scopi che non richiedono l'accesso ai dati in chiaro

79. Un esportatore di dati utilizza un fornitore di servizi di hosting in un paese terzo per memorizzare dati personali, ad esempio per scopi di backup

Se:

1. i dati personali sono trattati con una crittografia avanzata prima della trasmissione,
2. l'algoritmo di cifratura e la sua parametrizzazione (ad es. lunghezza della chiave, modalità di funzionamento, se applicabile) sono conformi allo stato dell'arte e possono essere considerati robusti rispetto all'analisi di cifratura effettuata dalle autorità pubbliche del Paese destinatario secondo le risorse e le capacità tecniche (ad es. potenza di calcolo per attacchi di forza bruta) a loro disposizione,
3. la robustezza della crittografia tiene conto del periodo di tempo specifico durante il quale la riservatezza dei dati personali crittografati deve essere preservata,
4. l'algoritmo di crittografia è implementato in modo impeccabile per mezzo di un software manutenuto correttamente, la cui conformità alle specifiche dell'algoritmo scelto è stata verificata, ad esempio, mediante certificazione,
5. le chiavi sono gestite in modo affidabile (generate, amministrate, memorizzate, se del caso, collegate all'identità di un destinatario e revocate), e
6. 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, territorio o in uno o più settori specifici all'interno di un paese terzo, o presso un'organizzazione internazionale per la quale la Commissione ha stabilito, in conformità all'articolo 45 GDPR, che è assicurato un livello di protezione adeguato,

allora l'EDPB ritiene che la cifratura eseguita fornisca un'efficace misura supplementare di protezione.

Caso 2: Trasferimento di dati con pseudonimo

80. Un esportatore di dati prima di tutto utilizza uno pseudonimo per i dati in suo possesso e poi li trasferisce in un paese terzo per l'analisi, ad esempio, a scopo di ricerca.

Se:

1. un esportatore di dati trasferisce i dati personali trattati in modo tale che i dati personali non possono più essere attribuiti ad un determinato interessato, né essere utilizzati per individuare l'interessato in un gruppo più ampio, senza l'uso di informazioni supplementari [4] (69),

2. che le informazioni supplementari sono detenute esclusivamente dall'esportatore di dati e conservate separatamente in uno Stato membro o in un paese terzo, in un territorio o in uno o più settori specifici all'interno di un paese terzo, o presso un'organizzazione internazionale per la quale la Commissione ha stabilito, conformemente all'articolo 45 GDPR che è garantito un livello di protezione adeguato,

3. la divulgazione o l'uso non autorizzato di tali informazioni supplementari sia impedito da misure di protezione tecniche e organizzative adeguate, inoltre si garantisce che l'esportatore di dati mantenga il controllo esclusivo dell'algoritmo o del repository che consente la re-identificazione utilizzando le informazioni supplementari, e

4. il responsabile 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 con pseudonimo non possono essere attribuiti a una persona fisica identificata o identificabile, anche se incrociati con tali informazioni,

allora l'EDPB ritiene che la pseudonimizzazione effettuata fornisca un' efficace misura supplementare di protezione.

81. Si noti che in molte situazioni, fattori specifici all'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di una persona fisica, la sua posizione fisica o la sua interazione con un servizio disponibile in Internet, in determinati momenti[5] (70) possono consentire l'identificazione di tale persona anche se il suo nome, l'indirizzo o altri semplici identificatori sono omessi.

82. Ciò vale in particolare quando i dati riguardano l'utilizzo di servizi di informazione (orario di accesso, sequenza delle funzionalità a cui si accede, caratteristiche del dispositivo utilizzato, ecc.) Tali servizi potrebbero essere, come per l'importatore di dati personali, soggetti all'obbligo di concedere l'accesso alle stesse autorità pubbliche nella loro giurisdizione, che saranno quindi probabilmente in possesso di dati relativi all'utilizzo di tali servizi informativi da parte della persona o delle persone a cui si rivolgono.

83. Inoltre, considerato che l'utilizzo di alcuni servizi informativi è per natura pubblico e che i medesimi servizi siano fruibili da parte di soggetti che dispongono di risorse sostanziali, i responsabili del trattamento dovranno prestare

[4] In linea con l'articolo 4, paragrafo 5, GDPR: "'pseudonimizzazione' significa il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a una specifica persona interessata senza l'uso di informazioni supplementari, a condizione che tali informazioni supplementari siano conservate separatamente e siano soggette a misure tecniche e organizzative per garantire che i dati personali non siano attribuiti a una persona fisica identificata o identificabile;"

[5] Art. 4(1) GDPR: "'dati personali': qualsiasi informazione concernente una persona fisica identificata o identificabile ('interessato'); per persona fisica identificabile si intende una persona fisica che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un identificatore quale il nome, un numero di identificazione, dati relativi all'ubicazione, un identificatore online o ad uno o più elementi specifici caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale della persona fisica;".

particolare attenzione, considerando che le autorità pubbliche nella loro giurisdizione sono probabilmente in possesso di dati relativi all'uso dei servizi di informazione da parte di una persona a cui si rivolgono.

Caso 3: Semplice transito di dati criptati in paesi terzi

84. Un esportatore di dati desidera trasferire i dati verso una destinazione riconosciuta che offra una protezione adeguata ai sensi dell'articolo 45 del GDPR. I dati vengono solo inoltrati attraverso un paese terzo.

Se:

1. un esportatore di dati trasferisce i dati personali a un importatore di dati in una giurisdizione che garantisce una protezione adeguata, i dati sono trasportati attraverso la rete Internet e possono essere trasportati geograficamente attraversando un paese terzo che non offre un livello di protezione sostanzialmente equivalente,

2. viene utilizzata la cifratura durante il trasporto, per la quale si garantisce che i protocolli di cifratura impiegati siano all'avanguardia e forniscano una protezione efficace contro gli attacchi attivi e passivi con risorse notoriamente a disposizione delle autorità pubbliche del Paese terzo,

3. La decrittazione è possibile solo al di fuori del paese terzo in questione,

4. le parti coinvolte nella comunicazione si accordano su un'autorità o un'infrastruttura di certificazione a chiave pubblica affidabile,

5. vengono utilizzate misure di protezione specifiche ed all' avanguardia contro gli attacchi attivi e passivi ai trasporti criptati,

6. nel caso in cui la cifratura del trasporto non fornisca di per sé una sicurezza adeguata a causa di conosciute vulnerabilità dell'infrastruttura o del software utilizzato, i dati personali sono anche cifrati end-to-end a livello applicativo utilizzando metodi di cifratura all'avanguardia,

7. l'algoritmo di cifratura e la sua parametrizzazione (ad es. lunghezza della chiave, modalità di funzionamento, se del caso) sono conformi allo stato dell'arte e possono essere considerati robusti rispetto alle analisi di cifratura effettuate dalle autorità pubbliche del paese di transito tenendo conto delle risorse e delle capacità tecniche (ad es. potenza di calcolo per attacchi di forza bruta) a loro disposizione,

8. la robustezza della crittografia tiene conto del periodo di tempo specifico durante il quale la riservatezza dei dati personali crittografati deve essere preservata,

9. l'algoritmo di cifratura è implementato in modo impeccabile da software opportunamente manutenuto, la cui conformità alle specifiche dell'algoritmo scelto è stata verificata, ad es. mediante certificazione,

10. è stata esclusa l'esistenza di backdoor (nell' hardware o nel software),

11. le chiavi sono gestite in modo affidabile (generate, amministrate, immagazzinate, se del caso, collegate all'identità del destinatario previsto, e revocate), dall'esportatore o da un ente di fiducia dell'esportatore sotto una giurisdizione che offre un livello di protezione sostanzialmente equivalente,

allora l'EDPB ritiene che la cifratura del trasporto, se necessario in combinazione con la cifratura end-to-end crittografia dei contenuti, fornisce un'efficace misura supplementare.

Caso 4: Destinatario sotto vincolo di riservatezza

85. Un esportatore di dati trasferisce dati personali ad un importatore di dati in un paese terzo specificamente protetto da la legge di quel paese, ad esempio, allo scopo di fornire congiuntamente cure mediche a un paziente o servizi legali a un cliente.

Se

1. la legge di un paese terzo esonera un importatore di dati residente da un accesso potenzialmente illecito ai dati detenuti da tale destinatario per lo scopo prefissato, ad esempio in virtù dell'applicazione all'importatore di dati di un obbligo di segreto professionale,
2. tale esenzione si estende a tutte le informazioni in possesso dell'importatore di dati che possono essere utilizzate per eludere la protezione delle informazioni privilegiate (chiavi crittografiche, password, altre credenziali, ecc.),
3. l'importatore di dati non si avvale dei servizi di un responsabile del trattamento in modo da consentire alle autorità pubbliche di accedere ai dati in possesso del responsabile del trattamento, né inoltra i dati ad un altro soggetto non protetto, sulla base delle modalità di trasferimento di cui all'articolo 46 del GDPR,
4. i dati personali sono criptati prima di essere trasmessi con un metodo conforme allo stato dell'arte che garantisce che la decriptazione non sarà possibile senza la conoscenza della chiave di decriptazione (cifratura end-to-end) per tutto il tempo in cui i dati devono essere protetti,
5. la chiave di decrittazione è nell'esclusiva custodia dell'importatore dei dati protetti e opportunamente protetta contro l'uso o la divulgazione non autorizzata mediante misure tecniche e organizzative conformi allo stato dell'arte, e
6. l'esportatore di dati ha stabilito in modo affidabile che la chiave di cifratura che intende utilizzare corrisponde alla chiave di decifrazione in possesso del destinatario,

allora l'EDPB ritiene che la cifratura del trasporto effettuata fornisca un efficace misura supplementare.

Caso 5: trattamento separato o condiviso tra più parti

86. L'esportatore di dati desidera che i dati personali siano trattati congiuntamente da due o più responsabili indipendenti situati in giurisdizioni diverse senza rivelare loro il contenuto dei dati. Prima della trasmissione, separa i dati in modo tale che nessuna delle parti ricevute da ogni responsabile sia sufficiente per ricostruire i dati personali in tutto o in parte. L'esportatore di dati riceve il risultato dell'elaborazione da ciascuno dei responsabili del trattamento in modo indipendente, e unisce i pezzi ricevuti per arrivare al risultato finale che può costituire un dato personale o aggregato.

Se

1. un esportatore di dati tratta i dati personali in modo tale che siano suddivisi in due o più parti ognuna delle quali non può più essere interpretata o attribuita a un determinato interessato senza l'utilizzo di informazioni supplementari,

2. ognuno delle porzioni viene trasferita ad un responsabile diverso situato in una giurisdizione diversa,

3. i responsabili optano per trattare i dati congiuntamente, ad es. mediante un calcolo sicuro a più parti, in modo che non venga rivelata a nessuno di loro alcuna informazione che non posseggono prima del calcolo,

4. l'algoritmo utilizzato per il calcolo condiviso è sicuro contro avversari attivi,

5. non vi è alcuna prova di collaborazione tra le autorità pubbliche situate nelle rispettive giurisdizioni in cui si trovano i responsabili del trattamento, il che consentirebbe loro di accedere a tutti i set di dati personali in possesso dei responsabili del trattamento e permetterebbe loro di ricostituire e sfruttare il contenuto dei dati personali in una forma chiara in circostanze in cui tale sfruttamento non rispetterebbe l'essenza dei diritti e delle libertà fondamentali degli interessati. Analogamente, le autorità pubbliche di entrambi i paesi non dovrebbero avere l'autorità di accedere ai dati personali detenuti dai responsabili del trattamento in tutte le giurisdizioni interessate,

6. il responsabile del trattamento ha stabilito, mediante un'analisi approfondita dei dati in questione, tenendo conto di ogni informazione in possesso delle autorità pubbliche dei paesi destinatari, che i dati personali da esso trasmessi ai responsabili del trattamento non possono essere ricondotti a una persona fisica identificata o identificabile, anche se incrociati con tali informazioni,

allora l'EDPB ritiene che l'elaborazione separata effettuata fornisca un'efficace misura supplementare.

Scenari in cui non è stato possibile trovare misure

87. Le misure descritte di seguito in alcuni scenari non sarebbero efficaci nel garantire un livello di protezione sostanzialmente equivalente per i dati trasferiti nel paese terzo. Pertanto, non si tratterebbe di misure supplementari.

Caso 6: Trasferimento a fornitori di servizi cloud o ad altri processori che richiedono l'accesso a dati in chiaro

88. Un esportatore di dati si avvale di un fornitore di servizi cloud o di un altro elaboratore per il trattamento dei dati personali secondo le sue istruzioni in un paese terzo

Se

1. un titolare trasferisce i dati a un fornitore di servizi cloud o ad un altro responsabile,

2. il fornitore di servizi cloud o altro responsabile ha bisogno di accedere ai dati in chiaro per eseguire l'incarico assegnato, e

3. il potere concesso alle autorità pubbliche del paese destinatario di accedere ai dati trasferiti va al di là di quanto necessario e proporzionato in una società democratica, [6]

allora l'EDPB, considerando l'attuale stato dell'arte, è incapace di immaginare un'efficace misura tecnica per impedire che tale accesso violi i diritti degli interessati. L'EDPB non esclude che l'ulteriore sviluppo tecnologico possa offrire misure in grado di raggiungere gli scopi imprenditoriali previsti, senza che sia richiesto l'accesso in chiaro.

89. Negli scenari indicati, in cui i dati personali non crittografati sono tecnicamente necessari per la fornitura del servizio da parte dell'responsabile, la cifratura del trasporto e la cifratura dei dati a riposo, anche se considerati nel loro insieme, non costituiscono una misura supplementare che garantisca un livello di protezione sostanzialmente equivalente se l'importatore dei dati è in possesso delle chiavi crittografiche.

Caso 7: Accesso remoto ai dati per scopi commerciali

90. Un esportatore di dati mette a disposizione di soggetti in un paese terzo dati personali da utilizzare per la condivisione di scopi imprenditoriali. Una costellazione tipica può consistere in un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro che trasferisce dati personali a un titolare del trattamento o responsabile del trattamento in un paese terzo appartenente allo stesso gruppo di imprese o a un gruppo di imprese che esercitano un'attività economica comune. L'importatore di dati può, ad esempio, utilizzare i dati ricevuti per fornire servizi di gestione del personale all'esportatore di dati per il quale ha bisogno di dati relativi alle risorse umane, o per comunicare con i clienti dell'esportatore di dati che vivono nell'Unione europea per telefono o per e-mail,

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, attraverso l'utilizzo 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,

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

91. Negli scenari indicati, in cui i dati personali non criptati sono tecnicamente necessari per la fornitura del servizio da parte del responsabile, la cifratura del trasporto e la cifratura dei dati a riposo, anche se presi insieme, non costituiscono

[6] V, artt. 47 e 52 della Carta Europea dei diritti Fondamentali, l'art. 23.1 del GDPR, e le raccomandazioni EDPB sulle European Essential Guarantees for Suveillance Measures.

una misura supplementare che garantisca un livello di protezione sostanzialmente equivalente se l'importatore dei dati è in possesso delle chiavi crittografiche.

Ulteriori misure contrattuali

92. Queste misure consisteranno generalmente in impegni contrattuali [7] unilaterali, bilaterali o multilaterali. [8] Se si utilizza uno strumento di trasferimento di cui all'articolo 46 del GDPR, nella maggior parte dei casi esso conterrà già una serie di impegni (per lo più contrattuali) da parte dell'esportatore e dell'importatore di dati, volti a garantire protezione ai dati personali.[9]

93. In alcune situazioni, queste misure potrebbero integrare e rafforzare le misure di salvaguardia previste dallo strumento di trasferimento e dalla normativa del paese terzo se, tenuto conto delle circostanze del trasferimento, queste non soddisfano tutte le condizioni necessarie per assicurare un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'UE. Considerata la natura delle misure contrattuali, che normalmente non sono in grado di vincolare le autorità di quel paese terzo, se non sono parte del contratto[10] , dette misure dovrebbero essere integrate con altre misure tecniche e organizzative per conseguire il livello di protezione dei dati richiesto. La scelta e l'attuazione di una o più di queste misure non garantirà necessariamente e sistematicamente che il trasferimento soddisfi lo standard di equivalenza sostanziale richiesto dal diritto dell'UE.

94. A seconda di quali misure contrattuali sono già incluse nello strumento di trasferimento prescelto di cui all' articolo 46 del GDPR, potrebbero essere utili anche misure contrattuali aggiuntive per consentire agli esportatori di dati con sede nel SEE di venire a conoscenza di nuovi sviluppi che incidono sulla protezione dei dati trasferiti in paesi terzi.

95. Come già ricordato, le misure contrattuali non potranno escludere l'applicazione della normativa di un paese terzo che non soddisfa lo standard delle European Essential Guarantees individuate dall'EDPB nei casi in cui la normativa obbliga gli importatori a rispettare gli ordini di accesso ai dati che essi ricevono dalle autorità pubbliche.[11]

[7] Ad esempio all'interno delle BCR che dovrebbero in ogni caso regolamentare alcune delle misure elencate di seguito.

[8] Essi avranno carattere privato e non saranno considerati come accordi internazionali di diritto internazionale pubblico. Di conseguenza, di norma non vincolano l'autorità pubblica del paese terzo in quanto non parte del contratto quando sono conclusi con organismi privati di paesi terzi, come sottolineato dalla Corte nella sentenza C-311/18 (Schrems II), punto 125.

[9] Cfr. sentenza C-311/18 (Schrems II), punto 137, in cui la Corte ha riconosciuto che le SCC contengono "*meccanismi efficaci che consentono, in pratica, di garantire il rispetto del livello di protezione richiesto dalla normativa comunitaria e che i trasferimenti di dati personali ai sensi delle clausole di tale decisione sono sospesi o vietati in caso di violazione di tali clausole o di impossibilità di rispettarle"* si veda anche il paragrafo 148).

[10] C-311/18 (Schrems II), paragrafo 125.

[11] Sentenza della CGUE C-311/18 (Schrems II), punto 132.

96. Qui di seguito sono elencati alcuni esempi di queste possibili misure contrattuali, classificate in base alla loro natura:

La previsione dell'obbligo contrattuale di utilizzare misure tecniche specifiche

97. ***A seconda delle circostanze specifiche dei trasferimenti, il contratto potrebbe dover prevedere l'adozione di specifiche misure tecniche per poter effettuare i trasferimenti (cfr. sopra le misure tecniche suggerite).***

98. Condizioni di efficacia:

- Questa clausola potrebbe essere efficace nelle situazioni in cui la necessità di adottare le misure tecniche è stata individuata dall'esportatore. Dovrebbe poi essere inserita in una previsione legale per garantire che anche l'importatore si impegni a mettere in atto le necessarie misure tecniche, laddove ce ne fosse bisogno.

Obblighi di trasparenza:

99. L'esportatore potrebbe aggiungere degli allegati al contratto con le informazioni che l'importatore gli avrà procurato con la massima diligenza possibile, relative all'accesso ai dati da parte delle autorità pubbliche, anche nell'ambito dell'attività di intelligence, sul presupposto che la normativa nel paese di destinazione sia conforme alle European Essential Guarantees individuate dall'EDPB. Ciò potrebbe aiutare l'esportatore di dati a rispettare l'obbligo di documentare la sua valutazione sul livello di protezione nel paese terzo.

100. L'importatore potrebbe, ad esempio, essere tenuto a:

(1) indicare tutte le leggi e i regolamenti del paese di destinazione applicabili all'importatore o ai suoi (sub) responsabili del trattamento che possono consentire l'accesso da parte delle autorità pubbliche ai dati personali oggetto del trasferimento, in particolare nei settori dell'intelligence, polizia, sorveglianza amministrativa applicabile ai dati trasferiti;

(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 report provenienti da varie fonti (ad esempio, partner, fonti pubbliche, giurisprudenza nazionale e decisioni degli organi di controllo) in merito all'accesso ai dati personali da parte delle autorità pubbliche in situazioni di trasferimento di dati dello stesso tipo di quelle in questione (ad esempio, nel settore normativo specifico; relative alla categoria di soggetti cui appartiene l'importatore di dati;...)

(3) indicare quali misure vengono adottate per impedire l'accesso ai dati trasferiti (se del caso);

(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 acro temporale[12] , in particolare nei settori menzionati al

[12] La durata del periodo dovrebbe dipendere dal rischio per i diritti e le libertà degli interessati i cui dati sono oggetto del trasferimento in questione - ad esempio l'ultimo anno precedente la conclusione dello strumento di trasferimento dei dati con l'esportatore.

punto (1), e che comprendono informazioni relative alle richieste pervenute, ai dati richiesti, al soggetto richiedente e alla base giuridica per l'accesso e in che misura l'importatore ha divulgato la richiesta di dati;[13]

(5) specificare se e in quale misura all'importatore è vietato dalla legge fornire le informazioni di cui ai precedenti punti (1) - (5).

101. Tali informazioni potrebbero essere fornite mediante questionari prestabiliti da compilare e firmare da parte dell'importatore, e completate con l'obbligo contrattuale dell'importatore di dichiarare entro un determinato periodo di tempo qualsiasi potenziale modifica di tali informazioni, come avviene normalmente per i processi di due diligence.

102. Condizioni di efficacia:

- L'importatore deve essere in grado di fornire all'esportatore tutte le informazioni di cui sia a conoscenza e dopo aver fatto tutto il possibile per ottenerle.[14]
- Questo obbligo imposto all'importatore è un mezzo per assicurare che l'esportatore diventi e resti consapevole dei rischi connessi al trasferimento dei dati verso un paese terzo. Consentirà quindi all'esportatore di rinunciare a concludere il contratto o, nel caso in cui le informazioni dovessero mutare successivamente alla sua conclusione, di adempiere all'obbligo di sospendere il trasferimento e/o risolvere il contratto se la legge del paese terzo, le garanzie contenute nello strumento utilizzato per di trasferimento di cui all'articolo 46 del GDPR e le eventuali misure di sicurezza supplementari da esso adottate non possono più garantire un livello di protezione sostanzialmente equivalente a quello dell'UE. Tale obbligo non può tuttavia né giustificare la divulgazione dei dati personali da parte dell'importatore, né dare adito alla aspettativa che non vi saranno ulteriori richieste di accesso.

***

103. L'esportatore potrebbe anche aggiungere clausole in base alle quali l'importatore certifica che (1) non ha intenzionalmente creato back doors o programmazioni simili che potrebbero essere utilizzate per accedere al sistema e/o ai dati personali (2) non ha creato o modificato intenzionalmente i suoi processi aziendali in modo da facilitare l'accesso ai dati personali o ai sistemi, e (3) che la legge nazionale o la politica governativa non richiede all'importatore di creare o mantenere back doors o di facilitare l'accesso ai dati personali o ai sistemi o che l'importatore sia in possesso o consegni la chiave di cifratura. [15]

104. Condizioni di efficacia:

[13] L'adempimento di questo dovere non equivale, in quanto tale, a fornire un livello di protezione adeguato. Al tempo stesso, qualsiasi rivelazione inadeguata che si sia effettivamente verificata porta alla necessità di implementare misure supplementari.
[14] Si veda il precedente paragrafo 32.5.
[15] Questa clausola è importante per garantire un adeguato livello di protezione dei dati personali trasferiti e di norma dovrebbe essere richiesta.

- L'esistenza di una normativa o di politiche governative che impediscono agli importatori di diffondere le informazioni possono rendere inefficace questa clausola. L'importatore non potrà quindi stipulare il contratto o dovrà comunicare all'esportatore di non essere in grado di continuare a rispettare i suoi impegni contrattuali. [16]
- Il contratto deve prevedere sanzioni e/o la possibilità per l'esportatore di risolvere il contratto con breve preavviso nelle ipotesi in cui l'importatore non riveli l'esistenza di una back door o programmazione simile o di processi aziendali manipolati o l'eventuale richiesta di implementare una di queste misure o non ne informi tempestivamente l'esportatore non appena ne venga a conoscenza.

***

105. L'esportatore potrebbe rafforzare il proprio potere di condurre audit[17] o verifiche presso le strutture di elaborazione dati dell'importatore, in loco e/o a distanza, per verificare se i dati sono stati comunicati alle autorità pubbliche e a quali condizioni (accesso non oltre quanto ritenuto necessario e proporzionato in una società democratica), ad esempio prevedendo un breve preavviso e meccanismi che garantiscano il rapido intervento di organismi di controllo e rafforzino l'autonomia dell'esportatore nella scelta degli organismi di controllo.

106. Condizioni di efficacia:

- Per essere pienamente efficace l'ambito dell'audit dovrebbe comprendere dal punto di vista legale e tecnico qualsiasi trattamento effettuato da parte dei responsabili (processors) o sub responsabili (processors) dell'importatore sui dati personali trasmessi nel paese terzo.
- I log di accesso e tracciamenti simili dovrebbero essere immodificabili in modo che gli auditor possano trovare prova dell'accesso. I log di accesso e tracciamenti simili dovrebbero anche distinguere tra gli accessi determinati da regolari operazioni aziendali e gli accessi dovuti a ordini o richieste di accesso.

107. Laddove la legge e la prassi del paese terzo dell'importatore sia stata inizialmente valutata e si sia ritenuto che la stessa offra un livello di protezione per i dati trasferiti dall'esportatore sostanzialmente equivalente a quello previsto nell'UE, l'esportatore potrebbe comunque rafforzare l'obbligo dell'importatore di dati di informare tempestivamente l'esportatore dell'incapacità di rispettare gli impegni contrattuali e di conseguenza lo standard richiesto di "livello di protezione sostanzialmente equivalente". [18]

[16] Si veda il precedente paragrafo 32.5.

[17] Si veda ad esempio la clausola 5.f degli SCC tra titolari (controllers) e responsabili (processors) Decisione 2010/87/UE, le verifiche potrebbero essere fornite anche con l'adesione a un codice di condotta o attraverso la certificazione.

[18] Clausola 5.a e d.i della decisione 2010/87/UE del CSC.

108. Tale incapacità di rispettare gli impegni può essere dovuta a modifiche intervenute nella normativa o nella prassi del paese terzo. [19] Le clausole potrebbero stabilire specifici e rigorosi termini e procedure per una rapida sospensione del trasferimento dei dati e/o la risoluzione del contratto e la restituzione o la cancellazione dei dati ricevuti da parte dell'importatore. Il monitoraggio delle richieste ricevute, la loro finalità e l'efficacia delle misure adottate per contrastarle dovrebbero fornire all'esportatore indicazioni sufficienti per esercitare il suo diritto di sospendere o cessare il trasferimento e/o risolvere il contratto.

109. Condizioni di efficacia:

- La comunicazione deve avvenire prima che venga concesso l'accesso ai dati.
- Diversamente, nel momento in cui l'esportatore riceve la comunicazione, i diritti dell'individuo potrebbero essere già stati violati se la richiesta è basata sulle leggi di quel paese terzo che vanno oltre ciò che il livello di protezione dei dati offerto dal diritto dell'UE consente. La comunicazione può comunque servire a prevenire future violazioni e a consentire all'esportatore di adempiere al suo dovere di sospendere il trasferimento dei dati personali verso il paese terzo e/o di risolvere il contratto.
- L'importatore di dati deve monitorare qualsiasi sviluppo legale o politico che possa portare alla sua impossibilità di adempiere ai suoi obblighi, e informare tempestivamente l'esportatore di tali cambiamenti e sviluppi, e se possibile prima della loro attuazione, per consentire all'esportatore di recuperare i dati dall'importatore.
- Le clausole devono prevedere un rapido meccanismo in base al quale l'esportatore di dati autorizzi l'importatore a mettere in sicurezza o a restituire prontamente i dati all'esportatore o, se ciò non è possibile, a cancellare o cifrare i dati in modo sicuro senza necessariamente attendere le istruzioni dell'esportatore, laddove venga raggiunta una soglia specifica da concordare tra l'esportatore e l'importatore di dati. L'importatore dovrebbe attuare questo meccanismo fin dall'inizio del trasferimento dei dati e testarlo regolarmente per garantire che possa essere applicato con un breve preavviso.
- Altre clausole potrebbero consentire all'esportatore di controllare il rispetto di tali obblighi da parte dell'importatore attraverso audit, ispezioni e altre misure di verifica e di farli valere con sanzioni a carico dell'importatore e/o con la facoltà per l'esportatore di sospendere il trasferimento e/o risolvere immediatamente il contratto.

***

110. Nella misura consentita dalla legislazione nazionale del paese terzo, il contratto potrebbe rafforzare gli obblighi di trasparenza dell'importatore prevedendo un metodo "Warrant Canary" [20], in base al quale l'importatore si impegna a pubblicare regolarmente (ad es. almeno ogni 24 ore) un messaggio crittografato con cui informa l'esportatore che a partire da una certa data e ora non ha ricevuto alcun ordine di rivelare dati personali o simili. La

[19] Cfr. C-311/18 (Schrems II), paragrafo 139, in cui la Corte afferma che *"sebbene la clausola 5, lettera d)*, punto *i), consenta a un destinatario di dati personali di non notificare a un Titolare (controller) del trattamento stabilito nell'Unione europea una richiesta giuridicamente vincolante di divulgazione dei dati personali da parte di un'autorità incaricata dell'applicazione della legge, nel caso in cui la legislazione lo vieti a tale destinatario, come ad esempio un divieto di diritto penale il cui scopo è quello di preservare la riservatezza di un'indagine di polizia, il destinatario è tuttavia tenuto, ai sensi della clausola 5 a) dell'allegato alla decisione CSC, a informare il titolare (controller) del trattamento della sua incapacità di rispettare le clausole standard di protezione dei dati."*

[20] N.D.T. La clausola warrant canary prende il nome dagli uccelli delle canarie (I canarini) che venivano usati nelle miniere per rilevare la presenza dei gas tossici.

mancanza di un aggiornamento di questa comunicazione indicherà all'esportatore che l'importatore potrebbe aver ricevuto un ordine.

111. Condizioni di efficacia:

- Le norme del paese terzo devono consentire all'importatore di dati di emettere questa forma di comunicazione passiva all'esportatore.
- L'esportatore di dati deve monitorare automaticamente i messaggi "Warrant Canary".
- L'importatore di dati deve garantire che la sua chiave privata per la firma del Warrant Canary sia conservata in maniera sicura e che non possa essere costretto ad emettere falsi Warrant Canary dalla normativa del paese terzo. A tal fine, potrebbe essere utile ove siano necessarie più firme da parte di persone diverse e/o se il Warrant Canary viene emesso da una persona al di fuori della giurisdizione del paese terzo.

Obblighi di intraprendere azioni specifiche

112. Qualora rientri tra i poteri conferiti all'autorità pubblica richiedente, l'importatore, sulla base della legge del paese di destinazione, potrebbe impegnarsi a verificare la legalità di qualsiasi ordine di trasmettere i dati e di contestare l'ordine se, dopo un'attenta valutazione, conclude che vi sono motivi, sulla base della legge del paese di destinazione, per farlo. Nel caso l'ordine venga contestato, l'importatore dei dati dovrebbe individuare delle misure provvisorie per sospendere gli effetti dell'ordine stesso fino a quando il tribunale non si sarà pronunciato in merito. L'importatore avrebbe l'obbligo di non trasmettere i dati personali richiesti fino a quando non sarà tenuto a farlo sulla base delle norme procedurali applicabili. A seguito di un'attenta valutazione, nell'eseguire l'ordine l'importatore si impegnerebbe inoltre a fornire la quantità minima di informazioni consentite.

113. Condizioni di efficacia

- L'ordinamento giuridico del paese terzo deve offrire vie legali efficaci per contestare gli ordini di trasmettere i dati.
- Questa clausola offrirà sempre una protezione aggiuntiva molto limitata in quanto un ordine di trasmissione dei dati può essere legale secondo l'ordinamento giuridico del paese terzo, ma tale ordinamento giuridico potrebbe non soddisfare gli standard dell'UE. Questo metodo di contrattazione dovrà necessariamente essere complementare ad altre misure supplementari.
- Le contestazioni degli ordini devono produrre un effetto sospensivo secondo il diritto del paese terzo. In caso contrario, le autorità pubbliche avrebbero comunque accesso ai dati delle persone e qualsiasi azione conseguente a favore della persona avrebbe l'effetto limitato di consentirle di chiedere il risarcimento dei danni per le conseguenze negative derivanti dalla trasmissione dei dati.
- L'importatore dovrà essere in grado di documentare e dimostrare all'esportatore le azioni intraprese, esercitando i suoi migliori sforzi, per adempiere a questo impegno.

114. Nella stessa situazione sopra descritta, l'importatore potrebbe impegnarsi a informare la richiedente

autorità pubblica dell'incompatibilità dell'ordine rispetto alle garanzie circa i meccanismi di trasferimento [21] ***contenuti nell'articolo 46 del GDPR e il conseguente conflitto di obblighi per l'importatore. L'importatore notificherebbe contemporaneamente e al più presto possibile l'esportatore e/o l'autorità di controllo competente del SEE, nei limiti del possibile secondo quanto stabilito dall'ordinamento giuridico del paese terzo.***

115. Condizioni di efficacia:

- Tali informazioni sulla protezione conferita dal diritto comunitario e sul conflitto di obblighi dovrebbero avere un certo effetto giuridico nell'ordinamento giuridico del paese terzo, come ad esempio un riesame giudiziario o amministrativo dell'ordine o della richiesta di accesso, il requisito di un mandato giudiziario e/o una sospensione temporanea dell'ordine per garantire una maggiore protezione sui dati.

- L'ordinamento giuridico del paese non deve impedire all'importatore di notificare l'esportatore o almeno l'autorità di controllo competente del SEE per l'ordine o la richiesta di accesso ricevuti.

- L'importatore dovrà essere in grado di documentare e dimostrare all'esportatore le azioni intraprese, esercitando i suoi migliori sforzi, per adempiere a questo impegno.

Responsabilizzare gli interessati all'esercizio dei propri diritti

116. Il contratto potrebbe prevedere che i dati personali trasmessi in chiaro nel normale corso di un'attività di business (incluse le attività di supporto) possono essere accessibili solo con il consenso espresso o implicito dell'esportatore e/o dell'interessato.

117. Condizioni di efficacia:

- Questa clausola potrebbe essere efficace in quelle situazioni in cui gli importatori ricevono richieste dalle autorità pubbliche di cooperare su base volontaria, in contrapposizione, ad esempio, all'accesso ai dati da parte delle autorità pubbliche che avviene all'insaputa dell'importatore o contro la sua volontà.
- In alcune situazioni l'interessato può non essere in grado di opporsi all'accesso o di dare un consenso che soddisfi tutte le condizioni previste dal diritto comunitario (libero, specifico, informato e non ambiguo) (ad esempio nel caso dei dipendenti)[22] .
- Le normative o le politiche nazionali che obbligano l'importatore a non procedere con l'ordine di accesso potrebbero rendere superflua questa clausola, a meno che non possa essere supportata da misure tecniche che richiedano l'intervento dell'esportatore o dell'interessato affinché i dati in chiaro siano accessibili. Queste misure tecniche per limitare l'accesso potrebbero essere previste in particolare se l'accesso è concesso solo in casi specifici di supporto o di servizio, a condizione che i dati stessi siano memorizzati nello SEE.

[21] Ad esempio, gli SCC prevedono che il trattamento dei dati, compreso il trasferimento degli stessi, sia stato e continuerà ad essere effettuato in conformità con "la legge applicabile sulla protezione dei dati". Tale legge è definita come "la legislazione che tutela i diritti e le libertà fondamentali delle persone fisiche e, in particolare, il loro diritto alla privacy in relazione al trattamento dei dati personali applicabile a un responsabile del trattamento dei dati nello Stato membro in cui è stabilito l'esportatore di dati". La CGUE conferma che le disposizioni del GDPR, lette alla luce della Carta dei diritti fondamentali dell'UE, fanno parte di tale legislazione, cfr. CGUE C-311/18 (Schrems II), paragrafo 138.
[22] Art. 4(11) GDPR

***

118. 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 dell'incapacità dell'importatore di rispettare gli impegni contrattuali, per consentire all'interessato di chiedere informazioni e di ottenere una tutela effettiva (ad esempio, presentando un reclamo alla sua autorità di controllo competente e/o all'autorità giudiziaria e dimostrando la sua posizione dinanzi ai tribunali del paese terzo).

119 Condizioni di efficacia:

- Tale notifica potrebbe allertare l'interessato di potenziali accessi ai suoi dati da parte delle autorità pubbliche di paesi terzi. Potrebbe così consentire all'interessato di chiedere informazioni supplementari agli esportatori e di presentare un reclamo all'autorità di controllo competente del proprio paese. Questa clausola potrebbe anche affrontare alcune delle difficoltà che una persona può incontrare nel dimostrare la propria posizione (*locus standi*) dinanzi ai tribunali di paesi terzi per contestare l'accesso ai suoi dati da parte delle autorità pubbliche.
- Le normative e le politiche nazionali possono impedire questa notifica all'interessato. L'esportatore e l'importatore potrebbero tuttavia impegnarsi ad informare l'interessato non appena le restrizioni alla divulgazione dei dati saranno revocate e a fare il possibile per ottenere la deroga al divieto di divulgazione. Come minimo, l'esportatore o l'autorità di controllo competente potrebbe notificare all'interessato la sospensione o la cessazione del trasferimento dei suoi dati personali a causa dell'incapacità dell'importatore di adempiere ai suoi impegni contrattuali a seguito della ricezione di una richiesta di accesso.

120. Il contratto potrebbe impegnare l'esportatore e l'importatore ad assistere l'interessato nell'esercizio dei suoi diritti nella giurisdizione del paese terzo attraverso meccanismi ad hoc di tutela e consulenza legale.

121. Condizioni di efficacia

- Le normative e le politiche nazionali potrebbero imporre condizioni in grado di pregiudicare l'efficacia dei meccanismi di tutela ad hoc previsti.
- La consulenza legale potrebbe essere utile per la persona interessata, soprattutto considerando quanto possa essere complesso e costoso per una persona interessata capire il sistema giuridico di un paese terzo ed esercitare azioni legali dall'estero, potenzialmente in una lingua straniera. Tuttavia, questa clausola offrirà sempre una protezione aggiuntiva limitata, poiché fornire assistenza e consulenza legale alle persone interessate non può di per sé porre rimedio all'incapacità dell'ordinamento giuridico di un paese terzo di fornire un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'UE. Questa misura contrattuale dovrà necessariamente essere complementare ad altre misure supplementari.

Misure organizzative

122. Ulteriori misure organizzative possono consistere in politiche interne, metodi organizzativi, che i titolari e i responsabili del trattamento potrebbero applicare a se stessi e imporre agli importatori di dati in paesi terzi. Essi potrebbero contribuire a garantire la coerenza della protezione dei dati personali durante l'intero ciclo del trattamento. Le misure organizzative potrebbero anche migliorare la consapevolezza degli esportatori dei rischi e dei tentativi di accedere ai dati nei paesi terzi nonché la loro capacità di reagire ad essi. La selezione e l'implementazione di una o più di queste misure non garantirà necessariamente e sistematicamente che il trasferimento soddisfi gli standard essenziali di equivalenza richiesti dalla legislazione dell'UE. A seconda delle circostanze specifiche del trasferimento e della valutazione effettuata sulla legislazione del paese terzo, le misure organizzative sono necessarie per integrare le misure contrattuali e/o tecniche, al fine di garantire un livello di protezione dei dati personali sostanzialmente equivalente a quello garantito all'interno dell'UE.

123. La valutazione delle misure più adeguate deve essere effettuata caso per caso, tenendo presente la necessità per i titolari e i responsabili del trattamento di rispettare il principio di responsabilizzazione. Di seguito, l'EDPB elenca alcuni esempi di misure organizzative che gli esportatori possono attuare, anche se l'elenco non è esaustivo e altre misure potrebbero essere appropriate:

Politiche interne per la gestione dei trasferimenti in particolare tra gruppi di imprese

124. Adozione di adeguate politiche interne con una chiara attribuzione delle responsabilità circa il trasferimento dei dati, canali di segnalazione e procedure operative standard per i casi di richieste sia segrete che ufficiali di accesso ai dati da parte di autorità pubbliche. Soprattutto in caso di trasferimenti di dati tra gruppi di imprese, queste politiche potrebbero includere, tra le altre, la nomina di un team specifico, che dovrebbe avere sede all'interno del SEE, composto da esperti IT, protezione dei dati e leggi sulla privacy, per trattare le richieste che implicano i dati personali trasferiti dall'UE; la notifica alla direzione legale e corporate e all'esportatore di dati attraverso ricevimento di tali richieste; le fasi procedurali per contestare richieste sproporzionate o illegali e la fornitura di informazioni trasparenti agli interessati.

125. Sviluppo di procedure di formazione specifiche per il personale incaricato della gestione delle richieste di accesso ai dati personali da parte delle autorità pubbliche, che dovrebbero essere periodicamente aggiornate per riflettere i nuovi sviluppi legislativi e giurisprudenziali nel paese terzo e nel SEE. Le procedure di formazione dovrebbero includere i requisiti del diritto dell'UE in materia di accesso delle autorità pubbliche ai dati personali, secondo quanto previsto in particolare dall'articolo 52, paragrafo 1, della Carta dei diritti fondamentali. Il personale dovrebbe essere sensibilizzato in particolare mediante la valutazione di esempi pratici di richieste di accesso ai dati da parte delle autorità pubbliche e applicando a tali esempi pratici la norma di cui all'articolo 52, paragrafo 1, della Carta dei diritti fondamentali. Tale formazione dovrebbe tener conto della situazione particolare dell'importatore di dati, ad esempio della legislazione e dei regolamenti del paese terzo a cui l'importatore di dati è soggetto, e dovrebbe essere sviluppata, ove possibile, in collaborazione con l'esportatore di dati.

126. Condizioni di efficacia:

- Queste politiche potrebbero essere previste solo per quei casi dove la richiesta da parte delle autorità pubbliche del paese terzo è compatibile con il diritto dell'Unione europea. [23] Quando la richiesta è incompatibile, queste politiche non sarebbero sufficienti a garantire un livello equivalente di protezione dei dati personali e, come detto sopra, i trasferimenti devono essere interrotti o devono essere messe in atto adeguate misure supplementari per evitare l'accesso.

Misure di trasparenza e responsabilità

127. Documentare e registrare le richieste di accesso ricevute dalle autorità pubbliche e la relativa risposta, accanto alle motivazioni legali e agli attori coinvolti (ad esempio, se l'esportatore è stato avvisato e la sua risposta, la valutazione del team incaricato di trattare con queste richieste, ecc.)). Tali registrazioni dovrebbero essere messe a disposizione dell'esportatore, che dovrebbe a sua volta fornirle agli interessati, se necessario.

128. Condizioni di efficacia:

- La legislazione nazionale del paese terzo potrebbe impedire la divulgazione delle richieste o delle informazioni sostanziali e quindi rendere inefficace questa pratica. L'importatore di dati dovrebbe informare l'esportatore della sua incapacità di fornire tali documenti e registrazioni, offrendogli così la possibilità di sospendere i trasferimenti se tale incapacità comportasse una diminuzione del livello di protezione.

***

129. Pubblicazione regolare di rapporti sulla trasparenza o di sintesi riguardanti le richieste governative di accesso ai dati e il tipo di risposta fornita, nella misura in cui la pubblicazione è consentita dalla legge locale.

130. Condizioni di efficacia:

- Le informazioni fornite devono essere pertinenti, chiare e il più possibile dettagliate. La legislazione nazionale del paese terzo potrebbe impedire la divulgazione di informazioni dettagliate. In questi casi, l'importatore di dati dovrebbe impegnarsi il più possibile per pubblicare informazioni statistiche o informazioni aggregate di tipo analogo.

Metodi di organizzazione e misure di minimizzazione dei dati

131. Requisiti organizzativi già esistenti sulla base del principio di responsabilità, come anche l'adozione di politiche rigorose e granulari sull'accesso e la confidenzialità dei dati e delle migliori pratiche, basate su un rigido principio della necessità di sapere, monitorate attraverso audit regolari e applicate attraverso misure disciplinari potrebbero

[23] Cfr. causa C-362/14 (" Schrems I "), par. 94; C-311/18 ("Schrems II"), punti 168, 174, 175 e 176.

essere misure utili in un contesto di trasferimento. A questo proposito si dovrebbe considerare 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 viene consentito un accesso limitato invece di un accesso completo; oppure quando la fornitura di un servizio richiede solo il trasferimento di un insieme limitato di dati e non di un'intera banca dati).

132. Condizioni di efficacia:

- Dovrebbero essere introdotti audit regolari e forti misure disciplinari al fine di monitorare e
- far rispettare la conformità con le misure di minimizzazione dei dati anche nel contesto del trasferimento.
- L'esportatore di dati dovrebbe effettuare una valutazione dei dati personali in suo possesso prima che si verifichi il trasferimento, al fine di identificare quegli insiemi di dati che non sono necessari ai fini del trasferimento e che, quindi, non saranno condivisi con l'importatore dei dati.
- Le misure di minimizzazione dei dati dovrebbero essere accompagnate da misure tecniche per garantire che i dati non siano soggetti ad accesso non autorizzato. Ad esempio, l'implementazione di sicuri meccanismi computazionali multi-party e la diffusione di insiemi di dati criptati tra diverse entità di fiducia può impedire by design che qualsiasi accesso unilaterale comporti una divulgazione di dati identificabili.

***

133. Sviluppo delle migliori pratiche per coinvolgere e fornire accesso alle informazioni in modo appropriato e tempestivo al responsabile della protezione dei dati, se esistente, e ai servizi legali e di revisione interna su questioni relative ai trasferimenti internazionali di dati personali.

134. Condizioni di efficacia:

- Il responsabile della protezione dei dati, se esistente, e il team legale e di revisione interna dovrebbero venire a conoscenza di tutte le informazioni pertinenti prima del trasferimento e dovrebbero essere consultati sulla necessità del trasferimento e sulle eventuali misure di salvaguardia.
- Le informazioni pertinenti dovrebbero includere, ad esempio, la valutazione sulla necessità di trasferire i dati personali specifici, una panoramica delle leggi applicabile al paese terzo e le garanzie che l'importatore si è impegnato ad attuare.

Adozione di standard e migliori pratiche

135. Adozione di rigide politiche di sicurezza e protezione dei dati, basate su certificazioni EU o su codici di condotta o su standard internazionali (ad es. norme ISO) e sulle migliori pratiche (ad es. ENISA) tenendo conto dello stato dell'arte, in funzione del rischio delle categorie di dati trattati e della probabilità di tentativi di accesso da parte delle autorità pubbliche.

Altre misure

136. Adozione e revisione periodica delle politiche interne per valutare l'adeguatezza delle misure complementari implementate ed individuare nonché attuare, se necessario, soluzioni aggiuntive o alternative per garantire che sia mantenuto un livello di protezione dei dati personali trasferiti equivalente a quello garantito all'interno dell'UE.

***

137. Impegni da parte dell'importatore di dati a non procedere con alcun trasferimento successivo dei dati personali all'interno dello stesso paese o di altri paesi terzi, o sospendere i trasferimenti in corso, qualora non possa essere garantito nel paese terzo un livello di protezione dei dati personali equivalente a quello offerto all'interno dell'UE. [24]

[24] C-311/18 (Schrems II), paragrafi 135 e 137.