Translations proofread by EDPB Members.
This language version has not yet been proofread.

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

Adottate il 10 novembre 2020

Sintesi

Il regolamento generale sulla protezione dei dati (RGPD) dell'UE è stato adottato per un duplice scopo: agevolare la libera circolazione dei dati personali all'interno dell'Unione europea preservando al contempo i diritti e le libertà fondamentali delle persone, in particolare il loro diritto alla protezione dei dati personali.

Nella recente sentenza C-311/18 (Schrems II) la Corte di giustizia dell'Unione europea (CGUE) ricorda che la protezione concessa ai dati personali nello Spazio economico europeo (SEE) deve transitare con i dati ovunque essi siano trasferiti. Il trasferimento di dati personali verso paesi terzi non può essere un mezzo per minare o indebolire la protezione che viene garantita nel SEE. La Corte afferma ciò chiarendo inoltre che il livello di protezione nei paesi terzi non deve necessariamente essere identico a quello garantito all'interno del SEE, ma sostanzialmente equivalente. La Corte sostiene inoltre la validità delle clausole contrattuali tipo, in quanto strumento di trasferimento che può servire a garantire sul piano contrattuale un livello di protezione sostanzialmente equivalente per i dati trasferiti verso paesi terzi.

Le clausole contrattuali tipo e gli altri strumenti di trasferimento di cui all'articolo 46 del RGPD non operano in modo isolato. La Corte afferma che i titolari o responsabili del trattamento, in qualità di esportatori, hanno la responsabilità di verificare, caso per caso e, ove necessario, in collaborazione con l'importatore nel paese terzo, se la legge o la prassi di quest'ultimo incide sull'efficacia delle garanzie adeguate contenute negli strumenti di trasferimento di cui all'articolo 46 del RGPD. In tali casi la Corte lascia comunque aperta la possibilità per gli esportatori di attuare misure supplementari che colmino queste lacune nella protezione e la portino al livello richiesto dal diritto dell'UE. La Corte non specifica di quali misure potrebbe trattarsi, ma sottolinea che gli esportatori dovranno identificarle caso per caso. Ciò è in linea con il principio di responsabilità di cui all'articolo 5, paragrafo 2, del RGPD, che richiede che i titolari del trattamento siano responsabili del rispetto dei principi del suddetto regolamento relativi al trattamento dei dati personali e siano in grado di dimostrarlo.

Per aiutare gli esportatori (siano essi titolari del trattamento o responsabili del trattamento, enti privati o organismi pubblici, che trattano dati personali nell'ambito di applicazione del RGPD) nel complesso compito di valutare i paesi terzi e di individuare, se necessario, misure supplementari adeguate, il comitato europeo per la protezione dei dati (EDPB) ha adottato le presenti raccomandazioni, le quali forniscono agli esportatori una serie di passi da seguire, potenziali fonti di informazione e alcuni esempi di misure supplementari che potrebbero essere messe in atto.

Come **primo passo**, l'EDPB consiglia a voi, esportatori, di **conoscere i vostri trasferimenti**. La mappatura di tutti i trasferimenti di dati personali verso paesi terzi può essere un esercizio difficile. Essere consapevoli della destinazione dei dati personali è tuttavia necessario per garantire un livello di protezione sostanzialmente equivalente in tutti i luoghi in cui vengono trattati. Dovete inoltre verificare che i dati trasferiti siano adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per le quali vengono trasferiti e trattati nel paese terzo.

Un **secondo** passo consiste nel **verificare lo strumento di trasferimento su cui si basa il vostro trasferimento** tra quelli elencati al capo V del RGPD. Qualora la Commissione europea abbia già dichiarato il paese, la regione o il settore verso cui trasferirete i dati come adeguato, attraverso una decisione di adeguatezza ai sensi dell'articolo 45 del RGPD o della precedente direttiva 95/46 fintanto che la decisione è ancora in vigore, non dovrete adottare ulteriori misure, se non controllare che la decisione di adeguatezza sia ancora valida. In assenza di una decisione di adeguatezza, dovete fare affidamento su uno degli strumenti di trasferimento elencati all'articolo 46 del RGPD per i

trasferimenti regolari e ripetitivi. Solo in alcuni casi di trasferimenti occasionali e non ripetitivi potete fare affidamento su una delle deroghe previste dall'articolo 49 del RGPD, se soddisfate le condizioni.

Un **terzo passo** consiste nel **valutare** se vi sia qualcosa **nella legge o nella prassi del paese terzo** che possa incidere sull'efficacia delle garanzie adeguate degli strumenti di trasferimento su cui fate affidamento, nel contesto del vostro specifico trasferimento. La vostra valutazione deve concentrarsi principalmente sulla legislazione del paese terzo rilevante per il trasferimento e sullo strumento di trasferimento ai sensi dell'articolo 46 del RGPD su cui fate affidamento e che potrebbe pregiudicarne il livello di protezione. Per valutare gli elementi da prendere in considerazione nella valutazione della legislazione di un paese terzo che disciplina l'accesso ai dati da parte delle autorità pubbliche ai fini della sorveglianza, è opportuno fare riferimento alle raccomandazioni dell'EDPB relative alle garanzie essenziali europee. In particolare, occorre considerare attentamente questo aspetto quando la legislazione che disciplina l'accesso ai dati da parte delle autorità pubbliche è ambigua o non è disponibile al pubblico. In assenza di una legislazione che disciplini le circostanze in cui le autorità pubbliche possono accedere ai dati personali, se desiderate comunque procedere con il trasferimento, dovete esaminare altri fattori pertinenti e oggettivi e non basarvi su fattori soggettivi, come la probabilità che le autorità pubbliche accedano ai vostri dati in modo non conforme agli standard dell'UE. Dovete condurre questa valutazione con la dovuta diligenza e documentarla accuratamente, in quanto sarete ritenuti responsabili della decisione che prenderete su tale base.

Un **quarto passo** consiste nell'**individuare e adottare le misure supplementari** necessarie per portare il livello di protezione dei dati trasferiti a un livello sostanzialmente equivalente a quello dell'UE. Questa misura è necessaria solo se la vostra valutazione rivela che la legislazione del paese terzo incide sull'efficacia dello strumento di trasferimento ai sensi dell'articolo 46 del RGPD su cui fate affidamento o su cui intendete fare affidamento nel contesto del vostro trasferimento. Le presenti raccomandazioni contengono (nell'allegato 2) un elenco non esaustivo di esempi di misure supplementari con alcune delle condizioni eventualmente richieste per essere efficaci. Come nel caso delle garanzie adeguate contenute negli strumenti di trasferimento di cui all'articolo 46, alcune misure supplementari possono essere efficaci in alcuni paesi, ma non necessariamente in altri. Sarete responsabili della valutazione della loro efficacia nel contesto del trasferimento e alla luce della legge del paese terzo e dello strumento di trasferimento su cui fate affidamento; sarete inoltre ritenuti responsabili della decisione presa. Ciò potrebbe anche richiedere la combinazione di diverse misure supplementari. In ultima analisi, potreste scoprire che nessuna misura supplementare riesce a garantire un livello di protezione sostanzialmente equivalente per il vostro specifico trasferimento. Nei casi in cui nessuna misura supplementare sia adeguata, dovete evitare, sospendere o interrompere il trasferimento per evitare di pregiudicare il livello di protezione dei dati personali. Anche questa valutazione delle misure supplementari va condotta con la dovuta diligenza e documentata.

Un **quinto passo** consiste nell'**adozione** di eventuali **passi procedurali formali** richiesti dall'adozione della vostra misura supplementare, a seconda dello strumento di trasferimento di cui all'articolo 46 del RGPD su cui fate affidamento. Le presenti raccomandazioni riportano nel dettaglio tali formalità; in alcuni casi potrebbe essere necessario consultare le autorità di controllo competenti.

Il **sesto e ultimo passo** consisterà nel rivalutare a intervalli adeguati il livello di protezione dei dati che trasferite verso paesi terzi e di controllare se ci sono stati o ci saranno sviluppi che possano influire in questo senso. Il principio di responsabilizzazione richiede vigilanza continua circa il livello di protezione dei dati personali.

Le autorità di controllo continueranno a esercitare il loro mandato per monitorare l'applicazione del RGPD e farlo rispettare. Le autorità di controllo terranno in debita considerazione le azioni intraprese dagli esportatori per garantire che i dati da essi trasferiti godano di un livello di protezione sostanzialmente equivalente. Come ricorda la Corte, le autorità di controllo sospenderanno o vieteranno il trasferimento dei dati nei casi in cui, a seguito di un'indagine o di un reclamo, ritengano che non possa essere garantito un livello di protezione sostanzialmente equivalente.

Le autorità di controllo continueranno a sviluppare orientamenti per gli esportatori e a coordinarne le azioni in seno all'EDPB per garantire la coerenza nell'applicazione della legislazione dell'UE in materia di protezione dei dati.

Indice

Il comitato europeo per la protezione dei dati

visto l'articolo 70, paragrafo 1, lettera e), del regolamento 2016/679/UE del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (in appresso: il «RGPD»),

visto l'accordo sullo Spazio economico europeo (SEE), in particolare l'allegato XI e il protocollo 37 dello stesso, modificato dalla decisione del comitato misto SEE n. 154/2018, del 6 luglio 2018[1],

visto l'articolo 12 e l'articolo 22 del regolamento interno,

considerando quanto segue:

(1) Nella sentenza del 16 luglio 2020 *Data Protection Commissioner contro Facebook Ireland Limited e Maximillian Schrems*, C-311/18, la Corte di giustizia dell'Unione europea (CGUE) conclude che l'articolo 46, paragrafo 1, e l'articolo 46, paragrafo 2, lettera c), del RGPD, devono essere interpretati nel senso che le garanzie adeguate, i diritti azionabili e i mezzi di ricorso effettivi richiesti da tali disposizioni devono garantire che i diritti delle persone i cui dati personali sono trasferiti verso un paese terzo sul fondamento di clausole tipo di protezione dei dati godano di un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione da tale regolamento, letto alla luce della Carta dei diritti fondamentali dell'Unione europea[2].

(2) Come sottolineato dalla Corte, un livello di protezione delle persone fisiche sostanzialmente equivalente a quello garantito all'interno dell'Unione dal RGPD, letto alla luce della Carta, deve essere garantito indipendentemente dalla disposizione del capo V sul cui fondamento viene effettuato un trasferimento di dati personali verso un paese terzo. Le disposizioni del capo V mirano a garantire la continuità del livello elevato di tale protezione in caso di trasferimento di dati personali verso un paese terzo[3].

(3) Il considerando 108 e l'articolo 46, paragrafo 1, del RGPD, prevedono che, in mancanza di una decisione di adeguatezza dell'Unione, 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. Il titolare del trattamento o il responsabile del trattamento può fornire garanzie adeguate, senza richiedere un'autorizzazione specifica da parte di un'autorità di controllo, utilizzando uno degli strumenti di trasferimento elencati all'articolo 46, paragrafo 2, del RGPD, come le clausole tipo di protezione dei dati.

[1] Nel presente documento, con «Stati membri» si fa riferimento agli «Stati membri del SEE».
[2] Sentenza della CGUE del 16 luglio 2020, *Data Protection Commissioner contro Facebook Ireland Limited e Maximillian Schrems*, [in appresso: C-311/18 (Schrems II)], seconda conclusione.
[3] C-311/18 (Schrems II), paragrafi 92 e 93.

(4) La Corte chiarisce che le clausole tipo di protezione dei dati adottate dalla Commissione hanno il solo scopo di fornire garanzie contrattuali che si applicano in modo uniforme in tutti i paesi terzi ai titolari del trattamento e ai responsabili del trattamento stabiliti nell'Unione. Visto il loro carattere contrattuale, le clausole tipo di protezione dei dati non possono vincolare le autorità pubbliche di paesi terzi, poiché queste ultime non sono parti del contratto. Di conseguenza, gli esportatori di dati potrebbero dover integrare le garanzie contenute in tali clausole tipo di protezione dei dati con misure supplementari per garantire il rispetto del livello di protezione richiesto dal diritto dell'Unione in un determinato paese terzo. La Corte fa riferimento al considerando 109 del RGPD, che menziona questa possibilità e incoraggia i titolari del trattamento e i responsabili del trattamento ad avvalersene[4].

(5) La Corte ha affermato che incombe anzitutto all'esportatore dei dati verificare, caso per caso e, eventualmente, in collaborazione con l'importatore dei dati, se il diritto del paese terzo di destinazione garantisce un livello di protezione sostanzialmente equivalente, alla luce del diritto dell'Unione, dei dati personali trasferiti sulla base di clausole tipo di protezione dei dati, fornendo, se necessario, garanzie supplementari rispetto a quelle offerte da tali clausole[5].

(6) Qualora il titolare del trattamento o il responsabile del trattamento, stabiliti nell'Unione, non possano adottare misure supplementari sufficienti a garantire un livello di protezione sostanzialmente equivalente ai sensi del diritto dell'Unione, essi o, in subordine, l'autorità di controllo competente, sono tenuti a sospendere o mettere fine al trasferimento di dati personali verso il paese terzo interessato[6].

(7) Il RGPD o la Corte non definiscono o specificano le «garanzie supplementari» o le «misure supplementari» alle garanzie degli strumenti di trasferimento elencati all'articolo 46, paragrafo 2, del RGPD, che i titolari del trattamento e i responsabili del trattamento possono adottare per garantire il rispetto del livello di protezione richiesto dal diritto dell'Unione in un determinato paese terzo.

(8) L'EDPB ha deciso, di propria iniziativa, di esaminare la questione e di fornire ai titolari del trattamento e ai responsabili del trattamento, in qualità di esportatori, raccomandazioni sul processo che possono seguire per individuare e adottare misure supplementari. Tali raccomandazioni mirano a fornire agli esportatori una metodologia per determinare se e quali misure supplementari dovrebbero essere adottate per i loro trasferimenti. È responsabilità primaria degli esportatori garantire che nel paese terzo sia offerto ai dati trasferiti un livello di protezione sostanzialmente equivalente a quello garantito nell'Unione. Con queste raccomandazioni, l'EDPB mira a incoraggiare l'applicazione coerente del RGPD e della sentenza della Corte, conformemente al proprio mandato[7].

HA ADOTTATO LA SEGUENTE RACCOMANDAZIONE:

[4] C-311/18 (Schrems II), paragrafi 132 e 133.
[5] C-311/18 (Schrems II), paragrafo 134.
[6] C-311/18 (Schrems II), paragrafo 135.
[7] Articolo 70, paragrafo 1, lettera e), del RGPD.

1 RESPONSABILIZZAZIONE NEL TRASFERIMENTO DEI DATI

1. Il diritto primario dell'Unione considera il diritto alla protezione dei dati come un diritto fondamentale[8]. Di conseguenza, il diritto alla protezione dei dati gode di un elevato livello di protezione e possono essere apportate limitazioni solo se sono previste dalla legge, rispettano il contenuto essenziale di detto diritto, rispettano il principio di proporzionalità, sono necessarie e rispondono effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui[9]. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità[10].

2. Un livello di protezione sostanzialmente equivalente a quello garantito nell'UE deve accompagnare i dati quando sono trasferiti verso paesi terzi al di fuori del SEE, per garantire che il livello di protezione assicurato dal RGPD non sia pregiudicato.

3. Il diritto alla protezione dei dati ha un carattere attivo, ossia impone agli esportatori e agli importatori (siano essi titolari del trattamento e/o responsabili del trattamento) di andare oltre il riconoscimento o il rispetto passivo di tale diritto[11]. I titolari del trattamento e i responsabili del trattamento devono cercare di rispettare il diritto alla protezione dei dati in modo attivo e continuo, attuando misure giuridiche, tecniche e organizzative che ne garantiscano l'efficacia. Essi devono inoltre essere in grado di comprovare questi sforzi agli interessati, al pubblico in generale e alle autorità di controllo in materia di protezione dei dati. Questo è il cosiddetto principio di responsabilizzazione[12].

4. Il principio di responsabilizzazione, necessario per garantire l'effettiva applicazione del livello di protezione conferito dal RGPD, si applica anche ai trasferimenti di dati verso paesi terzi[13], in quanto si tratta di una forma di trattamento dei dati in sé[14]. Come sottolineato dalla Corte nella sentenza, un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione dal RGPD, letto alla luce della Carta, deve essere garantito indipendentemente da quale sia la disposizione di detto capo sul cui fondamento viene effettuato un trasferimento di dati personali verso un paese terzo[15].

5. Nella sentenza Schrems II, la Corte sottolinea la responsabilità degli esportatori e degli importatori di garantire che il trattamento dei dati personali sia effettuato e continuerà a essere effettuato nel rispetto del livello di protezione stabilito dal diritto dell'Unione in materia di protezione dei dati e di sospendere il trasferimento e/o risolvere il contratto qualora l'importatore dei dati non sia o non sia più in grado di rispettare le clausole tipo di protezione dei dati inserite nel relativo contratto tra l'esportatore e l'importatore[16]. Il titolare del trattamento o il responsabile del trattamento che agisce

[8] Articolo 8, paragrafo 1, della Carta dei diritti fondamentali e articolo 16, paragrafo 1, TFUE, primo preambolo e articolo 1, paragrafo 2, del RGPD.
[9] Articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea.
[10] Considerando 4 del RGPD e C-507/17, Google LLC, succeduta alla Google Inc., contro Commission nationale de l'informatique et des libertés (CNIL), paragrafo 60.
[11] C-92/09 e C-93/02, Volker und Markus Schecke GbR contro Land Hessen, conclusioni dell'avvocato generale Sharpston, 17 giugno 2010, paragrafo 71.
[12] Articolo 5, paragrafo 2, e articolo 28, paragrafo 3, lettera h), del RGPD.
[13] Articolo 44 e considerando 101 del RGPD, nonché articolo 47, paragrafo 2, lettera d), del RGPD.
[14] Sentenza della Corte di giustizia dell'Unione europea del 6 ottobre 2015, *Maximillian Schrems contro il Data protection Commissioner [di seguito «C-362/14 (Schrems I)»], paragrafo 45.*
[15] C-311/18 (Schrems II), paragrafi 92 e 93.
[16] C-311/18 (Schrems II), paragrafi 134, 135, 139, 140, 141 e 142.

in qualità di esportatore deve garantire che gli importatori collaborino con l'esportatore, se del caso, nell'adempimento di tali responsabilità, tenendolo informato, ad esempio, di qualsiasi sviluppo che influisca sul livello di protezione dei dati personali ricevuti nel paese dell'importatore[17]. Tali responsabilità sono un'applicazione del principio di responsabilizzazione in materia di trasferimenti di dati ai sensi del RGPD[18].

2 TABELLA DI MARCIA: APPLICARE IL PRINCIPIO DI RESPONSABILIZZAZIONE AL TRASFERIMENTO DEI DATI NELLA PRATICA

6. Quella che segue è una tabella di marcia dei passi da compiere per scoprire se voi (esportatori di dati) dovete mettere in atto misure supplementari per poter trasferire legalmente i dati al di fuori del SEE. Nel presente documento, per «voi» si intendono i titolari del trattamento o i responsabili del trattamento che agiscono in qualità di esportatori di dati, che trattano dati personali nell'ambito di applicazione del RGPD (compreso il trattamento da parte di enti privati e organismi pubblici in caso di trasferimento di dati a enti privati)[19]. Per quanto riguarda i trasferimenti di dati personali effettuati tra organismi pubblici, le *linee guida 2/2020 sull'articolo 46, paragrafo 2, lettera a), e sull'articolo 46, paragrafo 3, lettera b), del regolamento 2016/679 per i trasferimenti di dati personali tra autorità e organismi pubblici del SEE ed extra SEE* forniscono orientamenti specifici[20].

7. Dovrete documentare adeguatamente questa valutazione e le misure supplementari da voi selezionate e attuate e, su richiesta, mettere a disposizione dell'autorità di controllo competente tale documentazione[21].

2.1 Primo passo: conoscere i propri trasferimenti

8. Per sapere cosa può essere necessario affinché voi (l'esportatore di dati) possiate continuare a effettuare trasferimenti di dati personali o possiate effettuarne di nuovi[22], il primo passo consiste nell'assicurarvi di essere pienamente consapevoli dei vostri trasferimenti (conoscere i vostri trasferimenti). La registrazione e la mappatura di tutti i trasferimenti può essere un esercizio complesso per le entità impegnate in trasferimenti multipli, diversificati e regolari con paesi terzi e che ricorrono a una serie di responsabili del trattamento a vari livelli. Conoscere i propri trasferimenti è un primo passo essenziale per adempiere ai propri obblighi ai sensi del principio di responsabilizzazione.

[17] C-311/18 (Schrems II), paragrafo 134.
[18] Articolo 5, paragrafo 2, e articolo 28, paragrafo 3, lettera h), del RGPD.
[19] Cfr. Linee-guida 3/2018 dell'EDPB sull'ambito di applicazione territoriale del RGPD (articolo 3) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_it
[20] Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies; cfr. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en
[21] Articolo 5, paragrafo 2, del RGPD e articolo 24, paragrafo 1, del RGPD.
[22] Si osservi che anche l'accesso remoto da parte di un'entità di un paese terzo a dati situati nel SEE è considerato un trasferimento.

9. Per acquisire piena consapevolezza dei vostri trasferimenti, potete basarvi sui registri delle attività di trattamento che potreste essere obbligati a tenere in qualità di titolari del trattamento o di responsabili del trattamento ai sensi dell'articolo 30 del RGPD[23]. Possono anche esservi di aiuto le azioni volte ad adempiere agli obblighi di informazione degli interessati ai sensi dell'articolo 13, paragrafo 1, lettera f), e dell'articolo 14, paragrafo 1, lettera f), del RGPD, sui vostri trasferimenti dei loro dati personali verso paesi terzi[24].

10. Nel mappare i trasferimenti, non dimenticate di tenere conto anche dei trasferimenti successivi, ad esempio se i vostri responsabili del trattamento al di fuori del SEE trasferiscono i dati personali che avete affidato loro a un responsabile del trattamento di secondo livello in un altro paese terzo o nello stesso paese terzo[25].

11. In linea con il principio della «minimizzazione dei dati»[26], dovete verificare che i dati trasferiti siano adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per le quali vengono trasferiti e trattati nel paese terzo.

12. Queste attività devono essere svolte prima di qualsiasi trasferimento e aggiornate prima di riprendere i trasferimenti dopo la sospensione delle operazioni di trasferimento dei dati: dovete sapere dove si trovano o possono essere trattati dagli importatori i dati personali che avete esportato (mappa delle destinazioni).

13. Occorre tenere presente che anche l'accesso remoto da un paese terzo (ad esempio in situazioni di supporto) e/o l'archiviazione in una piattaforma cloud situata al di fuori del SEE sono considerati un trasferimento[27]. In particolare, se si utilizza un'infrastruttura cloud internazionale, dovete valutare se i dati saranno trasferiti in paesi terzi e dove, a meno che il fornitore del cloud non dichiari chiaramente nel contratto che i dati non saranno in alcun modo elaborati in paesi terzi.

---

[23] Cfr. articolo 30 del RGPD, in particolare il paragrafo 1, lettera e), e il paragrafo 2, lettera c). Inoltre, i vostri registri di trattamento devono contenere una descrizione delle vostre attività di trattamento, comprese, tra l'altro, le categorie di persone interessate, le categorie di dati personali, le finalità del trattamento e informazioni specifiche sui trasferimenti di dati. Alcuni titolari del trattamento e responsabili del trattamento sono esonerati dall'obbligo di tenere i registri del trattamento (articolo 30, paragrafo 5, del RGPD). Per indicazioni su tale esenzione, si veda il documento di sintesi del Gruppo di lavoro «Articolo 29» per la tutela dei dati sulle deroghe all'obbligo di tenere la documentazione delle attività di trattamento ai sensi dell'articolo 30, paragrafo 5, del RGPD (approvati dall'EDPB il 25 maggio 2018).

[24] In base alle regole di trasparenza del RGPD, dovete informare gli interessati dei trasferimenti di dati personali verso paesi terzi (articolo 13, paragrafo 1, lettera f), e articolo 14, paragrafo 1, lettera f), del RGPD). In particolare, dovete informarli dell'esistenza o dell'assenza di una decisione di adeguatezza da parte della Commissione europea o, nel caso di trasferimenti di cui agli articoli 46 o 47 del RGPD, o al secondo comma dell'articolo 49, paragrafo 1, del RGPD, fare riferimento alle garanzie adeguate e ai mezzi con cui ottenerne una copia o dove sono stati resi disponibili. Le informazioni fornite all'interessato devono essere corrette e aggiornate, soprattutto alla luce della giurisprudenza della Corte in materia di trasferimenti.

[25] Qualora il titolare del trattamento abbia rilasciato la previa autorizzazione scritta, specifica o generale, ai sensi dell'articolo 28, paragrafo 2, del RGPD.

[26] Articolo 5, paragrafo 1, lettera c), del RGPD.

[27] Cfr. la FAQ n. 11 «*si tenga presente che anche fornire accesso ai dati da un paese terzo, ad esempio per finalità amministrative, costituisce un trasferimento*», domande più frequenti dell'EDPB in merito alla sentenza della Corte di giustizia dell'Unione europea nella causa C-311/18 – *Data Protection Commissioner contro Facebook Ireland Ltd e Maximillian Schrems*, 23 luglio 2020.

2.2 Secondo passo: individuare gli strumenti di trasferimento su cui fate affidamento

14. Un secondo passo da compiere consiste nell'individuare gli strumenti di trasferimento su cui fare affidamento tra quelli elencati e previsti nel capo V del RGPD.

Decisioni di adeguatezza

15. La Commissione europea può riconoscere, attraverso **decisioni di adeguatezza** relative ad alcuni o a tutti i paesi terzi verso i quali trasferite i dati personali, che essi offrono un adeguato livello di protezione dei dati personali[28].

16. L'effetto di una tale decisione di adeguatezza è che i dati personali possono circolare dal SEE verso quel paese terzo senza che sia necessario uno strumento di trasferimento ai sensi dell'articolo 46 del RGPD.

17. Le decisioni di adeguatezza possono riguardare un paese nel suo insieme o essere limitate a una parte di esso. Esse possono inoltre riguardare tutti i trasferimenti di dati verso un paese o essere limitate ad alcuni tipi di trasferimenti (ad esempio in un settore)[29].

18. La Commissione europea pubblica l'elenco delle decisioni di adeguatezza sul suo sito web[30].

19. Se trasferite dati personali verso paesi terzi, regioni o settori cui si riferisce una decisione di adeguatezza della Commissione (nella misura in cui sia applicabile), **non dovete adottare ulteriori misure come descritto nelle presenti raccomandazioni[31].** Tuttavia, dovete comunque controllare se le decisioni di adeguatezza pertinenti per detti trasferimenti sono revocate o invalidate[32].

20. Tuttavia, le decisioni di adeguatezza non impediscono agli interessati di presentare un reclamo, né impediscono alle autorità di controllo di adire un giudice nazionale in caso di dubbi sulla validità di una decisione, affinché il giudice nazionale possa adire la CGUE per l'esame di tale validità[33].

---

[28] La Commissione europea ha il potere di determinare, sulla base dell'articolo 45 del RGPD, se un paese al di fuori dell'UE offre un livello adeguato di protezione dei dati. Analogamente, la Commissione europea ha il potere di stabilire se un'organizzazione internazionale offre un livello di protezione adeguato.

[29] Articolo 45, paragrafo 1, del RGPD.

[30] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[31] A condizione che voi e l'importatore di dati abbiate attuato misure volte a rispettare gli altri obblighi previsti dal RGPD; in caso contrario, attuate tali misure.

[32] La Commissione europea deve riesaminare periodicamente tutte le decisioni di adeguatezza e controllare se i paesi terzi che ne beneficiano continuano a garantire un livello di protezione adeguato (cfr. articolo 45, paragrafi 3 e 4, del RGPD). Inoltre, la CGUE può invalidare le decisioni di adeguatezza [cfr. le sentenze nelle cause C-362/14 (Schrems I) e C-311/18 (Schrems II)].

[33] C-311/18 (Schrems II), paragrafi 118-120. Le autorità di controllo non possono ignorare la decisione di adeguatezza e sospendere o vietare i trasferimenti di dati personali verso tali paesi citando solo l'inadeguatezza del livello di protezione. Esse possono esercitare il loro potere di sospendere o vietare i trasferimenti di dati personali verso tale paese terzo solo per altri motivi (ad esempio, misure di sicurezza insufficienti in violazione dell'articolo 32 del RGPD, o nessuna base giuridica valida per il trattamento dei dati in quanto tale in violazione dell'articolo 6 del RGPD). Le autorità di controllo possono esaminare, in piena indipendenza, se il trasferimento di tali dati è conforme ai requisiti stabiliti dal RGPD e, se del caso, proporre un ricorso dinanzi al giudice nazionale affinché, in caso di dubbi sulla validità della decisione di adeguatezza della Commissione, sia presentata alla Corte di giustizia una domanda di pronuncia pregiudiziale ai fini dell'esame della validità.

Esempio: Un cittadino dell'UE, il sig. Schrems, ha presentato una denuncia nel giugno 2013 presso la Commissione irlandese per la protezione dei dati (DPC) e ha chiesto a tale autorità di controllo di vietare o sospendere il trasferimento dei suoi dati personali da Facebook Ireland agli Stati Uniti, in quanto riteneva che la legge e la prassi degli Stati Uniti non garantissero una protezione adeguata dei dati personali detenuti nel loro territorio rispetto alle attività di controllo che vi erano svolte dalle autorità pubbliche. La DPC ha respinto la denuncia a motivo del fatto, in particolare, che nella decisione 2000/520 la Commissione europea aveva ritenuto che, nell'ambito del regime dell'approdo sicuro, gli Stati Uniti garantissero un livello adeguato di protezione dei dati personali trasferiti (decisione sull'approdo sicuro). Il sig. Schrems ha impugnato la decisione della DPC e la Corte d'appello irlandese ha sottoposto alla Corte di giustizia dell'Unione europea (CGUE) un quesito sulla validità della decisione 2000/520. La CGUE ha successivamente deciso di invalidare la decisione 2000/520 della Commissione sull'adeguatezza della protezione fornita dai principi di approdo sicuro in materia di riservatezza[34].

Articolo 46 del RGPD – Strumenti di trasferimento

21. L'articolo 46 del RGPD elenca una serie di strumenti di trasferimento contenenti «*garanzie adeguate*» che gli esportatori possono utilizzare per trasferire dati personali verso paesi terzi in assenza di decisioni di adeguatezza. I principali tipi di strumenti di trasferimento di cui all'articolo 46 del RGPD sono:

    - le clausole contrattuali tipo di protezione dei dati;
    - le norme vincolanti d'impresa;
    - i codici di condotta;
    - i meccanismi di certificazione;
    - clausole contrattuali ad hoc.

22. Qualunque sia lo strumento di trasferimento di cui all'articolo 46 del RGPD che si sceglie di adottare, è necessario garantire che, nel complesso, i dati personali trasferiti godano di un livello di protezione sostanzialmente equivalente.

23. Gli strumenti di trasferimento di cui all'articolo 46 del RGPD contengono principalmente garanzie adeguate di natura contrattuale che possono essere applicate ai trasferimenti verso tutti i paesi terzi. La situazione nel paese terzo verso il quale sono trasferiti i dati può comunque richiedere di integrare questi strumenti di trasferimento e le garanzie in essi contenute con misure integrative («misure supplementari») volte a garantire un livello di protezione sostanzialmente equivalente[35].

Deroghe

24. Oltre alle decisioni di adeguatezza e agli strumenti di trasferimento di cui all'articolo 46 del RGPD, quest'ultimo contiene una terza via che consente il trasferimento di dati personali in determinate situazioni. A determinate condizioni specifiche, potreste comunque riuscire a trasferire dati personali in base a una delle deroghe elencate all'articolo 49 del RGPD.

[34] Causa C-362/14 (Schrems I).
[35] C-311/18 (Schrems II), paragrafi 130 e 133. Vedere anche il punto 2.3 in appresso.

25. Tale articolo ha carattere eccezionale e le deroghe in esso incluse devono essere interpretate in modo restrittivo e correlarsi principalmente alle attività di trattamento che presentano carattere occasionale e non ripetitivo. L'EDPB ha emanato le linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679. [36]

26. Prima di fare affidamento su una deroga di cui all'articolo 49 del RGPD dovete verificare se il trasferimento soddisfa le rigorose condizioni previste da questa disposizione per ciascuna di esse.

***

27. Se il vostro trasferimento non ha base giuridica né in una decisione di adeguatezza, né in una deroga di cui all'articolo 49, dovete continuare con il terzo passo.

2.3 Terzo passo: valutare se lo strumento di trasferimento di cui all'articolo 46 del RGPD su cui si fa affidamento è efficace alla luce di tutte le circostanze del trasferimento

28. Selezionare uno strumento di trasferimento di cui all'articolo 46 del RGPD potrebbe non essere sufficiente. Lo strumento di trasferimento deve garantire che il livello di protezione assicurato dal RGPD non sia pregiudicato dal trasferimento[37]. In altre parole, lo strumento di trasferimento adottato deve essere efficace nella pratica.

29. Efficace significa che i dati personali trasferiti godono nel paese terzo di un livello di protezione sostanzialmente equivalente a quello garantito nel SEE[38]. Ciò non avviene se l'importatore di dati non è in grado di adempiere agli obblighi previsti dallo strumento di trasferimento prescelto ai sensi dell'articolo 46 del RGPD a causa della legislazione e delle prassi del paese terzo applicabili al trasferimento.

30. Di conseguenza è necessario valutare, se del caso in collaborazione con l'importatore, se vi sia qualcosa nella legge o nella prassi del paese terzo che possa incidere sull'efficacia delle garanzie adeguate dello strumento di trasferimento di cui all'articolo 46 del RGPD su cui si fa affidamento, nel contesto dello specifico trasferimento. Se del caso, l'importatore di dati dovrebbe fornirvi le fonti e le informazioni pertinenti relative al paese terzo in cui è stabilito e alle leggi applicabili al trasferimento. È anche possibile fare riferimento ad altre fonti di informazione, come quelle elencate in modo non esaustivo nell'allegato 3[39].

31. La valutazione deve prendere in considerazione tutti gli attori che partecipano al trasferimento (ad esempio, titolari del trattamento, responsabili del trattamento a vari livelli che trattano i dati nel paese terzo), così come sono stati individuati nell'esercizio di mappatura dei trasferimenti. Più sono i titolari del trattamento, i responsabili del trattamento o gli importatori coinvolti, più complessa sarà la valutazione, nella quale occorre anche tener conto di eventuali trasferimenti successivi.

32. A tal fine, occorre esaminare le caratteristiche di ciascun trasferimento e determinare in che modo l'ordinamento giuridico nazionale del paese verso cui i dati vengono trasferiti (o successivamente trasferiti) si applica a tali trasferimenti.

---

[36] Per ulteriori indicazioni in merito cfr. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_it.
[37] Articolo 44 del RGPD.
[38] C-311/18 (Schrems II), paragrafi 105 e seconda conclusione.
[39] Si veda anche il paragrafo 43 infra.

33. Il contesto giuridico applicabile dipenderà dalle circostanze del trasferimento, in particolare da:

- finalità per le quali i dati vengono trasferiti ed elaborati (ad esempio marketing, risorse umane, archiviazione, supporto informatico, test clinici);
- tipi di entità coinvolte nel trattamento (pubblica/privata; titolare del trattamento/responsabile del trattamento);
- settore in cui avviene il trasferimento (ad esempio adtech, telecomunicazioni, finanziario, ecc.);
- categorie di dati personali trasferiti (ad esempio i dati personali che si riferiscono a minori possono rientrare nell'ambito di applicazione di una legislazione specifica del paese terzo);
- se i dati saranno conservati nel paese terzo o se vi è solo un accesso remoto ai dati conservati all'interno dell'UE/SEE;
- formato dei dati da trasferire (ad esempio in testo semplice/pseudonimizzati o cifrati)[40];
- possibilità che i dati siano soggetti a trasferimenti successivi dal paese terzo verso un altro paese terzo[41].

34. Tra le leggi applicabili, dovrete valutare se vi sia un'eventuale ingerenza con gli impegni previsti dallo strumento di trasferimento di cui all'articolo 46 RGPD che avete scelto. Dovreste verificare che gli impegni che consentono agli interessati di esercitare i loro diritti nell'ambito dei trasferimenti internazionali (quali le richieste di accesso, rettifica e cancellazione dei dati trasferiti) possano essere effettivamente applicati nella pratica e non siano ostacolati dalla legge del paese terzo di destinazione.

35. Dovrete valutare le norme pertinenti di carattere generale nella misura in cui hanno un impatto sull'effettiva applicazione delle garanzie contenute nello strumento di trasferimento di cui all'articolo 46 del RGPD e sui diritti fondamentali delle persone (in particolare, il diritto di ricorso concesso all'interessato in caso di accesso ai dati trasferiti da parte di autorità pubbliche di paesi terzi).

36. Dovreste in ogni caso prestare particolare attenzione a tutte le leggi pertinenti, in particolare quelle che stabiliscono i requisiti per la divulgazione dei dati personali alle autorità pubbliche o che conferiscono a tali autorità poteri di accesso ai dati personali (ad esempio per l'applicazione del diritto penale, per la vigilanza regolamentare e per scopi di sicurezza nazionale). Se tali requisiti o poteri sono limitati a quanto necessario e proporzionato in una società democratica[42], non possono pregiudicare gli impegni previsti dallo strumento di trasferimento di cui all'articolo 46 del RGPD su si fa affidamento.

37. Le norme dell'Unione, quali gli articoli 47 e 52 della Carta dei diritti fondamentali dell'Unione europea, devono essere utilizzate come riferimento per valutare se tale accesso da parte delle autorità pubbliche è limitato a quanto necessario e proporzionato in una società democratica e se agli interessati è consentito un ricorso effettivo.

38. Nell'effettuare tale valutazione, sono pertinenti anche diversi aspetti dell'ordinamento giuridico di tale paese terzo, ad esempio gli elementi elencati all'articolo 45, paragrafo 2, del RGPD[43]. Ad esempio, la

[40] Alcuni paesi terzi non consentono l'importazione di dati cifrati.
[41] Qualora il titolare del trattamento abbia rilasciato la previa autorizzazione scritta, specifica o generale, ai sensi dell'articolo 28, paragrafo 2, del RGPD.
[42] Si vedano gli articoli 47 e 52 della Carta dei diritti fondamentali dell'Unione europea, l'articolo 23, paragrafo 1, del RGPD e le raccomandazioni 02/2020 dell'EDPB, del 10 novembre 2020, relative alle garanzie essenziali europee per le misure di sorveglianza, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.
[43] C-311/18 (Schrems II), paragrafo 104.

situazione dello stato di diritto in un paese terzo può essere pertinente per valutare l'efficacia dei meccanismi disponibili per ottenere un ricorso (in sede giudiziale) contro l'accesso illegale ai dati personali da parte del governo. L'esistenza di una legge completa sulla protezione dei dati o di un'autorità indipendente per la protezione dei dati, nonché il rispetto degli strumenti internazionali che prevedono garanzie di protezione dei dati, possono contribuire a garantire la proporzionalità dell'ingerenza del governo[44].

***

39. Le raccomandazioni dell'EDPB relative alle garanzie essenziali europee forniscono elementi che devono essere valutati per determinare se il quadro giuridico che disciplina l'accesso ai dati personali da parte delle autorità pubbliche in un paese terzo, siano esse agenzie di sicurezza nazionale o autorità incaricate dell'applicazione della legge, possa essere considerato un'ingerenza giustificabile (e quindi non in contrasto con gli impegni assunti con lo strumento di trasferimento di cui all'articolo 46 del RGPD) oppure no. In particolare, occorre considerare attentamente questo aspetto quando la legislazione che disciplina l'accesso ai dati da parte delle autorità pubbliche è ambigua o non è disponibile al pubblico.

40. Applicata alla situazione dei trasferimenti di dati basati sugli strumenti di trasferimento di cui all'articolo 46, le raccomandazioni dell'EDPB relative alle garanzie essenziali europee possono guidare l'esportatore e l'importatore di dati nel valutare se tali poteri interferiscono in modo ingiustificato con gli obblighi dell'importatore di garantire la sostanziale equivalenza.

41. La mancanza di un livello di protezione sostanzialmente equivalente sarà particolarmente evidente laddove la legislazione o la prassi del paese terzo interessato dal trasferimento non soddisfino i requisiti delle garanzie essenziali europee.

42. La vostra valutazione deve basarsi innanzitutto sulla legislazione disponibile al pubblico. Tuttavia, in alcune situazioni ciò non sarà sufficiente perché la legislazione dei paesi terzi potrebbe essere carente. In tal caso, se desiderate comunque procedere con il trasferimento, dovreste esaminare altri fattori pertinenti e oggettivi[45] e non basarvi su fattori soggettivi, come la probabilità che le autorità pubbliche accedano ai vostri dati in modo non conforme agli standard dell'Unione. Dovreste condurre questa valutazione con la dovuta diligenza e documentarla accuratamente, in quanto sarete ritenuti responsabili della decisione che potrete prendere su tale base[46].

43. Potete completare la vostra valutazione con informazioni ottenute da altre fonti[47], come ad esempio:

    - elementi che dimostrino che un'autorità di un paese terzo cercherà di accedere ai dati, indipendentemente dal fatto che tale accesso sia effettuato con la consapevolezza dell'importatore, alla luce della legislazione, della prassi e dei precedenti segnalati;
    - elementi che dimostrino che un'autorità di un paese terzo sarà in grado di accedere ai dati attraverso l'importatore di dati o attraverso l'intercettazione diretta del canale di

[44] Ad esempio, la convenzione n. 108 (Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, STE n. 108) o la convenzione n. 108+ (Convenzione aggiornata sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, STCE n. 223) forniscono mezzi di ricorso in sede giudiziale internazionali applicabili in caso di violazioni della protezione dei dati e contribuiscono a garantire un livello minimo di protezione dei dati personali e il rispetto della vita privata.
[45] Si veda il paragrafo 43 in appresso e l'allegato 3.
[46] Articolo 5, paragrafo 2, del RGPD.
[47] Cfr. anche l'allegato 3.

comunicazione alla luce dei precedenti segnalati, dei poteri giuridici e delle risorse tecniche, finanziarie e umane a sua disposizione.

44. La vostra valutazione può in ultima analisi rivelare che lo strumento di trasferimento dell'articolo 46 del RGPD su cui fate affidamento e le opportune salvaguardie in esso contenute:

- garantisce in modo efficace che i dati personali trasferiti godono nel paese terzo di un livello di protezione sostanzialmente equivalente a quello garantito all'interno del SEE. La legislazione e le prassi del paese terzo applicabili al trasferimento mettono l'importatore di dati in grado di rispettare gli obblighi previsti dallo strumento di trasferimento scelto. Dovreste procedere a una nuova valutazione a intervalli adeguati o quando emergono cambiamenti significativi (cfr. sesto passo);
- non garantisce in modo efficace un livello di protezione sostanzialmente equivalente. L'importatore di dati non può adempiere ai suoi obblighi a causa della legislazione e/o delle prassi del paese terzo applicabili al trasferimento. La CGUE ha sottolineato che, qualora gli strumenti di trasferimento di cui all'articolo 46 del RGPD non siano sufficienti, spetta all'esportatore di dati mettere in atto misure supplementari efficaci o non trasferire i dati personali[48].

La CGUE ha ritenuto, ad esempio, che l'articolo 702 del Foreign Intelligence Surveillance Act (FISA) statunitense non rispetta le garanzie minime derivanti dal principio di proporzionalità ai sensi del diritto dell'Unione e non può essere considerato limitato allo stretto necessario. Ciò significa che il livello di protezione dei programmi autorizzati dall'articolo 702 della FISA non è sostanzialmente equivalente alle garanzie richieste dal diritto dell'Unione. Di conseguenza, se l'importatore di dati o qualsiasi altro destinatario al quale l'importatore può comunicare i dati rientra nell'ambito di applicazione di detto articolo[49], si può fare affidamento per tale trasferimento sulle clausole contrattuali tipo o su altri strumenti di trasferimento di cui all'articolo 46 del RGPD solo se ulteriori misure tecniche supplementari rendono impossibile o inefficace l'accesso ai dati trasferiti.

2.4 Quarto passo: adottare misure supplementari

45. Se la valutazione di cui al terzo passo ha rivelato che lo strumento di trasferimento di cui all'articolo 46 del RGPD scelto non è efficace, dovrete considerare, se del caso in collaborazione con l'importatore, l'eventuale esistenza di misure supplementari che, aggiunte alle garanzie contenute negli strumenti di trasferimento, potrebbero garantire che i dati trasferiti godano nel paese terzo di un livello di

[48] CGUE C-311/18 (Schrems II), paragrafi 134-135.

[49] L'articolo 702 della FISA si applica se i dati sono ottenuti «da o con l'aiuto di un fornitore di servizi di comunicazione elettronica» [articolo 702 FISA = titolo 50 dello United States Code (U.S.C.) § 1881 bis, lettera h), paragrafo 2, lettera A), punto vi)], che a sua volta è definito nel titolo 50 U.S.C. § 1881, lettera b), paragrafo 4), come
«A) un vettore di telecomunicazioni, secondo la definizione del termine di cui all'articolo 153 del titolo 47;
B) un fornitore di servizi di comunicazione elettronica, secondo la definizione del termine di cui all'articolo 2510 del titolo 18;
C) un fornitore di servizi di calcolo a distanza, secondo la definizione del termine di cui all'articolo 2711 del titolo 18;
D) qualsiasi altro fornitore di servizi di comunicazione che abbia accesso a comunicazioni via cavo o elettroniche, sia come comunicazioni trasmesse sia come comunicazioni memorizzate; o
E) un funzionario, dipendente o agente di un'entità descritta alle lettere A), B), C) o D)».

protezione sostanzialmente equivalente a quello garantito all'interno dell'UE[50]. Le «misure supplementari» integrano per definizione le garanzie già previste dallo strumento di trasferimento di cui all'articolo 46 del RGPD[51].

46. Dovete individuare caso per caso quali misure supplementari potrebbero essere efficaci per una serie di trasferimenti verso un determinato paese terzo quando utilizzate uno specifico strumento di trasferimento di cui all'articolo 46 del RGDP. Potrete basarvi sulle vostre precedenti valutazioni di cui al primo, secondo e terzo passo e verificare, sulla base di quelle conclusioni, la potenziale efficacia delle misure supplementari nel garantire il livello di protezione richiesto.

47. In linea di principio, le misure supplementari possono avere carattere contrattuale, tecnico o organizzativo. La combinazione di misure diverse in modo che si sostengano e si basino l'una sull'altra può migliorare il livello di protezione e può quindi contribuire a raggiungere gli standard dell'Unione.

48. Le misure contrattuali e organizzative, da sole, non riescono in genere a evitare l'accesso ai dati personali da parte delle autorità pubbliche del paese terzo (qualora ciò interferisca ingiustificatamente con gli obblighi dell'importatore di dati di garantire la sostanziale equivalenza). Vi saranno infatti situazioni in cui solo misure tecniche potrebbero impedire o rendere inefficace l'accesso ai dati personali da parte delle autorità pubbliche dei paesi terzi, in particolare a fini di sorveglianza[52]. In tali situazioni, le misure contrattuali o organizzative possono integrare le misure tecniche e rafforzare il livello generale di protezione dei dati, ad esempio creando ostacoli ai tentativi delle autorità pubbliche di accedere ai dati in modo non conforme alle norme dell'Unione.

49. In collaborazione con l'importatore di dati, se del caso, potete consultare il seguente elenco (non esaustivo) di fattori per individuare quali misure supplementari sarebbero più efficaci per proteggere i dati trasferiti:

    - formato dei dati da trasferire (ad esempio in testo semplice/pseudonimizzati o cifrati);
    - natura dei dati;
    - lunghezza e complessità del flusso di lavoro del trattamento dei dati, numero di attori coinvolti nel trattamento e rapporto esistente tra loro, [ad esempio se i trasferimenti coinvolgono più titolari del trattamento o sia titolari che responsabili del trattamento, oppure se sono coinvolti responsabili del trattamento che trasferiranno i dati da voi all'importatore dei vostri dati (considerando le relative disposizioni applicabili ad essi ai sensi della legislazione del paese terzo di destinazione][53];

[50] C-311/18 (Schrems II), paragrafo 96.
[51] Considerando 109 del RGPD e C-311/18 (Schrems II), paragrafo 133.
[52] Qualora tale accesso vada al di là di quanto necessario e proporzionato in una società democratica; cfr. gli articoli 47 e 52 della Carta dei diritti fondamentali dell'Unione europea, l'articolo 23, paragrafo 1, del RGPD e le raccomandazioni 02/2020 dell'EDPB, del 10 novembre 2020, relative alle garanzie essenziali europee per le misure di sorveglianza, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.
[53] Il RGPD assegna obblighi distinti ai titolari del trattamento e ai responsabili del trattamento. I trasferimenti possono essere da titolare del trattamento a titolare del trattamento, tra titolari del trattamento congiunti, da titolare del trattamento a responsabile del trattamento e, previa autorizzazione del titolare del trattamento, da responsabile del trattamento a titolare del trattamento o da responsabile del trattamento a responsabile del trattamento.

- possibilità che i dati siano oggetto di trasferimenti successivi, all'interno dello stesso paese terzo o anche verso altri paesi terzi (ad esempio coinvolgimento di responsabili del trattamento a vari livelli dell'importatore dei dati)[54].

Esempi di misure supplementari

50. Alcuni esempi di misure tecniche, contrattuali e organizzative che potrebbero essere prese in considerazione si possono trovare negli elenchi non esaustivi di cui all'allegato 2.

***

51. Se avete messo in atto misure supplementari efficaci, che, combinate con lo strumento di trasferimento di cui all'articolo 46 del RGPD prescelto, raggiungono un livello di protezione sostanzialmente equivalente al livello di protezione garantito all'interno del SEE, i vostri trasferimenti possono procedere.

52. Qualora non siate in grado di trovare o attuare misure supplementari efficaci che garantiscano che i dati personali trasferiti godano di un livello di protezione sostanzialmente equivalente[55], non dovete iniziare a trasferire i dati personali al paese terzo interessato sulla base dello strumento di trasferimento di cui all'articolo 46 del RGPD su cui fate affidamento. Se state già effettuando trasferimenti, siete tenuti a sospendere o a porre fine al trasferimento dei dati personali[56] . In conformità alle garanzie previste dallo strumento di trasferimento di cui all'articolo 46 del RGPD su cui fate affidamento, i dati che avete già trasferito a tale paese terzo e le relative copie devono esservi restituiti o distrutti interamente dall'importatore[57].

Esempio: la legge del paese terzo vieta le misure supplementari da voi individuate (ad esempio vieta l'uso della cifratura) o ne impedisce in altro modo l'efficacia. Non dovete iniziare a trasferire i dati personali verso questo paese, oppure dovete interrompere i trasferimenti in corso verso questo paese.

53. Se decidete di continuare il trasferimento nonostante il fatto che l'importatore non sia in grado di rispettare gli impegni assunti con lo strumento di trasferimento di cui all'articolo 46 del RGPD, dovreste informare l'autorità di controllo competente in conformità alle disposizioni specifiche previste dallo strumento di trasferimento di cui all'articolo 46 RGPD pertinente[58]. L'autorità di controllo competente sospenderà o vieterà il trasferimento dei dati nei casi in cui ritenga che non possa essere garantito un livello di protezione sostanzialmente equivalente[59].

[54] Cfr. nota 25.

[55] Qualora tale accesso vada al di là di quanto necessario e proporzionato in una società democratica; cfr. gli articoli 47 e 52 della Carta dei diritti fondamentali dell'Unione europea, l'articolo 23, paragrafo 1, del RGPD e le raccomandazioni 02/2020 dell'EDPB, del 10 novembre 2020, relative alle garanzie essenziali europee per le misure di sorveglianza, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

[56] C-311/18 (Schrems II), paragrafo 135.

[57] Cfr. la clausola 12 nell'allegato alla decisione 87/2010 sulle clausole contrattuali tipo; cfr. la clausola di risoluzione extra (facoltativa) nell'allegato B della decisione 2004/915/CE sulle clausole contrattuali tipo.

[58] Cfr. le domande più frequenti in merito alla sentenza della Corte di giustizia dell'Unione europea nella causa C-311/18 – Data Protection Commissioner contro Facebook Ireland Ltd e Maximillian Schrems, adottate dall'EDPB il 23 luglio 2020, in particolare le domande 5, 6 e 9. Cfr. anche la clausola 4, lettera g), della decisione 2010/87/UE della Commissione; la clausola 5, lettera a) della decisione 2001/497/CE della Commissione e la clausola II, lettera c), dell'insieme II dell'allegato della decisione 2004/915/CE della Commissione.

[59] C-311/18 (Schrems II), paragrafi 113 e 121.

54. L'autorità di controllo competente può imporre eventuali altre misure correttive (ad esempio una sanzione) se avviate o continuate il trasferimento sebbene non possiate dimostrare un livello di protezione sostanzialmente equivalente nel paese terzo.

2.5 Quinto passo: passaggi procedurali se avete individuato misure supplementari efficaci

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

2.5.1 Clausole tipo di protezione dei dati (articolo 46, paragrafo 2, lettere c) e d), del RGPD)

56. Quando intendete mettere in atto misure supplementari in aggiunta alle clausole contrattuali tipo, non è necessario richiedere un'autorizzazione all'autorità di controllo competente per aggiungere questo tipo di clausole o garanzie supplementari, a condizione che le misure supplementari individuate non contraddicano, direttamente o indirettamente, le clausole contrattuali tipo e siano sufficienti a garantire che il livello di protezione previsto dal RGPD non sia pregiudicato[60]. L'esportatore e l'importatore di dati devono garantire che le clausole aggiuntive non possano essere interpretate in alcun modo per limitare i diritti e gli obblighi previsti dalle clausole contrattuali tipo o in qualsiasi altro modo per abbassare il livello di protezione dei dati. Dovete essere in grado di dimostrare ciò, compresa l'univocità di tutte le clausole, secondo il principio di responsabilizzazione e l'obbligo di fornire un livello sufficiente di protezione dei dati. Le autorità di controllo competenti hanno il potere di rivedere tali clausole supplementari se necessario (ad esempio in caso di reclamo o di indagine di propria iniziativa).

57. Qualora intendiate modificare le clausole tipo di protezione dei dati o qualora le misure supplementari aggiunte «contraddicano» direttamente o indirettamente le clausole contrattuali tipo, non siete più tenuti a farvi affidamento[61] e dovete chiedere un'autorizzazione all'autorità di controllo competente ai sensi dell'articolo 46, paragrafo 3, lettera a), del RGPD.

---

[60] Il considerando 109 del RGPD recita: «La possibilità che il titolare del trattamento o il responsabile del trattamento utilizzi clausole tipo di protezione dei dati adottate dalla Commissione o da un'autorità di controllo non dovrebbe precludere ai titolari del trattamento o ai responsabili del trattamento la possibilità di includere tali clausole tipo in un contratto più ampio, anche in un contratto tra il responsabile del trattamento e un altro responsabile del trattamento, né di aggiungere altre clausole o garanzie supplementari, purché non contraddicano, direttamente o indirettamente, le clausole contrattuali tipo adottate dalla Commissione o da un'autorità di controllo o ledano i diritti o le libertà fondamentali degli interessati. I titolari del trattamento e i responsabili del trattamento dovrebbero essere incoraggiati a fornire garanzie supplementari attraverso impegni contrattuali che integrino le clausole tipo di protezione». Disposizioni simili sono previste negli insiemi di clausole contrattuali tipo adottate dalla Commissione europea ai sensi della direttiva 95/45/CE.

[61] Si veda, per analogia, il parere 17/2020 dell'EDPB sul progetto di clausole contrattuali tipo presentato dall'autorità di controllo slovena (articolo 28, paragrafo 8, del RGPD) in merito a clausole contrattuali tipo ai sensi dell'art. 28 già adottate che contengono una disposizione analoga («In aggiunta, il comitato ricorda che la possibilità di usufruire delle clausole contrattuali tipo adottate da un'autorità di controllo non impedisce alle parti di aggiungere altre clausole o salvaguardie supplementari, a condizione che esse non contraddicano, direttamente o indirettamente, le clausole contrattuali tipo adottate né pregiudichino i diritti o le libertà fondamentali degli interessati. Inoltre, in caso di modifica alle clausole contrattuali tipo sulla protezione dei dati, non si riterrà più che le parti abbiano dato esecuzione alle clausole contrattuali tipo adottate»), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_it.pdf.

2.5.2 Norme vincolanti d'impresa (articolo 46, paragrafo 2, lettera b), del RGPD)

58. Il ragionamento della sentenza Schrems II si applica anche ad altri strumenti di trasferimento di cui all'articolo 46, paragrafo 2, del RGPD, poiché tutti questi strumenti sono fondamentalmente di natura contrattuale, per cui le garanzie previste e gli impegni assunti dalle parti non possono vincolare le autorità pubbliche di paesi terzi[62].

59. La sentenza Schrems II è rilevante per i trasferimenti di dati personali sulla base di norme vincolanti d'impresa, poiché le leggi di paesi terzi possono influire sulla protezione fornita da tali strumenti. L'impatto preciso della sentenza Schrems II sulle norme vincolanti d'impresa è ancora oggetto di discussione. L'EDPB fornirà al più presto, nei criteri di riferimento ai sensi di WP 256/257, maggiori dettagli sull'eventuale necessità di includere nelle norme vincolanti d'impresa eventuali impegni aggiuntivi[63].

60. La Corte ha sottolineato che è responsabilità dell'esportatore e dell'importatore dei dati verificare il rispetto, nel paese terzo interessato, del livello di protezione richiesto dal diritto dell'Unione, al fine di determinare se le garanzie previste dalle clausole contrattuali tipo o dalle norme vincolanti d'impresa possano essere rispettate nella pratica. In caso contrario, si deve accertare che sia possibile prevedere misure supplementari atte a garantire un livello di protezione sostanzialmente equivalente a quello in vigore nel SEE e che il diritto o la prassi del paese terzo non interferiscano con tali misure supplementari in modo da impedirne l'efficacia.

2.5.3 Clausole contrattuali ad hoc (articolo 46, paragrafo 3, lettera a), del RGPD)

61. Il ragionamento della sentenza Schrems II si applica anche ad altri strumenti di trasferimento di cui all'articolo 46, paragrafo 2, del RGPD, poiché tutti questi strumenti sono fondamentalmente di natura contrattuale, per cui le garanzie previste e gli impegni assunti dalle parti non possono vincolare le autorità pubbliche di paesi terzi[64]. La sentenza Schrems II è dunque rilevante per i trasferimenti di dati personali sulla base di clausole contrattuali ad hoc, poiché le leggi di paesi terzi possono influire sulla protezione fornita da tali strumenti. L'impatto preciso della sentenza Schrems II sulle clausole contrattuali ad hoc è ancora oggetto di discussione. L'EDPB fornirà quanto prima ulteriori dettagli.

2.6 Sesto passo: rivalutare a intervalli appropriati

62. Dovete monitorare costantemente e, se del caso, in collaborazione con gli importatori di dati, gli sviluppi nel paese terzo verso cui avete trasferito i dati personali che potrebbero influenzare la vostra valutazione iniziale del livello di protezione e le decisioni che potreste aver preso di conseguenza sui vostri trasferimenti. La responsabilizzazione è un obbligo permanente (articolo 5, paragrafo 2, del RGPD).

[62] CGUE, C-311/18 (Schrems II), paragrafo 132.
[63] Gruppo di lavoro Articolo 29 per la protezione dei dati, Documento di lavoro che istituisce una tabella degli elementi e dei principi che devono figurare nelle norme vincolanti d'impresa, versione emendata e adottata da ultimo il 6 febbraio 2018, WP 256 rev.01; Gruppo di lavoro Articolo 29 per la protezione dei dati, Documento di lavoro che istituisce una tabella degli elementi e dei principi che devono figurare nelle norme vincolanti d'impresa per i responsabili del trattamento, versione emendata e adottata da ultimo il 6 febbraio 2018, WP 257 rev.01.
[64] CGUE, C-311/18 (Schrems II), paragrafo 132.

63. Dovreste mettere in atto meccanismi sufficientemente solidi per garantire la sospensione o la cessazione immediata dei trasferimenti qualora:

- l'importatore abbia violato o non sia in grado di onorare gli impegni assunti con lo strumento di trasferimento di cui all'articolo 46 del RGPD; oppure
- le misure supplementari non siano più efficaci in tale paese terzo.

3 CONCLUSIONI

64. Il RGPD stabilisce norme sul trattamento dei dati personali nel SEE e, in tal modo, consente la libera circolazione dei dati personali all'interno del SEE. Il capo V del regolamento disciplina i trasferimenti di dati personali verso paesi terzi e fissa un limite elevato: il trasferimento non deve pregiudicare il livello di protezione delle persone fisiche garantito dal RGPD (articolo 44 del RGPD). La sentenza C-311/18 (Schrems II) della CGUE sottolinea la necessità di garantire la continuità del livello di protezione garantito dal RGPD ai dati personali trasferiti verso un paese terzo[65].

65. Per garantire un livello di protezione sostanzialmente equivalente dei vostri dati, dovete innanzitutto conoscere a fondo i vostri trasferimenti. Dovete inoltre controllare che i dati trasferiti siano adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per le quali vengono trasferiti e trattati nel paese terzo.

66. Dovete anche individuare lo strumento di trasferimento su cui fate affidamento per i vostri trasferimenti. Se lo strumento di trasferimento non è una decisione di adeguatezza, dovete verificare caso per caso se la legge o la prassi del paese terzo di destinazione pregiudica (oppure no) le garanzie previste dallo strumento di trasferimento di cui all'articolo 46 del RGPD nel contesto dei vostri trasferimenti. Se il solo strumento di trasferimento di cui all'articolo 46 del RGPD non riesce a garantire un livello di protezione sostanzialmente equivalente per i dati personali da voi trasferiti, misure supplementari possono colmare la lacuna.

67. Qualora non siate in grado di trovare o attuare misure supplementari efficaci che garantiscano che i dati personali trasferiti godono di un livello di protezione sostanzialmente equivalente, non dovete iniziare a trasferire i dati personali verso il paese terzo interessato sulla base dello strumento di trasferimento da voi scelto. Se state già effettuando trasferimenti, siete tenuti a sospendere o a porre fine prontamente al trasferimento dei dati personali.

68. L'autorità di controllo competente ha il potere di sospendere o porre fine ai trasferimenti di dati personali verso il paese terzo se non è garantita la protezione dei dati trasferiti richiesta dal diritto dell'Unione, in particolare dagli articoli 45 e 46 del RGPD e dalla Carta dei diritti fondamentali.

Per il comitato europeo per la protezione dei dati

La presidente

(Andrea Jelinek)

[65] C-311/18 (Schrems II), paragrafo 93.

ALLEGATO 1: DEFINIZIONI

- Per «paese terzo» si intende qualsiasi paese che non sia uno Stato membro del SEE.
- Per «SEE» si intende lo Spazio economico europeo, che comprende gli Stati membri dell'Unione europea e l'Islanda, la Norvegia e il Liechtenstein. A questi ultimi si applica il RGPD in virtù dell'accordo SEE, in particolare l'allegato XI e il protocollo 37.
- «RGPD» si riferisce al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
- «La Carta» si riferisce alla Carta dei diritti fondamentali dell'Unione europea (GU C 326 del 26.10.2012, pagg. 391-407).
- «CGUE» o «la Corte» si riferisce alla Corte di giustizia dell'Unione europea, che costituisce l'autorità giudiziaria dell'Unione europea e, in collaborazione con le corti e i tribunali degli Stati membri, garantisce l'applicazione e l'interpretazione uniformi del diritto dell'Unione.
- Per «esportatore di dati» si intende il titolare del trattamento o il responsabile del trattamento all'interno del SEE che trasferisce dati personali a un titolare del trattamento o a un responsabile del trattamento in un paese terzo.
- Per «importatore di dati» si intende il titolare del trattamento o il responsabile del trattamento in un paese terzo che riceve o ottiene accesso ai dati personali trasferiti dal SEE.
- «Strumento di trasferimento di cui all'articolo 46 del RGPD» si riferisce alle garanzie adeguate ai sensi dell'articolo 46 del RGPD che gli esportatori di dati mettono in atto quando trasferiscono dati personali verso un paese terzo, in assenza di una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, del RGPD. L'articolo 46, paragrafi 2 e 3, del RGPD contiene l'elenco degli strumenti di trasferimento di cui all'articolo 46 del RGPD che i titolari del trattamento e i responsabili del trattamento possono utilizzare.
- Per «clausole contrattuali tipo» si intendono le clausole tipo di protezione dei dati adottate dalla Commissione europea per i trasferimenti di dati personali tra titolari del trattamento o responsabili del trattamento nel SEE e titolari del trattamento o responsabili del trattamento al di fuori del SEE. Le clausole contrattuali tipo adottate dalla Commissione europea sono uno strumento di trasferimento ai sensi dell'articolo 46, paragrafo 2, lettera c), e paragrafo 5, del RGPD.

ALLEGATO 2: ESEMPI DI MISURE SUPPLEMENTARI

69. Le seguenti misure sono esempi di misure supplementari che è possibile prendere in considerazione quando arrivate al quarto passo «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 di sostanziale equivalenza richiesti dal diritto dell'Unione. Dovreste selezionare le misure supplementari che possono garantire efficacemente tale livello di protezione per i vostri trasferimenti.

70. Qualsiasi misura supplementare può essere considerata efficace ai sensi della sentenza della CGUE «Schrems II» solo se e nella misura in cui affronta le specifiche carenze individuate nella valutazione della situazione giuridica nel paese terzo. Se, in ultima analisi, non riuscite a garantire un livello di protezione sostanzialmente equivalente, non dovete trasferire i dati personali.

71. In qualità di titolari del trattamento o di responsabili del trattamento, potreste già essere tenuti ad attuare alcune delle misure descritte nel presente allegato, anche se il vostro importatore di dati è coperto da una decisione di adeguatezza, così come potreste essere tenuti ad attuarle quando trattate i dati all'interno del SEE[66].

Misure tecniche

72. Questa sezione descrive in modo non esaustivo esempi di misure tecniche, che possono integrare le garanzie previste dagli strumenti di trasferimento di cui all'articolo 46 del RGPD, per garantire il rispetto del livello di protezione richiesto dal diritto dell'Unione nel contesto di un trasferimento di dati personali verso un paese terzo. Tali misure saranno particolarmente necessarie qualora la legislazione di tale paese imponga all'importatore di dati obblighi che sono in contrasto con le garanzie previste dagli strumenti di trasferimento di cui all'articolo 46 del RGPD e che sono, in particolare, in grado di pregiudicare la garanzia contrattuale di un livello di protezione sostanzialmente equivalente rispetto all'accesso a tali dati da parte delle autorità pubbliche di tale paese terzo[67].

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

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

74. Le misure elencate di seguito sono intese a garantire che l'accesso ai dati trasferiti da parte delle autorità pubbliche di paesi terzi non pregiudichi l'efficacia delle garanzie adeguate previste dagli strumenti di trasferimento di cui all'articolo 46 del RGPD. Tali misure si applicano anche se l'accesso delle autorità pubbliche è conforme alla legge del paese dell'importatore, qualora tale accesso vada al di là di quanto necessario e proporzionato in una società democratica[68]. Tali misure hanno lo scopo di impedire l'accesso potenzialmente illecito impedendo alle autorità di identificare gli interessati, di

[66] Articolo 5, paragrafo 2, del RGPD e articolo 32 del RGPD.
[67] C-311/18 (Schrems II), paragrafo 135.
[68] Si vedano gli articoli 47 e 52 della Carta dei diritti fondamentali dell'Unione europea, l'articolo 23, paragrafo 1, del RGPD e le raccomandazioni dell'EDPB relative alle garanzie essenziali europee per le misure di sorveglianza.

dedurre informazioni che li riguardano, di individuarli in un altro contesto o di associare i dati trasferiti ad altri insiemi di dati in loro possesso che possono contenere, tra gli altri dati, identificatori online forniti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati dagli interessati in altri contesti.

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

a) in transito 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. L'accesso può tuttavia essere anche attivo, nel senso che le autorità pubbliche si interpongono al processo di comunicazione non solo leggendo il contenuto, ma anche manipolando o sopprimendo parti di esso;

b) durante la custodia da parte di un destinatario dei dati, accedendo personalmente alle strutture di trattamento o chiedendo al destinatario dei dati di localizzarli, estrarre i dati di interesse e consegnarli alle autorità.

76. In questa sezione vengono presi in considerazione gli scenari in cui vengono applicate misure efficaci in entrambi i casi. Misure supplementari diverse possono essere applicate ed essere sufficienti in una determinata circostanza di un trasferimento concreto se la legge del paese destinatario prevede un solo tipo di accesso. È quindi necessario che l'esportatore di dati analizzi attentamente, con il supporto 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 titolo 50 U.S.C. § 1881 bis (sezione 702 della FISA) hanno l'obbligo diretto di concedere l'accesso a dati personali importati che sono in loro possesso, custodia o controllo, o di consegnarli. Ciò può estendersi a qualsiasi chiave crittografica necessaria per rendere i dati intelligibili.

77. Gli scenari descrivono circostanze specifiche e le misure adottate. Qualsiasi modifica degli scenari può portare a conclusioni diverse.

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

Caso d'uso 1: conservazione dei dati per il backup e per 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 conservare dati personali, ad esempio a scopo di backup.

Se

1. i dati personali sono trattati con una forte cifratura prima della trasmissione,
2. l'algoritmo di cifratura e la sua parametrizzazione (ad esempio la lunghezza della chiave o la modalità di funzionamento, se applicabili) sono conformi allo stato dell'arte e possono essere

considerati solidi rispetto all'analisi di cifratura effettuata dalle autorità pubbliche del paese destinatario tenendo conto delle risorse e delle capacità tecniche (ad esempio potenza di calcolo per attacchi di forza bruta) a loro disposizione,
3. la forza della cifratura tiene conto del periodo di tempo specifico durante il quale la riservatezza dei dati personali cifrati deve essere preservata,
4. l'algoritmo di cifratura è applicato in modo impeccabile da un software correttamente aggiornato 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, conservate, 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 RGPD, che è garantito un livello di protezione adeguato,

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

Caso d'uso 2: trasferimento di dati pseudonimizzati

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

Se

1. un esportatore di dati trasferisce i dati personali trattati in modo tale che non possano più essere attribuiti a un determinato interessato, né essere utilizzati per individuare l'interessato in un gruppo più ampio, senza l'uso di informazioni aggiuntive[69],
2. tali informazioni aggiuntive sono detenute esclusivamente dall'esportatore di dati e conservate separatamente in uno Stato membro 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 RGPD, che è garantito un livello di protezione adeguato,
3. la divulgazione o l'uso non autorizzato di tali informazioni aggiuntive sono impediti da adeguate misure di sicurezza tecniche e organizzative, si garantisce che l'esportatore di dati mantiene il controllo esclusivo dell'algoritmo o del repository che consente la re-identificazione utilizzando le informazioni aggiuntive, e
4. il titolare del trattamento ha stabilito, mediante un'analisi approfondita dei dati in questione, tenendo conto di ogni informazione in possesso delle autorità pubbliche del paese destinatario, che i dati personali pseudonimizzati non possono essere attribuiti a una persona fisica identificata o identificabile, anche se incrociati con tali informazioni,

l'EDPB ritiene che la pseudonimizzazione eseguita fornisca un'efficace misura supplementare.

[69] In linea con l'articolo 4, paragrafo 5, del RGPD: «"pseudonimizzazione": 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».

81. Si noti che in molte situazioni, fattori specifici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di una persona fisica, la sua ubicazione o la sua interazione con un servizio basato su Internet in determinati momenti[70] possono consentire l'identificazione di tale persona anche se il suo nome, indirizzo o altri identificativi semplici sono omessi.

82. Ciò vale in particolare quando i dati riguardano l'utilizzo di servizi d'informazione (orario di accesso, sequenza delle funzionalità a cui si è avuto accesso, 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 propria giurisdizione, che potranno così disporre di dati relativi all'utilizzo di tali servizi d'informazione da parte della persona o delle persone a cui si rivolgono.

83. Inoltre, dato che l'uso di alcuni servizi d'informazione è pubblico per natura, o lo è la possibilità di essere utilizzati da parte di soggetti che dispongono di notevoli risorse, i titolari del trattamento dovranno prestare particolare attenzione, considerando che le autorità pubbliche nella propria giurisdizione potrebbero essere in possesso di dati sull'uso dei servizi d'informazione da parte di una persona a cui si rivolgono.

Caso d'uso 3: dati cifrati che semplicemente transitano in paesi terzi

84. Un esportatore di dati desidera trasferire dati verso una destinazione riconosciuta come tale da offrire una protezione adeguata ai sensi dell'articolo 45 del RGPD. I dati vengono inoltrati tramite 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 su Internet e possono essere inoltrati geograficamente tramite un paese terzo che non fornisce un livello di protezione sostanzialmente equivalente,
2. viene utilizzata la cifratura del trasporto, per la quale si garantisce che i protocolli di cifratura impiegati sono all'avanguardia e forniscono una protezione efficace contro gli attacchi attivi e passivi con risorse notoriamente a disposizione delle autorità pubbliche del paese terzo,
3. la decifrazione 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 specifiche di protezione all'avanguardia contro gli attacchi attivi e passivi ai trasporti cifrati,
6. nel caso in cui la cifratura del trasporto non fornisca di per sé una sicurezza adeguata a causa di esperienze di vulnerabilità dell'infrastruttura o del software utilizzato, i dati personali vengono anche cifrati end-to-end sul livello dell'applicazione utilizzando metodi di cifratura all'avanguardia,
7. l'algoritmo di cifratura e la sua parametrizzazione (ad esempio la lunghezza della chiave o la modalità di funzionamento, se applicabili) sono conformi allo stato dell'arte e possono essere considerati solidi rispetto all'analisi di cifratura effettuata dalle autorità pubbliche del paese di

[70] Art. 4, paragrafo 1, del RGPD: «"dato personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

transito tenendo conto delle risorse e delle capacità tecniche (ad esempio potenza di calcolo per attacchi di forza bruta) a loro disposizione,
8. la forza della cifratura tiene conto del periodo di tempo specifico durante il quale la riservatezza dei dati personali cifrati deve essere preservata,
9. l'algoritmo di cifratura è applicato in modo impeccabile da un software correttamente aggiornato la cui conformità alle specifiche dell'algoritmo scelto è stata verificata, ad esempio mediante certificazione,
10. è stata esclusa l'esistenza di backdoor (in hardware o software),
11. le chiavi sono gestite in modo affidabile (generate, amministrate, conservate, se del caso, collegate all'identità del destinatario previsto, e revocate), dall'esportatore o da un entità di fiducia dell'esportatore in una giurisdizione che offre un livello di protezione sostanzialmente equivalente,

l'EDPB ritiene che la cifratura del trasporto, ove del caso in combinazione con la cifratura dei contenuti end-to-end, costituisce un'efficace misura supplementare.

Caso d'uso 4: destinatario protetto

85. Un esportatore di dati trasferisce dati personali a un importatore di dati in un paese terzo specificamente protetto dalla legge di tale paese, ad esempio per fornire congiuntamente cure mediche a un paziente o servizi legali a un cliente.

Se

1. la legge di un paese terzo esonera l'importatore di dati residente da una potenziale violazione dei dati in possesso di tale destinatario per la finalità prefissata, ad esempio in virtù di un obbligo di segreto professionale che si applica all'importatore di dati,
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 cifrate, 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 di quest'ultimo, né inoltra i dati a un'altra entità non protetta, sulla base degli strumenti di trasferimento di cui all'articolo 46 del GRDP,
4. i dati personali sono cifrati prima di essere trasmessi con un metodo conforme allo stato dell'arte che garantisce che la decifrazione non sarà possibile senza la conoscenza della chiave di decifrazione (cifratura end-to-end) per tutto il tempo in cui i dati devono essere protetti,
5. la chiave di decifrazione è in custodia esclusiva dell'importatore dei dati protetti e opportunamente protetta contro l'uso o la divulgazione non autorizzati 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,

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

Caso d'uso 5: trattamento frazionato o multilaterale

86. L'esportatore di dati desidera che i dati personali siano trattati congiuntamente da due o più responsabili del trattamento indipendenti situati in giurisdizioni diverse senza rivelare loro il contenuto dei dati. Prima della trasmissione, suddivide i dati in modo tale che nessuna parte che un singolo

responsabile del trattamento riceve sia sufficiente per ricostruire i dati personali in tutto o in parte. L'esportatore di dati riceve il risultato del trattamento da ciascuno dei responsabili del trattamento in modo indipendente e fonde i pezzi ricevuti per arrivare al risultato finale che può costituire dati personali o aggregati.

Se

1. un esportatore di dati tratta i dati personali in modo tale che essi siano suddivisi in due o più parti, ciascuna delle quali non può più essere interpretata o attribuita a un determinato interessato senza l'utilizzo di informazioni aggiuntive,
2. ognuno dei pezzi viene trasferito a un responsabile del trattamento separato situato in una giurisdizione diversa,
3. i responsabili del trattamento trattano opzionalmente i dati in comune, ad esempio 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 rispetto ad 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 che consentisse loro di accedere a tutti i set di dati personali in possesso dei responsabili del trattamento e permettesse 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 titolare 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 pezzi di dati personali che trasmette ai responsabili del trattamento non possono essere attribuiti a una persona fisica identificata o identificabile, anche se incrociati con tali informazioni,

l'EDPB ritiene che il trattamento frazionato eseguito fornisca un'efficace misura supplementare.

Scenari nei quali non è stato possibile trovare misure *efficaci*

87. Le misure descritte di seguito in alcuni scenari non sarebbero efficaci nel garantire un livello di protezione sostanzialmente equivalente dei dati trasferiti verso il paese terzo. Pertanto, non si qualificherebbero come misure supplementari.

Caso d'uso 6: trasferimento a fornitori di servizi cloud o ad altri responsabili del trattamento che richiedono l'accesso ai dati in chiaro

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

Se

1. un titolare del trattamento trasferisce i dati a un fornitore di servizi cloud o a un altro responsabile del trattamento,
2. il fornitore di servizi cloud o altro responsabile del trattamento deve accedere ai dati in chiaro per eseguire il compito assegnato, e

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[71],

l'EDPB, considerato l'attuale stato dell'arte, non è in grado di prevedere una misura tecnica efficace per impedire che tale accesso violi i diritti degli interessati. L'EDPB non esclude che l'ulteriore sviluppo tecnologico possa offrire misure in grado di conseguire gli scopi commerciali previsti, senza richiedere l'accesso in chiaro.

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

Caso d'uso 7: accesso remoto ai dati per scopi commerciali

90. Un esportatore di dati mette i dati personali a disposizione di entità di un paese terzo per essere utilizzati per scopi commerciali condivisi. Una tipica costellazione può essere costituita da un titolare del trattamento o da un responsabile del trattamento stabilito nel territorio di uno Stato membro che trasferisce dati personali a un titolare del trattamento o a un responsabile del trattamento in un paese terzo appartenente allo stesso gruppo di imprese o a un gruppo di imprese che esercita un'attività economica comune. L'importatore di dati può, ad esempio, utilizzare i dati ricevuti per fornire servizi di 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, mediante l'uso di un servizio di comunicazione,
2. l'importatore utilizza i dati in chiaro per i propri scopi,
3. il potere concesso alle autorità pubbliche del paese destinatario di accedere ai dati trasferiti va oltre quanto necessario e proporzionato in una società democratica,

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

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

[71] Si vedano gli articoli 47 e 52 della Carta dei diritti fondamentali dell'Unione europea, l'articolo 23, paragrafo 1, del RGPD e le raccomandazioni dell'EDPB relative alle garanzie essenziali europee per le misure di sorveglianza.

Misure contrattuali supplementari

92. Queste misure consisteranno generalmente in impegni contrattuali[72] unilaterali, bilaterali o multilaterali[73]. Se viene utilizzato uno strumento di trasferimento di cui all'articolo 46 del RGPD, nella maggior parte dei casi esso conterrà già una serie di impegni (per lo più contrattuali) per l'esportatore e l'importatore dei dati, volti a tutelare i dati personali[74].

93. In alcune situazioni, tali misure possono integrare e rafforzare le garanzie che lo strumento di trasferimento e la legislazione pertinente del paese terzo possono fornire, quando, tenuto conto delle circostanze del trasferimento, non soddisfano tutte le condizioni necessarie per assicurare un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'UE. Tenuto conto della natura delle misure contrattuali, generalmente non in grado di vincolare le autorità di tale paese terzo, quando non sono parte del contratto[75], tali misure dovrebbero essere combinate con altre misure tecniche e organizzative per fornire il livello di protezione dei dati richiesto. La selezione e l'attuazione di una o più di queste misure non garantirà necessariamente e sistematicamente che il vostro trasferimento soddisfi gli standard di sostanziale equivalenza richiesti dal diritto dell'Unione.

94. A seconda di quali misure contrattuali sono già incluse nello strumento di trasferimento di cui all'articolo 46 del RGPD su cui si fa affidamento, possono 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 verso paesi terzi.

95. Come detto, le misure contrattuali non potranno escludere l'applicazione della legislazione di un paese terzo che non soddisfa lo standard delle garanzie essenziali europee dell'EDPB nei casi in cui la legislazione obbliga gli importatori a rispettare gli ordini di divulgazione dei dati ricevuti dalle autorità pubbliche[76].

96. Alcuni esempi di queste potenziali misure contrattuali sono elencati qui di seguito e classificati in base alla loro natura:

Prevedere l'obbligo contrattuale di utilizzare misure tecniche specifiche

97. ***A seconda delle circostanze specifiche dei trasferimenti, il contratto potrebbe dover prevedere che, affinché i trasferimenti abbiano luogo, debbano essere messe in atto misure tecniche specifiche (vedi sopra le misure tecniche suggerite).***

98. ***Condizioni di efficacia***

---

[72] Essi avranno carattere privato e non saranno considerati accordi internazionali ai sensi del diritto internazionale pubblico. Di conseguenza, di norma non vincoleranno 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), paragrafo 125.

[73] Ad esempio nell'ambito delle norme vincolanti d'impresa, che dovrebbero in ogni caso disciplinare alcune delle misure elencate di seguito.

[74] Cfr. sentenza C-311/18 (Schrems II), paragrafo 137, in cui la Corte ha riconosciuto che le clausole contrattuali tipo contengono *«meccanismi efficaci che [consentono], in pratica, di garantire che sia rispettato il livello di protezione richiesto dal diritto dell'Unione e che i trasferimenti di dati personali, fondati su siffatte clausole, siano sospesi o vietati in caso di violazione di tali clausole o di impossibilità di rispettarle»*; cfr. anche paragrafo 148.

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

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

- Questa clausola potrebbe essere efficace nelle situazioni in cui l'esportatore abbia individuato la necessità di misure tecniche. Dovrebbe quindi essere fornita in una forma giuridica per garantire che anche l'importatore si impegni a mettere in atto le misure tecniche necessarie, se del caso.

Obblighi di trasparenza

99. ***L'esportatore potrebbe aggiungere al contratto allegati con informazioni che l'importatore fornirebbe, sulla base dei suoi migliori sforzi, sull'accesso ai dati da parte delle autorità pubbliche, anche nel campo dell'intelligence, a condizione che la legislazione sia conforme alle garanzie essenziali europee dell'EDPB, nel paese di destinazione. Ciò potrebbe aiutare l'esportatore di dati a rispettare l'obbligo di documentare la valutazione del livello di protezione nel paese terzo.***

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

(1) elencare le leggi e i regolamenti del paese di destinazione applicabili all'importatore o ai relativi responsabili del trattamento (a vari livelli) che consentirebbero alle autorità pubbliche di accedere ai dati personali oggetto del trasferimento, in particolare nei settori dell'intelligence, dell'applicazione della legge, del controllo amministrativo e regolamentare 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 relazioni provenienti da varie fonti (ad esempio partner, fonti aperte, giurisprudenza nazionale e decisioni degli organi di controllo) sull'accesso da parte delle autorità pubbliche ai dati personali in situazioni del tipo di trasferimento di dati in questione (ad esempio nel settore normativo specifico; riguardo al tipo di entità a cui appartiene l'importatore di dati; ...)
(3) indicare quali misure sono 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 periodo di tempo[77], in particolare nei settori di cui al punto 1) e che comprendono informazioni sulle richieste ricevute, sui dati richiesti, sull'organismo richiedente, sulla base giuridica per la divulgazione e sulla misura in cui l'importatore ha divulgato la richiesta di dati[78];
(5) specificare se e in quale misura all'importatore è legalmente vietato fornire le informazioni di cui ai punti da 1) a 5).

101. Tali informazioni potrebbero essere fornite mediante questionari strutturati che l'importatore compilerebbe e firmerebbe e che sarebbero integrati dall'obbligo contrattuale dell'importatore di dichiarare entro un determinato periodo di tempo qualsiasi potenziale cambiamento di tali informazioni, come è prassi corrente per i processi di due diligence.

[77] 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 prima della chiusura dello strumento di esportazione dei dati con l'esportatore di dati.
[78] Il rispetto di questo dovere non equivale, in quanto tale, a fornire un livello di protezione adeguato. Al tempo stesso, qualsiasi divulgazione inadeguata che sia effettivamente avvenuta porta alla necessità di attuare misure supplementari.

102. ***Condizioni di efficacia***

- L'importatore deve essere in grado di fornire all'esportatore questo tipo di informazioni al meglio delle sue conoscenze e dopo aver fatto del suo meglio per ottenerle[79].
- Questo obbligo imposto all'importatore è un mezzo per garantire che l'esportatore diventi e rimanga consapevole dei rischi connessi al trasferimento dei dati verso un paese terzo. Esso consentirà quindi all'esportatore di desistere dalla conclusione del contratto o, se le informazioni cambiano in seguito alla sua conclusione, di adempiere all'obbligo di sospendere il trasferimento e/o risolvere il contratto se la legge del paese terzo, le garanzie previste dallo strumento di trasferimento di cui all'articolo 46 del RGPD utilizzato e le eventuali garanzie 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 previsione 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 creato intenzionalmente backdoor o programmi simili che potrebbero essere utilizzati per accedere al sistema e/o ai dati personali, 2) non ha creato o modificato intenzionalmente i suoi processi commerciali in modo da facilitare l'accesso ai dati personali o ai sistemi, e 3) la legge nazionale o la politica governativa non impongono all'importatore di creare o mantenere backdoor o di agevolare l'accesso ai dati personali o ai sistemi, o di essere in possesso o consegnare la chiave di cifratura[80].***

104. ***Condizioni di efficacia***

- L'esistenza di una legislazione o di politiche governative che impediscono agli importatori di divulgare queste informazioni può rendere questa clausola inefficace. L'importatore non sarà quindi in grado di stipulare il contratto o dovrà comunicare all'esportatore la sua incapacità di continuare a rispettare gli impegni contrattuali[81].
- Il contratto deve includere sanzioni e/o la possibilità dell'esportatore di risolvere il contratto con breve preavviso nei casi in cui l'importatore non riveli l'esistenza di una backdoor o di un programma simile o di processi commerciali manipolati o l'obbligo di attuare uno di essi o non informi tempestivamente l'esportatore non appena ne venga a conoscenza.

***

105. ***L'esportatore potrebbe rafforzare il suo potere di effettuare verifiche[82] o ispezioni delle strutture di trattamento dei dati dell'importatore, in loco e/o da remoto, per verificare se i dati sono stati divulgati alle autorità pubbliche e a quali condizioni (accesso non oltre quanto necessario e proporzionato in una società democratica), ad esempio prevedendo un breve preavviso e meccanismi***

[79] Cfr. paragrafo 32, punto 5, supra.
[80] Questa clausola è importante per garantire un adeguato livello di protezione dei dati personali trasferiti e di solito dovrebbe essere richiesta.
[81] Cfr. paragrafo 32, punto 5, supra.
[82] Si veda ad esempio la clausola 5, lettera f), della decisione 2010/87/UE relativa alle clausole contrattuali tipo tra titolari e responsabili del trattamento; le verifiche potrebbero essere effettuate anche nell'ambito di un codice di condotta o mediante certificazione.

che garantiscano il rapido intervento degli organismi di controllo e rafforzino l'autonomia dell'esportatore nella scelta degli stessi.

106. ***Condizioni di efficacia***

- Per essere pienamente efficace, l'ambito della verifica deve coprire legalmente e tecnicamente qualsiasi trattamento dei dati personali trasmessi nel paese terzo da parte dei responsabili del trattamento, a vari livelli, dell'importatore.
- I registri di accesso e altri percorsi simili dovrebbero essere a prova di manomissione in modo che i revisori possano trovare le prove della divulgazione. I registri di accesso e altri percorsi simili dovrebbero inoltre distinguere tra gli accessi dovuti a regolari operazioni commerciali e gli accessi dovuti a ordini o richieste di accesso.

***

107. ***Qualora la legge e la prassi del paese terzo dell'importatore siano state inizialmente valutate e si sia ritenuto che forniscano un livello di protezione sostanzialmente equivalente a quello previsto nell'UE per i dati trasferiti dall'esportatore, quest'ultimo potrebbe comunque rafforzare l'obbligo dell'importatore dei dati di informare tempestivamente l'esportatore dell'impossibilità di rispettare gli impegni contrattuali e di conseguenza lo standard richiesto di «livello di protezione dei dati sostanzialmente equivalente».***[83]

108. Tale incapacità può derivare da cambiamenti nella legislazione o nella prassi del paese terzo[84]. Le clausole potrebbero stabilire termini e procedure specifici e rigorosi per la 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 portata e l'efficacia delle misure adottate per contrastarle dovrebbero fornire all'esportatore indicazioni sufficienti per esercitare il suo dovere di sospendere o terminare il trasferimento e/o risolvere il contratto.

109. ***Condizioni di efficacia***

- La notifica deve avvenire prima che l'accesso ai dati venga concesso. In caso contrario, al momento in cui l'esportatore riceve la notifica, i diritti della persona potrebbero essere già stati violati se la richiesta si basa su leggi di tale paese terzo che superano il livello di protezione dei dati consentito dal diritto dell'Unione. La notifica può comunque servire a prevenire future violazioni e a consentire all'esportatore di adempiere al suo dovere di sospendere il trasferimento dei dati personali al paese terzo e/o di rescindere il contratto.
- L'importatore di dati deve monitorare qualsiasi sviluppo legale o politico che potrebbe comportarne l'incapacità di adempiere ai suoi obblighi e informare tempestivamente l'esportatore di tali cambiamenti e sviluppi, se possibile prima della loro attuazione, per consentire all'esportatore di recuperare i dati.

[83] Clausola 5, lettera a) e lettera d), punto i) della decisione 2010/87/UE relativa alle clausole contrattuali tipo.
[84] Cfr. C-311/18 (Schrems II), paragrafo 139, in cui la Corte afferma che *«se è vero che la stessa clausola 5, lettera d), i), consente al destinatario del trasferimento di dati personali, in presenza di legislazione che gliene faccia divieto, ad esempio norme di diritto penale miranti a tutelare il segreto delle indagini, di non comunicare al titolare del trattamento stabilito nell'Unione una richiesta giuridicamente vincolante presentata da autorità giudiziarie o di polizia ai fini della comunicazione di dati personali, egli è tuttavia tenuto, conformemente alla clausola 5, lettera a), dell'allegato della decisione CPT, ad informare il titolare del trattamento dell'impossibilità di conformarsi alle clausole tipo di protezione dei dati»*.

- Le clausole dovrebbero prevedere un meccanismo rapido in base al quale l'esportatore di dati autorizza l'importatore di dati a mettere in sicurezza o a restituire prontamente i dati all'esportatore o, se ciò non è fattibile, a cancellare o cifrare in modo sicuro i dati senza necessariamente attendere le istruzioni dell'esportatore, se viene 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 verifiche, ispezioni e altre misure di verifica e di farle rispettare con sanzioni per l'importatore e/o la capacità dell'esportatore di sospendere il trasferimento e/o di rescindere 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», in base al quale l'importatore si impegna a pubblicare regolarmente (ad esempio, almeno ogni 24 ore) un messaggio firmato in forma cifrata che informa l'esportatore che a partire da una certa data e ora non ha ricevuto alcun ordine di rivelare dati personali o simili. L'assenza di un aggiornamento di questa comunicazione indicherà all'esportatore che l'importatore potrebbe aver ricevuto un ordine in questo senso.***

111. ***Condizioni di efficacia***

- Le norme del paese terzo devono consentire all'importatore di dati di emettere questa forma di notifica passiva all'esportatore.
- L'esportatore di dati deve controllare automaticamente le comunicazioni di *warrant canary*.
- L'importatore di dati deve garantire che la sua chiave privata per la firma del *warrant canary* sia tenuta al sicuro e che non possa essere costretto a emettere falsi *warrant canary* dalle norme del paese terzo. A tal fine, potrebbe essere utile la necessità di più firme da parte di persone diverse e/o l'emissione del *warrant canary* da parte di una persona al di fuori della giurisdizione del paese terzo.

Obblighi di intraprendere azioni specifiche

112. ***L'importatore potrebbe impegnarsi a verificare, in base alla legge del paese di destinazione, la legalità di eventuali ordini di divulgazione dei dati, in particolare se essi rimangono nei limiti dei poteri concessi all'autorità pubblica richiedente, e a contestare l'ordine se, dopo un'attenta valutazione, conclude che vi sono motivi per farlo in base alla legge del paese di destinazione. Nell'impugnare un ordine, l'importatore di dati dovrebbe chiedere misure provvisorie per sospendere gli effetti dello stesso fino a quando il tribunale non si sarà pronunciato nel merito. L'importatore avrebbe l'obbligo di non divulgare i dati personali richiesti fino a quando non sia tenuto a farlo in base alle norme procedurali applicabili. L'importatore si impegnerebbe inoltre a fornire la quantità minima di informazioni consentita in risposta all'ordine, sulla base di un'interpretazione ragionevole dello stesso.***

113. ***Condizioni di efficacia***

- L'ordinamento giuridico del paese terzo deve offrire vie legali efficaci per contestare gli ordini di divulgazione dei dati.
- Questa clausola offrirà sempre una protezione aggiuntiva molto limitata, poiché un ordine di divulgazione dei dati può essere legittimo secondo l'ordinamento giuridico del paese terzo, ma tale ordinamento giuridico potrebbe non soddisfare gli standard dell'Unione. Questa misura contrattuale dovrà necessariamente essere integrata da altre misure supplementari.
- Le contestazioni degli ordini devono avere un effetto sospensivo ai sensi della legge del paese terzo. In caso contrario, le autorità pubbliche avrebbero comunque accesso ai dati delle persone fisiche e qualsiasi azione conseguente a favore delle stesse avrebbe l'effetto limitato di consentire loro di chiedere il risarcimento dei danni per le conseguenze negative derivanti dalla divulgazione dei dati.
- L'importatore dovrà essere in grado di documentare e dimostrare all'esportatore le azioni che ha intrapreso, facendo del suo meglio, per adempiere a questo impegno.

***

114. ***Nella stessa situazione sopra descritta, l'importatore potrebbe impegnarsi a informare l'autorità pubblica richiedente dell'incompatibilità dell'ordine rispetto alle garanzie previste dallo strumento di trasferimento di cui all'articolo 46 del RGPD[85] e del conseguente conflitto di obblighi per l'importatore. L'importatore informerebbe contemporaneamente e al più presto possibile l'esportatore e/o l'autorità di controllo competente del SEE, nella misura del possibile ai sensi dell'ordinamento giuridico del paese terzo.***

115. ***Condizioni di efficacia***

- Tali informazioni sulla protezione conferita dal diritto dell'Unione e sul conflitto di obblighi dovrebbero avere un qualche effetto giuridico nell'ordinamento 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 aggiungere una qualche protezione ai dati.
- L'ordinamento giuridico del paese non deve impedire all'importatore di informare l'esportatore o almeno l'autorità di controllo competente del SEE dell'ordine o della richiesta di accesso ricevuta.
- L'importatore dovrà essere in grado di documentare e dimostrare all'esportatore le azioni che ha intrapreso, facendo del suo meglio, per adempiere a questo impegno.

[85] Ad esempio, le clausole contrattuali tipo prevedono che il trattamento dei dati, compreso il loro trasferimento, sia stato e continui a essere effettuato in conformità alla *«legge applicabile in materia di 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 al rispetto della vita privata in relazione al trattamento dei dati personali applicabile a un titolare del trattamento dei dati nello Stato membro in cui è stabilito l'esportatore di dati»*. La CGUE conferma che le disposizioni del RGPD, lette alla luce della Carta dei diritti fondamentali dell'Unione, fanno parte di tale legislazione; cfr. CGUE C-311/18 (Schrems II), paragrafo 138.

Consentire agli interessati di esercitare i loro diritti

116. ***Il contratto potrebbe prevedere che si possa accedere ai dati personali trasmessi in chiaro nel corso della normale attività commerciale (anche in casi di supporto) solo con il consenso espresso o implicito dell'esportatore e/o dell'interessato.***

117. ***Condizioni di efficacia***

- Questa clausola potrebbe essere efficace in quelle situazioni in cui gli importatori ricevono richieste di cooperazione da parte delle autorità pubbliche 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 potrebbe non essere in grado di opporsi all'accesso o di dare un consenso che soddisfi tutte le condizioni stabilite dal diritto dell'Unione (liberamente dato, specifico, informato e non ambiguo) (ad esempio nel caso dei dipendenti)[86].
- Le normative o le politiche nazionali che obbligano l'importatore a non divulgare l'ordine di accesso possono rendere inefficace questa clausola, a meno che non possa essere sostenuta con metodi tecnici che richiedano l'intervento dell'esportatore o dell'interessato affinché i dati in chiaro siano accessibili. Tali misure tecniche volte a limitare l'accesso possono essere previste in particolare se l'accesso è concesso solo in casi specifici di supporto o di servizio, ma i dati stessi sono conservati nel SEE.

***

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 l'impossibilità da parte dell'importatore di rispettare gli impegni contrattuali, per consentire all'interessato di chiedere informazioni e di ottenere un ricorso effettivo (ad esempio presentando un reclamo all'autorità di controllo competente e/o all'autorità giudiziaria e dimostrando la sua posizione dinanzi ai tribunali del paese terzo).***

119. ***Condizioni di efficacia***

- Questa comunicazione potrebbe allertare l'interessato di potenziali accessi ai suoi dati da parte di autorità pubbliche di paesi terzi. Potrebbe così consentire all'interessato di chiedere informazioni aggiuntive agli esportatori e di presentare un reclamo all'autorità di controllo competente. Questa clausola potrebbe anche affrontare alcune delle difficoltà che una persona può incontrare nel dimostrare la propria legittimazione processuale (*locus standi*) dinanzi ai tribunali di paesi terzi per contestare l'accesso ai propri dati da parte delle autorità pubbliche.
- Le normative e le politiche nazionali possono impedire questa comunicazione all'interessato. L'esportatore e l'importatore potrebbero tuttavia impegnarsi a informare l'interessato non appena le restrizioni alla divulgazione dei dati siano revocate e a fare il possibile per ottenere la deroga al divieto di divulgazione. Come minimo, l'esportatore o l'autorità di controllo competente potrebbero comunicare all'interessato la sospensione o la cessazione del

[86] Articolo 4, paragrafo 11, del RGPD.

trasferimento dei suoi dati personali a causa dell'impossibilità 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 mediante meccanismi di ricorso ad hoc e consulenza legale.***

121. ***Condizioni di efficacia***

- Le normative e le politiche nazionali possono imporre condizioni che possono compromettere l'efficacia dei meccanismi di ricorso ad hoc previsti.
- La consulenza legale potrebbe essere utile per l'interessato, soprattutto considerando quanto complesso e costoso possa essere per lo stesso comprendere 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 agli interessati 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 integrata da altre misure supplementari.

Questa misura supplementare sarebbe efficace solo a condizione che il diritto del paese terzo preveda un ricorso dinanzi ai tribunali nazionali o che esista un meccanismo di ricorso ad hoc. In ogni caso, non si tratterebbe comunque di una misura supplementare efficace contro le misure di sorveglianza se non esiste un meccanismo di ricorso.

Misure organizzative

122. Ulteriori misure organizzative possono consistere in politiche interne, metodi organizzativi e standard che i titolari del trattamento e i responsabili del trattamento potrebbero applicare a se stessi e imporre agli importatori di dati in paesi terzi. Esse possono contribuire a garantire la coerenza della protezione dei dati personali durante l'intero ciclo del trattamento. Le misure organizzative possono anche migliorare la consapevolezza degli esportatori rispetto ai rischi e ai tentativi di accedere ai dati nei paesi terzi e la loro capacità di reagire ad essi. La selezione e l'attuazione di una o più di queste misure non garantirà necessariamente e sistematicamente che il vostro trasferimento soddisfi gli standard di sostanziale equivalenza richiesti dal diritto dell'Unione. A seconda delle circostanze specifiche del trasferimento e della valutazione effettuata sulla legislazione del paese terzo, sono necessarie misure organizzative 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 idonee deve essere effettuata caso per caso, tenendo presente che i titolari del trattamento e i responsabili del trattamento devono 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 anche altre misure possono essere appropriate.

Politiche interne per la governance dei trasferimenti, in particolare con i gruppi di imprese

124. ***Adozione di adeguate politiche interne con una chiara attribuzione delle responsabilità per il trasferimento dei dati, canali di segnalazione e procedure operative standard per i casi di richieste di accesso ai dati da parte di autorità pubbliche, occulte o ufficiali. Soprattutto in caso di trasferimenti tra gruppi di imprese, tali politiche possono includere, tra l'altro, la nomina di un team specifico, che dovrebbe avere sede all'interno del SEE, composto da esperti in materia di informatica, protezione dei dati e leggi sulla privacy, per trattare le richieste che riguardano dati personali trasferiti dall'UE; la comunicazione alla direzione legale e aziendale e all'esportatore di dati al ricevimento di tali richieste; i passaggi 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 di gestire le 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'Unione in materia di accesso ai dati personali da parte delle autorità pubbliche, in particolare come previsto 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 elaborata, ove possibile, in collaborazione con l'esportatore di dati.

126. ***Condizioni di efficacia***

- Queste politiche possono essere previste solo nei casi in cui la richiesta delle autorità pubbliche del paese terzo è compatibile con il diritto dell'Unione[87]. Quando la richiesta è incompatibile, tali 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 misure supplementari adeguate per evitare l'accesso.

Misure per la trasparenza e la responsabilizzazione

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

128. ***Condizioni di efficacia***

- La legislazione nazionale del paese terzo può impedire la divulgazione delle richieste o delle informazioni sostanziali e quindi rendere inefficace questa prassi. L'importatore di dati dovrebbe informare l'esportatore della sua incapacità di fornire tali documenti e registrazioni,

[87] Cfr. causa C-362/14 («Schrems I»), paragrafo 94; C-311/18 (Schrems II), paragrafi 168, 174, 175 e 176.

offrendogli così la possibilità di sospendere i trasferimenti se tale incapacità comportasse una diminuzione del livello di protezione.

***

129. ***La pubblicazione regolare di relazioni 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 può impedire la divulgazione di informazioni dettagliate. In questi casi, l'importatore di dati dovrebbe adoperarsi al meglio per pubblicare informazioni statistiche o informazioni aggregate di tipo analogo.

Metodi di organizzazione e misure di minimizzazione dei dati

131. ***Anche i requisiti organizzativi già esistenti in base al principio di responsabilizzazione, come l'adozione di politiche di accesso ai dati e di riservatezza rigorose e granulari e le migliori pratiche, basate su un rigoroso principio di necessità di sapere, monitorate con verifiche regolari e applicate attraverso misure disciplinari, possono essere misure utili in un contesto di trasferimento. A questo proposito si dovrebbe prendere in considerazione la minimizzazione dei dati, al fine di limitare l'esposizione dei dati personali ad accessi non autorizzati. Ad esempio, in alcuni casi potrebbe non essere necessario trasferire determinati dati (ad esempio, in caso di accesso remoto ai dati SEE, come nei casi di supporto, quando è concesso l'accesso limitato invece di un accesso completo; oppure quando la fornitura di un servizio richiede solo il trasferimento di un set di dati limitato e non di un'intera banca dati).***

132. ***Condizioni di efficacia***

- Dovrebbero essere previste verifiche regolari e forti misure disciplinari per monitorare e far rispettare le misure di minimizzazione dei dati anche nel contesto del trasferimento.
- L'esportatore di dati effettua una valutazione dei dati personali in suo possesso prima che il trasferimento abbia luogo, al fine di individuare i set di dati che non sono necessari ai fini del trasferimento e che quindi non saranno condivisi con l'importatore di dati.
- Le misure di minimizzazione dei dati devono essere accompagnate da misure tecniche atte a garantire che i dati non siano soggetti ad accesso non autorizzato. Ad esempio, l'applicazione di meccanismi di calcolo multilaterali sicuri e la diffusione di set di dati cifrati tra diverse entità di fiducia può impedire, fin dalla progettazione, che un eventuale accesso unilaterale comporti la divulgazione di dati identificabili.

***

133. ***Sviluppo di migliori prassi per coinvolgere in modo appropriato e tempestivo e fornire accesso alle informazioni 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 ricevono tutte le informazioni pertinenti prima del trasferimento e sono consultati sulla necessità del trasferimento e sulle eventuali garanzie supplementari.
- Le informazioni pertinenti devono comprendere, ad esempio, la valutazione della necessità del trasferimento dei dati personali specifici, una panoramica delle leggi del paese terzo applicabili e le garanzie che l'importatore si è impegnato ad attuare.

Adozione di standard e migliori prassi

135. ***Adozione di politiche rigorose in materia di sicurezza e riservatezza dei dati, basate sulla certificazione UE o su codici di condotta o su standard internazionali (ad esempio norme ISO) e sulle migliori prassi (ad esempio ENISA), nel rispetto 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

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

***

137. ***L'impegno dell'importatore di dati a non effettuare trasferimenti successivi dei dati personali all'interno dello stesso paese o di altri paesi terzi, o a sospendere i trasferimenti in corso, qualora non possa essere garantito nel paese terzo un livello di protezione dei dati personali equivalente a quello garantito all'interno dell'UE[88].***

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

ALLEGATO 3: POSSIBILI FONTI DI INFORMAZIONI PER VALUTARE UN PAESE TERZO

138. Il vostro importatore di dati dovrebbe essere in grado di fornirvi le fonti e le informazioni pertinenti relative al paese terzo in cui è stabilito e alle leggi ad esso applicabili. Potete anche fare riferimento a svariate fonti di informazione, come quelle elencate di seguito in modo non esaustivo:

- giurisprudenza della Corte di giustizia dell'Unione europea (CGUE) e della Corte europea dei diritti dell'uomo (CEDU)[89], come indicato nelle raccomandazioni relative alle garanzie essenziali europee[90];
- decisioni di adeguatezza nel paese di destinazione se il trasferimento si basa su una base giuridica diversa[91];
- risoluzioni e relazioni di organizzazioni intergovernative, quali il Consiglio d'Europa[92], altri organismi regionali[93] e organi e agenzie dell'ONU (ad esempio il Consiglio dei diritti umani delle Nazioni Unite[94] o il Comitato dei diritti umani[95]);
- giurisprudenza nazionale o decisioni prese da autorità giudiziarie o amministrative indipendenti competenti in materia di privacy e di protezione dei dati di paesi terzi;
- relazioni di istituzioni accademiche e organizzazioni della società civile (ad esempio ONG e associazioni di categoria).

[89] Si veda la scheda della giurisprudenza della CEDU sulla sorveglianza di massa: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf
[90] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions
[91] C-311/18 (Schrems II), paragrafo 141; cfr. decisioni di adeguatezza in https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
[92] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions
[93] Cfr., ad esempio, i rapporti sui paesi della Commissione interamericana dei diritti dell'uomo (CIDH), https://www.oas.org/en/iachr/reports/country.asp.
[94] Cfr. https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx
[95] Cfr.: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5