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

Versione 2.0

Adottate il 18 giugno 2021

Cronologia delle versioni

Versione 2.0	18 giugno 2021	Adozione delle raccomandazioni dopo la consultazione pubblica
Versione 1.0	10 novembre 2020	Adozione delle raccomandazioni per consultazione pubblica

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 il diritto 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 responsabilizzazione di cui all'articolo 5, paragrafo 2, del RGPD, che prevede 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 trattati.

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. Solo in alcuni casi sarà possibile basarsi su una delle deroghe previste dall'articolo 49 del RGPD, se le condizioni sono soddisfatte. Le deroghe non possono diventare «la norma» nella pratica, ma devono essere limitate a situazioni specifiche.

Un **terzo passo** consiste nel **valutare** se vi sia qualcosa nella legislazione e/o nelle prassi vigenti del paese terzo che possa incidere sull'efficacia delle garanzie adeguate offerte dagli strumenti di trasferimento su cui fate affidamento, nel contesto del vostro specifico trasferimento. La vostra valutazione deve concentrarsi innanzitutto 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. Inoltre, l'esame delle prassi delle autorità pubbliche di paesi terzi vi permetterà di verificare se le garanzie contenute nello strumento di trasferimento possano assicurare, nella pratica, la protezione efficace dei dati personali trasferiti. L'esame di queste prassi sarà particolarmente pertinente per la valutazione nel caso in cui:

(i.) sia evidente che la legislazione del paese terzo, formalmente conforme agli standard dell'UE, non è applicata/rispettata nella pratica;

(ii.) esistano prassi incompatibili con gli impegni previsti dallo strumento di trasferimento qualora la legislazione pertinente del paese terzo sia carente;

(iii.) i dati trasferiti e/o l'importatore rientrino o possano rientrare nell'ambito di applicazione di una legislazione problematica (cioè una legislazione che pregiudica la garanzia contrattuale, prevista dallo strumento di trasferimento, di un livello di protezione sostanzialmente equivalente e non osserva le norme dell'UE in materia di diritti fondamentali, necessità e proporzionalità).

Nelle prime due situazioni, dovrete sospendere il trasferimento oppure mettere in atto misure supplementari adeguate se desiderate procedere con il trasferimento.

Nella terza situazione, considerando le incertezze relative alla potenziale applicazione al vostro trasferimento di una legislazione problematica, potete decidere di: sospendere il trasferimento; mettere in atto misure supplementari per procedere con il trasferimento; o, in alternativa, se ritenete e siete in grado di dimostrare e documentare di non avere motivo di credere che la legislazione problematica in questione verrà interpretata e/o attuata nella pratica in modo da riguardare i vostri dati trasferiti e l'importatore, potete scegliere di procedere con il trasferimento senza mettere in atto misure supplementari.

Per definire 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.

Questa valutazione va condotta con la dovuta diligenza e documentata accuratamente. Le vostre autorità di controllo e/o giudiziarie competenti potrebbero richiederla e ritenervi responsabili di qualsiasi decisione da voi presa 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 e/o le prassi del paese terzo incidono 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 legislazione e delle prassi del paese terzo e dello strumento di trasferimento su cui fate affidamento, in quanto sarete ritenuti responsabili di qualsiasi decisione presa su tale base. Ciò potrebbe anche richiedere la combinazione di più misure supplementari. In ultima analisi, potreste concludere che nessuna misura supplementare è in grado di garantire un livello di protezione sostanzialmente equivalente per il vostro specifico trasferimento. Ove 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 alcune di queste formalità; in alcuni casi potrebbe essere necessario consultare le autorità di controllo competenti.

Il **sesto e ultimo passo** consiste nel **riesaminare** a intervalli adeguati il livello di protezione dei dati personali che trasferite verso paesi terzi e di controllare se vi siano stati o vi saranno sviluppi che possano influire in questo senso. Il principio di responsabilizzazione richiede vigilanza continua rispetto al livello di protezione dei dati personali.

Le autorità di controllo continueranno a esercitare il mandato loro conferito di 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 ritengano che non possa essere garantito un livello di protezione sostanzialmente equivalente, a seguito di un'indagine o di un reclamo.

Le autorità di controllo continueranno a sviluppare orientamenti per gli esportatori e a coordinare le attività 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 né 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 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 nel SEE. 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, sia durante sia dopo il trasferimento.

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 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 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 e continui 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

([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]) Artiicolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea. Art
([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 Data Protection Commissioner [di seguito «C-362/14 (Schrems I)»], paragrafo 45.*
([15]) C-311/18 (Schrems II), paragrafi 92 e 93.

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 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 CRONOPROGRAMMA PER APPLICARE IL PRINCIPIO DI RESPONSABILIZZAZIONE AL TRASFERIMENTO DEI DATI NELLA PRATICA

6. Quello che segue è un cronoprogramma 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 ([19]) e 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) ([20]). 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 ([21]).

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 ([22]).

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 ([23]), il primo passo

([16]) C-311/18 (Schrems II), paragrafi 134, 135, 139, 140, 141 e 142.
([17]) C-311/18 (Schrems II), paragrafo 134.
([18]) Articolo 5, paragrafo 2, e articolo 28, paragrafo 3, lettera h), del RGPD.
([19]) Perciò, per esempio, non si considerano esportatori di dati gli interessati che forniscono i propri dati personali per mezzo di un questionario online a un titolare del trattamento stabilito in un paese terzo.
([20]) 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_en
([21]) Linee guida 2/2020 dell'EDPB 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 e di paesi non appartenenti al SEE; cfr. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_it
([22]) Articolo 5, paragrafo 2, del RGPD e articolo 24, paragrafo 1, del RGPD.
([23]) 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.

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 quei soggetti che sono coinvolti 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.

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 ([24]). Possono esservi di aiuto anche le attività già messe in atto al fine di 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, relativamente ai trasferimenti dei loro dati personali da voi effettuati verso paesi terzi ([25]).

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 ([26]).

11. In linea con il principio della «minimizzazione dei dati» ([27]) del RGPD, dovete verificare che i dati trasferiti siano adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per le quali vengono trattati.

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 offerta da un

---

([24]) 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 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 posizione 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 (approvato dall'EDPB il 25 maggio 2018).

([25]) 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, specificare le garanzie opportune o adeguate e i mezzi con cui ottenerne una copia ovvero il luogo dove sono state rese disponibili. Le informazioni fornite all'interessato devono essere corrette e aggiornate, soprattutto alla luce della giurisprudenza della Corte in materia di trasferimenti.

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

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

fornitore di servizi sono considerati un trasferimento ([28]). 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 sia stabilito nel SEE e dichiari espressamente nel contratto che i dati non saranno in alcun modo elaborati in paesi terzi.

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 ([29]).

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) ([30]).

18. La Commissione europea pubblica l'elenco delle decisioni di adeguatezza sul suo sito web ([31]).

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** ([32]). Tuttavia, dovete comunque controllare se le decisioni di adeguatezza pertinenti per detti trasferimenti sono revocate o invalidate ([33]).

([28]) 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.
([29]) 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.
([30]) Articolo 45, paragrafo 1, del RGPD.
([31]) https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
([32]) 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.
([33]) 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)].

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 ([34]).

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 ([35]).

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.

([34]) 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 assenza di una valida base giuridica 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.
([35]) Causa C-362/14 (Schrems I).

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 ([36]).

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, potrebbe essere comunque possibile trasferire dati personali in base a una delle deroghe elencate all'articolo 49 del RGPD.

25. Tale articolo ha carattere eccezionale e le deroghe in esso previste devono essere interpretate in modo da non contraddire la loro stessa natura, trattandosi di eccezioni alla regola secondo cui i dati personali non possono essere trasferiti verso un paese terzo, a meno che tale paese non preveda un livello adeguato di protezione dei dati o, in alternativa, non siano messe in atto garanzie adeguate. Le eccezioni non possono diventare «la regola» nella pratica, ma devono essere limitate a situazioni specifiche. L'EDPB ha emanato le linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679. [37]

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. Lo strumento di trasferimento selezionato di cui all'articolo 46 del RGPD deve essere efficace nel garantire che il livello di protezione assicurato dal RGPD non sia pregiudicato dal trasferimento nella pratica ([38]).

29. In particolare, la protezione dei dati personali trasferiti nel paese terzo deve essere sostanzialmente equivalente a quella garantita nel SEE dal RGPD, letto alla luce della Carta dei diritti fondamentali dell'UE ([39]). 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

([36]) C-311/18 (Schrems II), paragrafi 130 e 133. Vedere anche la sottosezione 2.3 in appresso.
([37]) Per ulteriori indicazioni in merito cfr. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_it.
([38]) Articolo 44 del RGPD e C-311/18 (Schrems II), paragrafi 126, 137 e 148.
([39]) C-311/18 (Schrems II), paragrafi 105 e seconda conclusione.

del RGPD a causa della legislazione e delle prassi del paese terzo applicabili al trasferimento, anche durante il transito dei dati dall'esportatore al paese dell'importatore ([40]).

30. È necessario prima di tutto valutare, se del caso in collaborazione con l'importatore, se vi siano elementi nel diritto e/o nelle prassi vigenti ([41]) nel paese terzo che possano incidere sull'efficacia delle garanzie adeguate offerte dallo strumento di trasferimento di cui all'articolo 46 del RGPD su cui si fa affidamento, nel contesto dello specifico trasferimento. Ciò comporta l'esigenza di determinare se il trasferimento in questione rientri o meno nell'ambito di applicazione della legislazione e/o delle prassi che potrebbero incidere sull'efficacia dello strumento di trasferimento utilizzato di cui all'articolo 46 del RGPD. La valutazione richiesta deve basarsi innanzitutto sulla legislazione disponibile al pubblico.

31. Questa valutazione deve contenere elementi riguardanti l'accesso ai dati da parte delle autorità pubbliche del paese terzo del vostro importatore, quali ad esempio:

    - elementi relativi alla possibilità o meno, per le autorità pubbliche del paese terzo del vostro importatore, di tentare di accedere ai dati, indipendentemente dal fatto che tale accesso sia effettuato con o senza la consapevolezza dell'importatore, alla luce della legislazione, della prassi e dei precedenti segnalati;
    - elementi relativi alla capacità o meno, per le autorità pubbliche del paese terzo del vostro importatore, di accedere ai dati attraverso l'importatore stesso o attraverso i fornitori di telecomunicazioni o i canali di comunicazione, alla luce dei poteri giuridici e delle risorse tecniche, finanziarie e umane a loro disposizione e dei precedenti segnalati.

Individuazione di legislazione e prassi pertinenti alla luce di tutte le circostanze del trasferimento

32. Occorre esaminare le caratteristiche di ciascun trasferimento e determinare se l'ordinamento giuridico nazionale e/o le prassi vigenti del paese verso cui i dati vengono trasferiti (o successivamente trasferiti) influiscano sui vostri trasferimenti. L'ambito della vostra valutazione è pertanto limitato alla legislazione e alle prassi pertinenti per la protezione dei dati specificamente trasferiti, a differenza di quanto avviene con le valutazioni di adeguatezza generali e di ampia portata svolte dalla Commissione europea in conformità dell'articolo 45 del RGPD.

33. Il contesto giuridico e/o le prassi applicabili dipenderanno dalle circostanze specifiche del vostro trasferimento, in particolare dai seguenti elementi:

    - finalità per le quali i dati vengono trasferiti ed elaborati (ad esempio marketing, risorse umane, archiviazione, supporto informatico, test clinici);
    - natura dei soggetti coinvolti nel trattamento (pubblica/privata; titolare del trattamento/responsabile del trattamento);
    - settore in cui avviene il trasferimento (ad esempio adtech, telecomunicazioni, finanziario, ecc.);

([40]) Cfr. C-311/18 (Schrems II), paragrafo 183 in combinato disposto con il paragrafo 184.
([41]) Cfr. il paragrafo 126 della sentenza C-311/18 (Schrems II), in cui la Corte allude espressamente al «diritto e [a]lle prassi vigenti nel paese terzo interessato» e richiede di «[...] garantire, in pratica, la protezione effettiva dei dati personali trasferiti nel paese terzo interessato» (sottolineatura aggiunta), e il paragrafo 158.

- 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) ([42]);
- conservazione dei dati nel paese terzo o accesso remoto ai dati conservati all'interno dell'UE/SEE;
- formato dei dati da trasferire (ad esempio in chiaro/pseudonimizzati o cifrati) ([43]);
- possibilità che i dati siano soggetti a trasferimenti successivi dal paese terzo verso un altro paese terzo ([44]).

34. La valutazione deve prendere in considerazione tutti i soggetti 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. Quanto maggiore è il numero dei titolari del trattamento, dei responsabili del trattamento o degli importatori coinvolti, tanto più complessa sarà la valutazione, nella quale occorre anche tener conto di eventuali trasferimenti successivi previsti.

35. Dovreste in ogni caso prestare particolare attenzione a tutte le normative pertinenti, in particolare quelle che stabiliscono i requisiti per la comunicazione dei dati personali alle autorità pubbliche o che conferiscono a tali autorità poteri di accesso ai dati personali (ad esempio in applicazione del diritto penale, per la vigilanza prevista dalle norme o per scopi di sicurezza nazionale). Se tali requisiti o poteri limitano i diritti fondamentali degli interessati, pur rispettando la loro essenza ed essendo necessari e proporzionati in una società democratica per salvaguardare importanti obiettivi riconosciuti anche nel diritto dell'Unione e degli Stati membri dell'UE ([45]), non possono pregiudicare gli impegni previsti dallo strumento di trasferimento di cui all'articolo 46 del RGPD su cui si fa affidamento.

36. Dovrete valutare le norme e le prassi 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.

37. Nell'effettuare tale valutazione, sono pertinenti anche diversi aspetti dell'ordinamento giuridico di tale paese terzo, quali gli elementi elencati all'articolo 45, paragrafo 2, del RGPD. Ad esempio, la situazione dello stato di diritto in un paese terzo può essere pertinente per valutare l'efficacia

---

([42]) Un trasferimento di dati personali è un'operazione di trattamento (articolo 4, paragrafo 2, RGPD). Se desiderate trasferire dati sensibili contemplati dall'ambito di applicazione degli articoli 9 e 10 del RGPD, potete effettuare un trasferimento solo se rientra nell'ambito di una delle deroghe e delle condizioni previste dagli articoli 9 e 10 del RGPD e dal diritto degli Stati membri dell'UE. Ai sensi dell'articolo 32 del RGPD, dovrete inoltre mettere in atto, con l'importatore che agisce in qualità di titolare del trattamento o responsabile del trattamento, misure tecniche e organizzative opportune per garantire un livello di sicurezza adeguato ai rischi per i diritti e le libertà degli interessati, costituiti da una potenziale violazione dei dati personali trasferiti (articolo 4, paragrafo 12, RGPD). Le categorie di dati trasferiti e la loro sensibilità saranno pertinenti per la valutazione del rischio e l'adeguatezza delle misure.
([43]) Alcuni paesi terzi non consentono l'importazione di dati cifrati.
([44]) Qualora il titolare del trattamento abbia rilasciato la previa autorizzazione scritta, specifica o generale, ai sensi dell'articolo 28, paragrafo 2, del RGPD.
([45]) 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.

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 di ampio respiro 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.

38. Gli obblighi o i poteri derivanti da tali leggi e prassi saranno ritenuti in contrasto/incompatibili con gli impegni previsti dallo strumento di trasferimento di cui all'articolo 46 del RGPD qualora ([46]):

    - non rispettino l'essenza dei diritti e delle libertà fondamentali della Carta dei diritti fondamentali dell'UE; oppure

    - vadano oltre quanto necessario e proporzionato in una società democratica per salvaguardare uno degli obiettivi importanti riconosciuti anche dal diritto dell'Unione e degli Stati membri, come quelli di cui all'articolo 23, paragrafo 1, del RGPD.

39. Dovreste verificare che gli impegni dell'importatore di dati che consentono agli interessati di esercitare i loro diritti, come previsti dallo strumento di trasferimento di cui all'articolo 46 del RGPD [quali le richieste di accesso, rettifica e cancellazione dei dati trasferiti, nonché l'esistenza di mezzi di ricorso (in sede giudiziale)], trovino effettiva applicazione nella pratica e non siano ostacolati dal diritto e/o dalle prassi del paese terzo di destinazione.

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

41. Le raccomandazioni dell'EDPB relative alle garanzie essenziali europee ([47]) chiariscono gli 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 ([48]) 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. Il primo requisito delle garanzie essenziali europee è la presenza di un quadro giuridico che contempli tale accesso, ove previsto, che sia disponibile al pubblico e sufficientemente chiaro.

42. Applicate ai trasferimenti di dati basati sugli strumenti di cui all'articolo 46, le raccomandazioni dell'EDPB relative alle garanzie essenziali europee possono guidare l'esportatore di dati nel valutare se i poteri in questione interferiscono in modo ingiustificato con gli obblighi dell'esportatore e dell'importatore di garantire la sostanziale equivalenza ai sensi del RGPD o conformemente agli impegni previsti dallo strumento di trasferimento. L'insussistenza di un livello di protezione sostanzialmente equivalente sarà particolarmente evidente laddove la legislazione

---

([46]) Si vedano gli articoli 47 e 52 della Carta dei diritti fondamentali dell'Unione europea, l'articolo 23, paragrafo 1, del RGPD, C-311/18 (Schrems II), paragrafi 174 e 187, e le raccomandazioni 02/2020 dell'EDPB, del 10 novembre 2020, relative alle garanzie essenziali europee per le misure di sorveglianza.

[47] EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10 November 2020.

([48]) E quindi non in contrasto con gli impegni assunti con lo strumento di trasferimento di cui all'articolo 46 del RGPD.

e/o le prassi del paese terzo interessato dal trasferimento non soddisfino i requisiti delle garanzie essenziali europee. L'EDPB ribadisce che le garanzie essenziali europee sono uno standard di riferimento per valutare l'ingerenza che le misure di sorveglianza di paesi terzi comportano nel contesto dei trasferimenti internazionali di dati. Tali standard derivano dal diritto dell'UE e dalla giurisprudenza della CGUE e della Corte CEDU, che è vincolante per gli Stati membri dell'UE.

43. La vostra valutazione deve basarsi innanzitutto sulla legislazione disponibile al pubblico. Inoltre, l'esame delle prassi delle autorità pubbliche di paesi terzi vi permetterà di verificare se le garanzie adeguate contenute nello strumento di trasferimento di cui all'articolo 46 del RGPD possano essere sufficienti a garantire, in concreto, la protezione efficace dei dati personali trasferiti ([49]). L'esame delle prassi vigenti nel paese terzo sarà particolarmente importante ai fini della vostra valutazione nelle situazioni descritte di seguito.

43.1 **La legislazione pertinente nel paese terzo potrebbe essere formalmente allineata alle norme dell'UE in materia di diritti e libertà fondamentali, nonché alla necessità e alla proporzionalità delle restrizioni ivi contemplate.** Tuttavia, le prassi delle autorità pubbliche di tale paese terzo (per esempio nell'accedere a dati personali detenuti da soggetti privati o nell'attuare o meno la legislazione in quanto organismi di controllo o giudiziari) potrebbero chiaramente indicare che non applicano legislazione che disciplina, in linea di principio, le loro attività o non si conformano a tale legislazione. In questo caso, dovete tenere conto di tali prassi nella vostra valutazione e considerare che lo strumento di cui all'articolo 46 del RGPD non sarà in grado di garantire efficacemente, di per sé (ossia in assenza di misure supplementari), un livello di protezione sostanzialmente equivalente. In tal caso, se desiderate procedere con il trasferimento, dovrete mettere in atto misure supplementari adeguate.

43.2 **Nel paese terzo potrebbe mancare legislazione pertinente (per esempio in materia di accesso a dati personali detenuti dal settore privato).** In questo caso non potete concludere automaticamente sulla base di tale assenza che il vostro strumento di trasferimento di cui all'articolo 46 del RGPD possa essere efficacemente applicato. Dovrete verificare l'eventuale presenza di indicazioni di prassi vigenti nel paese che sono incompatibili con il diritto dell'UE e con gli impegni previsti dallo strumento di trasferimento di cui all'articolo 46 del RGPD. Se esistono prassi incompatibili, lo strumento di trasferimento di cui all'articolo 46 del RGPD non potrà garantire efficacemente, di per sé (ossia in assenza di misure supplementari), un livello di protezione sostanzialmente equivalente. In tal caso, se desiderate procedere con il trasferimento, dovrete mettere in atto misure supplementari adeguate.

([49]) C-311/18 (Schrems II), paragrafo 126.

43.3 **Dalla valutazione può emergere che la legislazione pertinente nel paese terzo potrebbe essere problematica ([50]) e che i dati trasferiti e/o l'importatore in questione rientrano o possono rientrare nell'ambito di applicazione di tale legislazione problematica ([51]).**

Considerando le incertezze relative alla potenziale applicazione al vostro trasferimento di una legislazione problematica, potete quindi decidere di:

- sospendere il trasferimento;
- mettere in atto misure supplementari ([52]) per prevenire il rischio che possano essere applicate, nei confronti del vostro importatore e/o dei vostri dati trasferiti, norme e/o prassi del paese terzo dell'importatore di dati che siano atte a pregiudicare le garanzie contrattuali, previste dallo strumento di trasferimento, di un livello di protezione sostanzialmente equivalente a quella garantita nel SEE; oppure
- in alternativa, potete decidere di procedere con il trasferimento senza la necessità di mettere in atto misure supplementari, se ritenete di non avere motivo di credere che la legislazione problematica pertinente verrà applicata, in concreto, nei confronti dei vostri dati trasferiti e/o dell'importatore. Dovrete avere dimostrato e documentato, mediante la vostra valutazione, ove opportuno in collaborazione con l'importatore, che la normativa non viene interpretata e/o applicata nella pratica in modo tale da riguardare i dati trasferiti e l'importatore, tenendo inoltre conto dell'esperienza di altri soggetti che operano nello stesso settore e/o in relazione a dati personali trasferiti di natura analoga, nonché delle altre fonti di informazioni descritte qui di seguito ([53]).

  Pertanto, sarà necessario che abbiate dimostrato e documentato con una relazione dettagliata ([54]) che la legislazione problematica non troverà applicazione in concreto nei confronti dei dati trasferiti e/o dell'importatore e che, di conseguenza, non impedirà all'importatore di assolvere gli obblighi previsti dallo strumento di trasferimento di cui all'articolo 46 del RGPD ([55]).

([50]) Per «legislazione problematica» si intende una legislazione che 1) impone obblighi sul destinatario del trasferimento di dati personali provenienti dall'Unione europea e/o influisce sui dati trasferiti in modo tale da poter pregiudicare la garanzia contrattuale, prevista dagli strumenti di riferimento, di un livello di protezione sostanzialmente equivalente e 2) non rispetta l'essenza dei diritti e delle libertà fondamentali riconosciuti dalla Carta dei diritti fondamentali dell'UE o va al di là di quanto necessario e proporzionato in una società democratica per salvaguardare uno degli obiettivi importanti riconosciuti anche dal diritto dell'Unione o degli Stati membri dell'UE, come quelli di cui all'articolo 23, paragrafo 1, del RGPD.

([51]) Potrebbe non essere chiaro se l'importatore e/o i dati trasferiti rientrino o meno nell'ambito di applicazione delle disposizioni formulate spesso in termini generali nella normativa nazionale in materia di sicurezza , quali ad esempio «fornitore di servizi di comunicazioni elettroniche» e «informazioni di intelligence esterna».

([52]) Cfr. considerando 109 del RGPD e C-311/18 (Schrems II), paragrafo 132.

([53]) Cfr. punti da 45 a 47.

([54]) Le relazioni che redigerete dovranno includere informazioni esaustive sulla valutazione giuridica della legislazione e delle prassi, nonché della loro applicazione ai trasferimenti specifici, la procedura interna impiegata per eseguire la valutazione (ivi comprese informazioni sugli attori in essa coinvolti: per esempio studi legali, consulenti o servizi interni) e le date delle verifiche. Le relazioni dovrebbero essere approvate dal legale rappresentante dell'esportatore.

([55]) L'avvenuta dimostrazione della non applicabilità della legislazione problematica, in concreto, ai dati trasferiti e all'importatore, anche tenendo conto dell'esperienza di altri soggetti che operano nello stesso settore e/o in

Possibili fonti di informazioni

44. L'importatore di dati dovrebbe fornirvi le fonti e le informazioni pertinenti relative al paese terzo in cui è stabilito e alle leggi e alle prassi vigenti applicabili al trasferimento.

45. Voi e l'importatore potete completare la vostra valutazione con informazioni ottenute da fonti come quelle elencate a titolo esemplificativo nell'allegato 3.

46. Oltre al quadro giuridico del paese terzo applicabile al trasferimento, le fonti e le informazioni devono essere pertinenti, oggettive, attendibili, verificabili e disponibili al pubblico o altrimenti accessibili per determinare se il vostro strumento di trasferimento di cui all'articolo 46 possa essere effettivamente applicato ([56]) e dovrete valutare e documentare che siano tali.

Pertinenti: le informazioni devono essere pertinenti per il trasferimento specifico e/o l'importatore, nonché per la loro conformità ai requisiti previsti dal diritto dell'UE e dallo strumento di trasferimento di cui all'articolo 46 del RGPD, senza essere eccessivamente generiche o astratte.

Informazioni oggettive: sono informazioni suffragate da prove empiriche basate sulle conoscenze acquisite in passato, e non ipotesi su eventi e rischi potenziali.

Attendibili: l'esportatore e l'importatore devono valutare obiettivamente l'attendibilità della fonte di informazioni e delle informazioni stesse, oltre a valutarle separatamente.

Verificabili: le informazioni e le conclusioni dovrebbero essere verificabili o confrontabili con altri tipi di informazioni o fonti, nel quadro di una valutazione generale, per consentire inoltre all'autorità di controllo o giudiziaria competente di verificare l'oggettività e l'attendibilità di tali informazioni, se necessario.

Informazioni disponibili al pubblico o altrimenti accessibili: le informazioni dovrebbero preferibilmente essere pubbliche o almeno accessibili per facilitare la verifica dei criteri di cui sopra e garantire la possibilità di condividerli con autorità di controllo, autorità giudiziarie e, in ultima analisi, con gli interessati.

47. Potreste tenere conto altresì dell'esperienza documentata dell'importatore con riguardo a casi precedenti e pertinenti di richieste di accesso pervenute da autorità pubbliche nel paese terzo. Potrete avvalervi dell'esperienza dell'importatore in quanto fonte ulteriore di informazioni solo se il quadro giuridico del paese terzo non vieta all'importatore di fornire informazioni su richieste di comunicazione da parte di autorità pubbliche o sull'assenza di tali richieste (e dovreste anche documentare tale valutazione). Occorre comunque considerare che l'assenza di casi precedenti di richieste ricevute dall'importatore non può mai essere ritenuta, di per sé, un fattore decisivo in

relazione a dati personali trasferiti di natura analoga, non vi esenta dal prevedere le misure supplementari necessarie per proteggere i dati personali durante la loro trasmissione e il trattamento nel paese terzo di destinazione (per esempio la cifratura end-to-end dei dati; cfr. gli esempi di misure tecniche supplementari nell'allegato 2) se la vostra analisi della legislazione applicabile del paese terzo di destinazione indica che l'accesso ai dati potrebbe verificarsi, anche in assenza dell'intervento dell'importatore, in questa fase del trasferimento. È possibile che abbiate già previsto tali misure con l'importatore che agisce in qualità di titolare del trattamento o responsabile del trattamento, ai sensi dell'articolo 32 del RGPD.

([56]) Cfr. l'allegato 3 per un elenco non esaustivo di fonti di informazioni che voi e l'importatore potreste utilizzare.

merito all'efficacia dello strumento di trasferimento di cui all'articolo 46 del RGPD, tale da consentire di procedere con il trasferimento senza adottare misure supplementari. Potrete prendere in considerazione queste informazioni, unitamente ad altre categorie di informazioni ottenute da altre fonti, nell'ambito della vostra valutazione generale delle norme e delle prassi del paese terzo in relazione al vostro trasferimento. L'esperienza pertinente e documentata dell'importatore dovrebbe essere corroborata, e non contraddetta, da informazioni pertinenti, oggettive, attendibili, verificabili e disponibili al pubblico o altrimenti accessibili sull'applicazione pratica della normativa pertinente (per esempio sull'esistenza o sull'assenza di richieste di accesso ricevute da altri soggetti che operano nello stesso settore e/o in relazione a dati personali trasferiti di natura analoga ([57]) e/o in merito all'applicazione concreta della normativa, ad esempio giurisprudenza e relazioni a cura di organi di vigilanza indipendenti).

Risultati della vostra valutazione

48. Dovete condurre questa valutazione generale della legislazione e delle prassi del paese terzo del vostro importatore, applicabili al trasferimento, con la dovuta diligenza e documentarla accuratamente. Le vostre autorità di controllo e/o giudiziarie competenti potrebbero richiederla e ritenervi responsabili per qualsiasi decisione da voi presa su tale base ([58]).

49. La vostra valutazione può in ultima analisi indicare che lo strumento di trasferimento di cui all'articolo 46 del RGPD su cui fate affidamento:

    - garantisce in modo efficace che i dati personali trasferiti godano nel paese terzo di un livello di protezione sostanzialmente equivalente a quello garantito nel SEE. La legislazione e le prassi del paese terzo applicabili al trasferimento permettono all'importatore di dati di rispettare gli obblighi previsti dallo strumento di trasferimento prescelto. Dovreste procedere a una nuova valutazione a intervalli adeguati o quando emergono cambiamenti significativi (cfr. sesto passo); oppure

    - non garantisce in modo efficace un livello di protezione sostanzialmente equivalente. L'importatore di dati non può adempiere i suoi obblighi, a causa della legislazione e/o delle prassi del paese terzo applicabili al trasferimento che non sono conformi alle norme dell'UE in materia di diritti e libertà fondamentali e alla necessità e proporzionalità delle restrizioni ivi contemplate per salvaguardare obiettivi legittimi di pubblico interesse. 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 ([59]).

Esempio:

<u>Contesto</u>

([57]) L'esperienza potrebbe essere quella di altri soggetti a voi noti direttamente per via di trasferimenti precedenti dello stesso tipo da voi effettuati, o quella riferita nella giurisprudenza pertinente, in relazioni a cura di ONG, ecc. (cfr. allegato 3).
([58]) Articolo 5, paragrafo 2, del RGPD.
([59]) C-311/18 (Schrems II), paragrafi 134 e 135.

La CGUE ha ritenuto che l'articolo 702 del Foreign Intelligence Surveillance Act (FISA) statunitense non rispetti le garanzie minime derivanti dal principio di proporzionalità ai sensi del diritto dell'Unione e non possa 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.

Valutazione

Se la valutazione della legislazione statunitense pertinente vi induce a ritenere che il vostro trasferimento possa rientrare nell'ambito di applicazione dell'articolo 702 della FISA, ma non siete certi che rientri in concreto nel suo campo di applicazione, potete decidere di:

1. interrompere il trasferimento;
2. adottare misure supplementari adeguate che garantiscano in modo efficace un livello di protezione per i dati trasferiti sostanzialmente equivalente a quello garantito nel SEE; oppure
3. considerare altre informazioni oggettive, attendibili, pertinenti, verificabili e preferibilmente disponibili al pubblico (comprese eventualmente informazioni che vi ha fornito l'importatore di dati) per precisare in concreto il campo di applicazione dell'articolo 702 della FISA nei confronti del vostro trasferimento. Queste informazioni dovrebbero fornire risposte ad alcune domande pertinenti, quali:

- le informazioni disponibili al pubblico dimostrano l'esistenza di un divieto legale di fornire informazioni su una specifica richiesta di accesso a dati ricevuti e la presenza di ampie limitazioni alla possibilità di fornire informazioni generali su richieste di accesso a dati ricevuti o sull'assenza di tali richieste?

- L'importatore di dati ha confermato di avere ricevuto in passato richieste di accesso ai dati da parte di autorità pubbliche statunitensi? Oppure l'importatore di dati ha confermato di non avere ricevuto in passato richieste di accesso ai dati da parte di autorità pubbliche statunitensi e che gli è consentito fornire informazioni su tali richieste o sulla loro assenza?

- Le informazioni disponibili al pubblico ottenute sulla giurisprudenza statunitense e sulle relazioni a cura di organi di vigilanza, organizzazioni della società civile e istituzioni accademiche ([60]) indicano che importatori di dati operanti nello stesso settore del vostro importatore hanno ricevuto in passato richieste di accesso a dati trasferiti di natura analoga?

Le risposte a queste domande, da voi ottenute per mezzo della valutazione generale, vi inducono a concludere che:

- l'articolo 702 della FISA si applica in concreto al vostro trasferimento e, pertanto, incide sull'efficacia del vostro strumento di trasferimento di cui all'articolo 46 del RGPD. Di conseguenza, se desiderate procedere con il trasferimento, dovete valutare, ove opportuno in collaborazione con l'importatore, la possibilità di adottare misure supplementari che garantiscano in modo efficace un livello di protezione per i dati trasferiti sostanzialmente equivalente a quello garantito nel SEE. Qualora non possiate individuare misure supplementari efficaci, non dovete trasferire i dati personali;

([60]) Per esempio disposizioni dell'articolo 702 della FISA, norme procedurali della Foreign Intelligence Surveillance Court (FISC), decisioni e pareri declassificati della FISC; giurisprudenza dei tribunali statunitensi; relazioni e trascrizioni di udienze dell'Autorità per la tutela della vita privata e delle libertà civili (Privacy and Civil Liberties Oversight Board, PCLOB); relazioni a cura dell'Ispettorato generale - Dipartimento della Giustizia statunitense; relazioni del direttore dell'Ufficio per la tutela della vita privata e delle libertà civili dell'NSA; relazioni a cura del Servizio di ricerca del Congresso; relazioni a cura dell'American Civil Liberties Union Foundation (ACLU).

oppure
- l'articolo 702 della FISA non si applica in concreto al vostro trasferimento e, pertanto, non incide sull'efficacia del vostro strumento di trasferimento di cui all'articolo 46 del RGPD. Potete quindi procedere con il trasferimento senza adottare misure supplementari.

2.4 Quarto passo: adozione di misure supplementari

50. Se la valutazione di cui al terzo passo ha indicato che lo strumento di trasferimento di cui all'articolo 46 del RGPD 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 protezione sostanzialmente equivalente a quello garantito all'interno dell'UE ([61]). Le «misure supplementari» integrano per definizione le garanzie già previste dallo strumento di trasferimento di cui all'articolo 46 del RGPD e qualsiasi altro requisito di sicurezza applicabile (per esempio misure tecniche di sicurezza) previste dal RGPD ([62]).

51. Dovete individuare caso per caso quali misure supplementari potrebbero essere efficaci per i trasferimenti verso un determinato paese terzo quando utilizzate uno specifico strumento di trasferimento di cui all'articolo 46 del RGPD. Non è necessario che ripetiate la valutazione ogni volta che effettuate lo stesso trasferimento di una specifica tipologia di dati verso lo stesso paese terzo. Alcuni dei dati per cui è previsto il trasferimento potrebbero richiedere misure supplementari, mentre per altri dati ciò potrebbe non essere necessario (considerando l'applicazione formale e/o concreta della legislazione del paese terzo). Potrete basarvi sulle precedenti valutazioni e conclusioni 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.

52. In linea di principio, le misure supplementari possono avere carattere contrattuale, tecnico o organizzativo. La combinazione di misure diverse che si integrino e supportino a vicenda può migliorare il livello di protezione e può quindi contribuire a raggiungere gli standard dell'Unione.

53. 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 in forza di una legislazione e/o di prassi problematiche ([63]). Vi saranno infatti situazioni in cui solo misure tecniche adeguatamente attuate potrebbero impedire o rendere inefficace l'accesso ai dati personali da parte delle autorità pubbliche dei paesi terzi, in particolare a fini di sorveglianza ([64]). In tali situazioni, le misure

([61]) C-311/18 (Schrems II), paragrafo 96.
([62]) Considerando 109 del RGPD e C-311/18 (Schrems II), paragrafo 133.
([63]) Per «legislazione problematica» si intende una legislazione che 1) impone obblighi sul destinatario del trasferimento di dati personali provenienti dall'Unione europea e/o influisce sui dati trasferiti in modo tale da poter pregiudicare la garanzia contrattuale, prevista dagli strumenti di riferimento, di un livello di protezione sostanzialmente equivalente e 2) non rispetta l'essenza dei diritti e delle libertà fondamentali riconosciuti dalla Carta dei diritti fondamentali dell'UE o va al di là di quanto necessario e proporzionato in una società democratica per salvaguardare uno degli obiettivi importanti riconosciuti anche dal diritto dell'Unione o degli Stati membri dell'UE, come quelli di cui all'articolo 23, paragrafo 1, del RGPD.
([64]) 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

contrattuali o organizzative possono integrare le misure tecniche e rafforzare il livello generale di protezione dei dati, ad esempio introducendo controlli ed eliminando automatismi in relazione ai tentativi delle autorità pubbliche di accedere ai dati in modo non conforme alle norme dell'Unione.

54. In collaborazione con l'importatore di dati, se del caso, potete consultare il seguente elenco (non esaustivo) di fattori al fine di individuare quali misure supplementari sarebbero più efficaci per proteggere i dati trasferiti dalle richieste di accesso agli stessi da parte di autorità pubbliche in forza di una legislazione problematica applicata in concreto al trasferimento:

    - formato dei dati da trasferire (ad esempio in chiaro/dati pseudonimizzati o cifrati);
    - natura dei dati (per esempio, nel SEE le categorie di dati contemplate dagli articoli 9 e 10 del RGPD godono di un livello di protezione superiore) ([65]);
    - lunghezza e complessità della catena di trattamento dei dati, numero di soggetti coinvolti nel trattamento e rapporti intercorrenti (ad esempio se i trasferimenti coinvolgono più titolari del trattamento ovvero titolari e responsabili del trattamento, oppure se sono coinvolti responsabili del trattamento che trasferiranno i dati da voi all'importatore dei dati, considerando le relative disposizioni loro applicabili ai sensi della legislazione del paese terzo di destinazione) ([66]);
    - tecnica o parametri dell'applicazione pratica nel paese terzo riscontrati nel corso del terzo passo;
    - 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 sub-responsabili del trattamento dell'importatore dei dati) ([67]).

Esempi di misure supplementari

55. Alcuni esempi di misure tecniche, contrattuali e organizzative che potrebbero essere prese in considerazione, ove non siano già incluse nello strumento di trasferimento utilizzato di cui all'articolo 46 del RGPD, sono disponibili negli elenchi non esaustivi di cui all'allegato 2.

***

56. 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, potete procedere con i vostri trasferimenti.

---

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.

([65]) Cfr. nota 42.

([66]) Il RGPD attribuisce obblighi distinti ai titolari del trattamento e ai responsabili del trattamento. I trasferimenti possono avvenire da titolare del trattamento a titolare del trattamento, tra co-titolari del trattamento, 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.

([67]) Cfr. nota 26.

57. Qualora non siate in grado di individuare o attuare misure supplementari efficaci che garantiscano che i dati personali trasferiti godano di un livello di protezione sostanzialmente equivalente ([68]), non dovete iniziare a trasferire i dati personali verso il 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 ([69]). 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 ([70]).

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.

58. L'autorità di controllo competente può imporre 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

59. 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)

60. 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 ([71]). L'esportatore e l'importatore di dati devono garantire che le clausole

([68]) 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.
([69]) C-311/18 (Schrems II), paragrafo 135.
([70]) Cfr. per esempio la clausola 12 nell'allegato alla decisione 87/2010 sulle clausole contrattuali tipo; cfr. la clausola di risoluzione (facoltativa) nell'allegato B della decisione 2004/915/CE sulle clausole contrattuali tipo.
([71]) 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

aggiuntive non possano essere interpretate in alcun modo che comporti limitazioni dei diritti e degli obblighi previsti dalle clausole contrattuali tipo o che comunque riduca il livello di protezione dei dati. Dovete essere in grado di dimostrare quanto sopra, compresa l'inequivocabilità di tutte le clausole, ai sensi del principio di responsabilizzazione e dell'obbligo di fornire un livello sufficiente di protezione dei dati. Le autorità di controllo competenti hanno il potere di esaminare tali clausole supplementari se necessario (ad esempio in caso di reclamo o a seguito di indagine d'ufficio).

61. Qualora intendiate modificare le clausole tipo di protezione dei dati o qualora le misure supplementari aggiunte «contraddicano» direttamente o indirettamente le clausole contrattuali tipo, si riterrà che non vi facciate più affidamento ([72]) e dovrete chiedere un'autorizzazione all'autorità di controllo competente ai sensi dell'articolo 46, paragrafo 3, lettera a), del RGPD.

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

62. 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 ([73]).

63. La sentenza Schrems II è rilevante per i trasferimenti di dati personali sulla base di norme vincolanti d'impresa (BCR), poiché le normative di paesi terzi possono influire sulla protezione fornita da tali strumenti.

64. Tutti gli impegni che devono essere inclusi saranno riportati nei criteri di riferimento WP256/257 aggiornati ([74]) cui tutti i gruppi facenti affidamento su BCR ai fini dei trasferimenti di dati dovranno allineare le loro BCR vigenti e future.

65. 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

---

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.» Disposizioni simili sono previste negli insiemi di clausole contrattuali tipo adottate dalla Commissione europea ai sensi della direttiva 95/45/CE.

([72]) 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_en.pdf.

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

([74]) 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, da ultimo riveduto e approvato 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.

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)

66. 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 ([75]). La sentenza Schrems II è dunque rilevante per i trasferimenti di dati personali sulla base di clausole contrattuali ad hoc, poiché le normative di paesi terzi possono influire sulla protezione fornita da tali strumenti.

2.6 Sesto passo: rivalutare a intervalli appropriati

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

68. 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.

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

3 CONCLUSIONI

69. Il RGPD stabilisce norme sul trattamento dei dati personali nel SEE e, in tal senso, 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 ([76]).

70. 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 trattati.

71. 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 il diritto o le prassi del paese terzo di destinazione pregiudicano (oppure no) le garanzie previste dallo strumento di trasferimento di cui all'articolo 46 del RGPD nel contesto dei vostri trasferimenti. Se lo strumento di trasferimento di cui all'articolo 46 del RGPD non riesce a garantire, di per sé, un livello di protezione sostanzialmente equivalente per i dati personali da voi trasferiti, misure supplementari possono colmare la lacuna.

72. Qualora non siate in grado di individuare o attuare misure supplementari efficaci che garantiscano che i dati personali trasferiti beneficino 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 prescelto. Se state già effettuando trasferimenti, siete tenuti a sospendere o a porre fine prontamente al trasferimento dei dati personali.

73. 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)

([76]) 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 standard 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 dell'articolo 46, paragrafo 5, del RGPD.

ALLEGATO 2: ESEMPI DI MISURE SUPPLEMENTARI

74. Le seguenti misure sono esempi di misure supplementari che è possibile prendere in considerazione quando si renda necessario (v. quarto passo) «adottare misure supplementari». L'elenco presentato non è esaustivo, ed è possibile prendere in considerazione altre misure supplementari. Sviluppi tecnologici, giuridici od organizzativi futuri potrebbero comportare la necessità di valutare nuove misure supplementari. La selezione e l'implementazione 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.

75. Qualsiasi misura supplementare può essere considerata efficace ai sensi della sentenza della CGUE «Schrems II» solo se e nella misura in cui, di per sé o in combinazione con altre, affronta le specifiche carenze individuate nella valutazione della situazione del paese terzo per quanto riguarda il diritto e le prassi di tale paese applicabili al vostro trasferimento. Se, in ultima analisi, non riuscite a garantire un livello di protezione sostanzialmente equivalente, non dovete trasferire i dati personali.

76. In qualità di titolari o di responsabili del trattamento, potreste essere già tenuti ad attuare alcune delle misure descritte nel presente allegato, ai fini della conformità al RGPD. Ciò implica la possibilità di mettere in atto misure analoghe per i dati personali trattati nel SEE che siano trasferiti a un importatore di dati coperto da una decisione di adeguatezza o verso altri paesi terzi ([77]).

2.1 Misure tecniche

77. 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 assicurare 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 ([78]).

78. Per maggiore chiarezza, questa sezione descrive in primo luogo esempi di scenari in cui determinate misure tecniche potrebbero essere efficaci per garantire un livello di protezione sostanzialmente equivalente. La sezione prosegue con alcuni scenari per i quali non sono individuate le misure tecniche atte a garantire tale livello di protezione.

([77]) Articolo 5, paragrafo 2, e articolo 32, del RGPD.
([78]) C-311/18 (Schrems II), paragrafo 135.

Esempi di scenari relativi a casi per i quali sono individuate misure *efficaci*

79. 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 sarebbero necessarie per assicurare un livello di protezione sostanzialmente equivalente a quello garantito nel SEE, anche se l'accesso delle autorità pubbliche è conforme alla legge del paese dell'importatore, qualora, in concreto, tale accesso vada al di là di quanto necessario e proporzionato in una società democratica ([79]). Le misure hanno lo scopo di impedire l'accesso potenzialmente illecito impedendo alle autorità di identificare gli interessati, di dedurre informazioni che li riguardano, di individuarli in un altro contesto o di associare i dati trasferiti ad altri insiemi di dati che possono contenere, tra l'altro, identificatori online forniti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati dagli interessati in altri contesti.

80. 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 nel 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 direttamente alle strutture di trattamento o chiedendo al destinatario dei dati di localizzarli, estrarre i dati di interesse e consegnarli alle autorità.

81. In questa sezione vengono presi in considerazione gli scenari in cui vengono applicate misure efficaci in entrambi i casi. L'applicazione di misure supplementari di diverso genere può risultare sufficiente nelle circostanze specifiche di un determinato trasferimento se la legislazione 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.

82. Gli scenari descrivono circostanze specifiche e le misure adottate a titolo di esempio. Qualsiasi modifica degli scenari può portare a conclusioni diverse. Gli scenari si riferiscono a situazioni in cui si è concluso preliminarmente che occorrono misure supplementari, vale a dire situazioni ove,

([79]) 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.

in concreto, la legislazione problematica del paese terzo venga applicata al trasferimento in questione.

83. I titolari del trattamento possono essere tenuti ad applicare alcune o la totalità delle misure qui descritte indipendentemente dal livello di protezione previsto dalle norme 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, nello stesso modo in cui titolari e 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

84. 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 crittografia forte prima della trasmissione e l'identità dell'importatore è verificata,
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 alla crittoanalisi 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 ([80]),
3. l'efficacia della crittografia e la lunghezza della chiave tengono conto del periodo di tempo specifico durante il quale la riservatezza dei dati personali cifrati deve essere preservata ([81]),

([80]) Al fine di valutare l'efficacia degli algoritmi di cifratura, la loro conformità allo stato dell'arte e la loro solidità nel tempo rispetto alla crittoanalisi, gli esportatori di dati possono basarsi sugli orientamenti tecnici pubblicati dalle autorità ufficiali di cibersicurezza dell'UE e dei suoi Stati membri. Cfr. per esempio la relazione dell'ENISA «What is "state of the art" in IT security? », 2019, https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security; gli orientamenti forniti dall'Ufficio federale per la sicurezza delle tecniche dell'informazione nelle sue linee guida tecniche della serie TR-02102 e «Algorithms, Key Size and Protocols Report (2018), H2020-ICT-2014 – Project 645421, D5.4, ECRYPT-CSA, 02/2018» all'indirizzo https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf.

([81]) La capacità di protezione degli algoritmi crittografici è soggetta a declino nel corso del tempo per la scoperta di nuove tecniche crittoanalitiche, la comparsa di nuovi paradigmi di calcolo come l'informatica quantistica e l'aumento generale della potenza di calcolo disponibile, a meno che gli algoritmi applicati non si dimostrino teoricamente sicuri per le informazioni. Questo problema vale in particolare per gli algoritmi delle chiavi pubbliche che sono di uso comune al momento della stesura del presente documento. Di conseguenza, l'esportatore di dati deve considerare che le autorità pubbliche potrebbero impegnarsi ad accedere a dati cifrati nelle circostanze descritte al paragrafo n. 80 e archiviarli finché le loro risorse non saranno sufficienti per decifrarli. La misura supplementare può essere ritenuta efficace solo se tale decifrazione e l'ulteriore trattamento successivo non configurano più, in tale momento, una violazione dei diritti degli interessati, ad esempio perché i dati non possono più essere utilizzati per la loro identificazione diretta o indiretta.

4. l'algoritmo di cifratura è applicato correttamente da un software adeguatamente aggiornato e senza vulnerabilità note, 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) ([82]), e
6. le chiavi sono conservate esclusivamente sotto il controllo dell'esportatore di dati, o di un soggetto incaricato dall'esportatore nel SEE o in una giurisdizione che offre un livello di protezione sostanzialmente equivalente a quello garantito all'interno del SEE,

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

Caso d'uso 2: trasferimento di dati pseudonimizzati

85. 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. l'esportatore 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'impiego di informazioni aggiuntive ([83]),
2. tali informazioni aggiuntive sono detenute esclusivamente dall'esportatore di dati e conservate separatamente in uno Stato membro o in un paese terzo da un soggetto incaricato dall'esportatore nel SEE o in una giurisdizione che offre un livello di protezione sostanzialmente equivalente a quello garantito all'interno del SEE,
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 che le autorità pubbliche del paese destinatario potrebbero presumibilmente possedere e utilizzare, 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 allora che la pseudonimizzazione eseguita costituisca un'efficace misura supplementare.

([82]) Pubblicazione speciale del NIST 800-57, Raccomandazione per la gestione delle chiavi, https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final.

([83]) 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». I dati aggiuntivi possono essere costituiti da tavole in cui gli pseudonimi vengono giustapposti agli attributi identificativi che sostituiscono, chiavi crittografiche o altri parametri per la trasformazione degli attributi, oppure altri dati che permettano di attribuire i dati pseudonimizzati a persone fisiche identificate o identificabili.

86. 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 ([84]) possono consentirne l'identificazione anche se il suo nome, indirizzo o altri identificativi semplici sono omessi.

87. Ciò vale in particolare quando i dati riguardano l'utilizzo di servizi d'informazione (orario di accesso, sequenza delle funzionalità a cui è stato effettuato l'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 oggetto di attenzione.

88. Inoltre, dato che l'uso di alcuni servizi d'informazione è pubblico per natura, o che tali servizi sono utilizzabili 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 oggetto della loro attenzione.

89. Se, nel corso della pseudonimizzazione, gli attributi contenuti nei dati personali vengono trasformati per mezzo di un algoritmo crittografico, si applicano gli orientamenti di cui alle note 80 e 81. Si raccomanda quindi di rinunciare all'uso esclusivo della crittografia e di applicare le trasformazioni in base ai meccanismi di consultazione (look-up) delle tabelle.

Caso d'uso 3: cifratura dei dati per proteggerli dall'accesso delle autorità pubbliche del paese terzo dell'importatore quando transitano dall'esportatore all'importatore

90. Un esportatore di dati desidera trasferire dati verso una destinazione in cui il diritto e/o le prassi consentono l'accesso delle autorità pubbliche ai dati mentre questi ultimi transitano dal paese dell'esportatore a quello di destinazione.

    Se

    1. un esportatore di dati trasferisce i dati personali a un importatore di dati in una giurisdizione in cui il diritto e/o le prassi consentono alle autorità pubbliche di accedere ai dati mentre questi vengono trasportati su Internet verso questo paese terzo senza le garanzie essenziali europee riguardanti tale accesso, viene utilizzata la cifratura del trasporto, per la quale si garantisce che i protocolli di cifratura impiegati sono conformi allo stato dell'arte e forniscono una protezione efficace contro gli attacchi attivi e passivi con risorse notoriamente a disposizione delle autorità pubbliche del paese terzo,
    2. le parti coinvolte nella comunicazione si accordano su un'autorità o un'infrastruttura di certificazione a chiave pubblica affidabile,

([84]) Articolo 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».

3. vengono utilizzate misure specifiche di protezione conformi allo stato dell'arte contro gli attacchi attivi e passivi all'interno dei sistemi di invio e di ricezione che permettono la cifratura del trasporto, tra cui test per rilevare le vulnerabilità del software e possibili backdoor,
4. 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 conformi allo stato dell'arte,
5. 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 quando i dati sono in transito verso il paese terzo, tenendo conto delle risorse e delle capacità tecniche (ad esempio potenza di calcolo per attacchi di forza bruta) a loro disposizione (cfr. la precedente nota 80) ([85]),
6. l'efficacia della crittografia tiene conto del periodo di tempo specifico durante il quale la riservatezza dei dati personali cifrati deve essere preservata,
7. l'algoritmo di cifratura è applicato correttamente da un software adeguatamente aggiornato e senza vulnerabilità note, la cui conformità alle specifiche dell'algoritmo scelto è stata verificata, ad esempio mediante certificazione,
8. 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 soggetto di fiducia dell'esportatore in una giurisdizione che offre un livello di protezione sostanzialmente equivalente,

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

Caso d'uso 4: destinatario protetto

91. 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 legislazione del paese terzo esclude che l'importatore di dati residente possa essere interessato da forme di accesso ai dati da quest'ultimo detenuti per la finalità specifica potenzialmente in violazione delle garanzie previste, ad esempio in virtù di un obbligo di segreto professionale che si applica all'importatore di dati,
2. tale esclusione 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 tale da consentire alle autorità pubbliche di accedere ai dati in possesso di quest'ultimo, né inoltra i dati a un altro soggetto che non gode delle tutele di cui sopra, sulla base degli strumenti di trasferimento di cui all'articolo 46 del RGPD,

([85]) Cfr. la nota 80 per alcuni riferimenti agli orientamenti tecnici pubblicati dalle autorità ufficiali di cibersicurezza dell'UE e dei suoi Stati membri.

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 protetto nonché, eventualmente, dell'esportatore stesso o di un altro soggetto incaricato dall'esportatore che è situato nel SEE o in un territorio che offre un livello di protezione sostanzialmente equivalente a quello garantito all'interno del SEE, ed è 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 allora che la cifratura del trasporto fornisca un'efficace misura supplementare.

Caso d'uso 5: trattamento frazionato o multilaterale

92. L'esportatore di dati desidera che i dati personali siano trattati congiuntamente da due o più responsabili del trattamento indipendenti situati in Stati diversi senza rivelare loro il contenuto dei dati. Prima della trasmissione, suddivide i dati in modo tale che nessun elemento ricevuto da un singolo responsabile del trattamento sia sufficiente per ricostruire i dati personali in tutto o in parte. L'esportatore di dati riceve il risultato del trattamento separatamente da ciascuno dei responsabili e fonde gli elementi ricevuti per arrivare al risultato finale sotto forma di dati personali o di aggregati di dati.

Se

1. l'esportatore di dati tratta i dati personali in modo tale che essi siano suddivisi in due o più parti, ciascuna delle quali non è interpretabile né può essere attribuita a un determinato interessato senza l'utilizzo di informazioni aggiuntive,
2. ciascuna parte viene trasferita a un distinto responsabile del trattamento situato in un diverso Stato,
3. i responsabili del trattamento hanno la possibilità di trattare i dati congiuntamente, ad esempio mediante un calcolo sicuro a più parti (*multi-party computation*), in modo che non venga rivelata a nessuno di loro alcuna informazione che non possedessero già prima del calcolo,
4. l'algoritmo utilizzato per il calcolo condiviso è sicuro rispetto ad avversari attivi,
5. il titolare del trattamento ha stabilito, mediante un'analisi approfondita dei dati in questione, tenendo conto delle informazioni mancanti che le autorità pubbliche dei paesi destinatari potrebbero presumibilmente possedere e utilizzare, che i dati personali trasmessi ai responsabili del trattamento non possono essere attribuiti a una persona fisica identificata o identificabile, anche se incrociati con tali informazioni,
6. non vi sono evidenze di collaborazioni tra le autorità pubbliche degli Stati in cui operano rispettivamente i responsabili del trattamento tali da consentire alle suddette autorità di accedere a tutti i set di dati personali in possesso dei responsabili del trattamento e di ricostituire e sfruttare il contenuto dei dati personali in chiaro secondo modalità tali per cui ciò non rispetterebbe l'essenza dei diritti e delle libertà fondamentali degli interessati. Analogamente, nessuna delle autorità pubbliche in nessuno di tali Stati dovrebbe avere il potere di accedere ai dati personali detenuti dai responsabili del trattamento,

l'EDPB ritiene allora che il trattamento eseguito in modalità frazionata fornisca un'efficace misura supplementare.

Esempi di scenari relativi a casi per i quali non sono individuate misure *efficaci*

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

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

94. Un esportatore di dati trasferisce dati personali, sia mediante trasmissione elettronica sia rendendoli disponibili a un fornitore di servizi cloud o a un altro responsabile del trattamento per far trattare i dati personali secondo le sue istruzioni in un paese terzo (ad esempio per fornire assistenza tecnica o effettuare qualsiasi tipo di trattamento sul cloud) e tali dati non sono - o non possono essere - pseudonimizzati come descritto nel caso d'uso 2 né cifrati come descritto nel caso d'uso 1, perché il trattamento richiede l'accesso ai dati in chiaro.

Se

1. il titolare del trattamento trasferisce i dati personali 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 riconosciuto alle autorità pubbliche del paese destinatario di accedere ai dati trasferiti in questione va oltre quanto necessario e proporzionato in una società democratica qualora, in concreto, la legislazione problematica del paese terzo si applichi ai trasferimenti in questione (cfr. terzo passo) ([86]),

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 fondamentali degli interessati. L'EDPB non esclude che ulteriori sviluppi tecnologici possano offrire misure in grado di conseguire gli scopi commerciali previsti, senza richiedere l'accesso in chiaro.

95. Negli scenari indicati, in cui 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 congiuntamente, non costituiscono una misura supplementare che garantisce un livello di protezione sostanzialmente equivalente se l'importatore dei dati è in possesso delle chiavi crittografiche.

([86]) 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.

Caso d'uso 7: trasferimento di dati personali per scopi commerciali, anche tramite accesso remoto

96. Un esportatore di dati trasferisce i dati personali a soggetti in un paese terzo affinché siano utilizzati per scopi commerciali condivisi, sia mediante trasmissione elettronica sia rendendoli disponibili per l'accesso remoto da parte dell'importatore, e tali dati non sono (o non possono essere) pseudonimizzati come descritto nel caso d'uso 2 né cifrati come descritto nel caso d'uso 1, perché il trattamento richiede l'accesso ai dati in chiaro. Una situazione tipica è quella in cui un titolare del trattamento o un responsabile del trattamento stabilito nel territorio di uno Stato membro 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 gestione del personale all'esportatore di dati, e per far ciò ha bisogno di dati relativi alle risorse umane, o per comunicare con i clienti dell'esportatore di dati che vivono nell'Unione europea tramite telefono o e-mail.

Se

1. L'esportatore di dati trasferisce dati personali a un importatore di dati in un paese terzo rendendoli disponibili in un sistema informatico 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 ([87]) tratta i dati in chiaro nel paese terzo (anche per i propri scopi, nel caso in cui sia un titolare del trattamento),
3. il potere riconosciuto alle autorità pubbliche del paese destinatario di accedere ai dati trasferiti va oltre quanto necessario e proporzionato in una società democratica qualora, in concreto, la legislazione problematica del paese terzo si applichi ai trasferimenti in questione (cfr. terzo passo),

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

97. Negli scenari indicati, in cui 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 congiuntamente, non costituiscono una misura supplementare che garantisce un livello di protezione sostanzialmente equivalente se l'importatore dei dati è in possesso delle chiavi crittografiche.

([87]) Indipendentemente dal fatto che sia un titolare o un responsabile del trattamento in un paese terzo a ricevere od ottenere accesso ai dati personali trasferiti dal SEE.

2.2 Misure contrattuali supplementari

98. Queste misure consisteranno generalmente in impegni contrattuali ([88]) unilaterali, bilaterali o multilaterali ([89]). 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 ([90]).

99. 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, essi non soddisfano tutte le condizioni necessarie per assicurare un livello di protezione sostanzialmente equivalente a quello garantito all'interno del SEE. Alla luce della natura delle misure contrattuali, che generalmente non possono vincolare le autorità di tale paese terzo quando queste ultime non sono parti del contratto ([91]), è possibile che tali misure debbano spesso 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.

100. 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.

101. 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 tale legislazione obbliga gli importatori a ottemperare agli ordini ricevuti dalle autorità pubbliche di comunicare i dati ([92]).

102. Alcuni esempi di queste possibili misure contrattuali sono elencati qui di seguito e classificati in base alla loro natura.

([88]) Si tratta di accordi aventi 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 parte non contraente, quando sono conclusi con organismi privati di paesi terzi, come sottolineato dalla Corte nella sentenza C-311/18 (Schrems II), paragrafo 125.
([89]) Ad esempio nell'ambito delle norme vincolanti d'impresa, che dovrebbero in ogni caso disciplinare alcune delle misure elencate di seguito.
([90]) 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.
([91]) C-311/18 (Schrems II), paragrafo 125.
([92]) Sentenza della CGUE C-311/18 (Schrems II), paragrafo 132.

Prevedere l'obbligo contrattuale di utilizzare misure tecniche specifiche

103. A seconda delle circostanze specifiche dei trasferimenti (ivi compresa l'applicazione concreta della legislazione del paese terzo), potrebbe essere necessario prevedere contrattualmente l'obbligo di attuare misure tecniche specifiche affinché i trasferimenti abbiano luogo (vedi sopra le misure tecniche suggerite).

104. Condizioni di efficacia:

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

Obblighi di trasparenza

105. L'esportatore potrebbe aggiungere al contratto allegati contenenti informazioni che l'importatore avrà fornito prima della conclusione del contratto, con la massima diligenza possibile, in merito all'accesso ai dati da parte delle autorità pubbliche nel paese di destinazione, anche nel campo dell'intelligence, a condizione che la legislazione sia conforme alle garanzie essenziali europee dell'EDPB. Ciò potrebbe aiutare l'esportatore di dati a rispettare l'obbligo di documentare la valutazione del livello di protezione nel paese terzo. Così facendo si darebbe inoltre evidenza all'obbligo dell'importatore di assistere l'esportatore nella sua valutazione assumendosi la responsabilità di fornire, in tale contesto, informazioni che siano oggettive, pertinenti, attendibili, verificabili e disponibili al pubblico o altrimenti accessibili.

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

(1) elencare le leggi e i regolamenti del paese di destinazione applicabili all'importatore o ai suoi eventuali (sub)responsabili del trattamento che consentirebbero alle autorità pubbliche di accedere ai dati personali oggetto del trasferimento, in particolare nei settori dell'intelligence, delle attività giudiziarie e di polizia, del controllo amministrativo e regolamentare applicabile ai dati trasferiti;

(2) in assenza di norme 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 commerciali, fonti pubbliche, giurisprudenza nazionale e decisioni degli organi di controllo) rispetto all'accesso da parte delle autorità pubbliche ai dati personali in situazioni assimilabili al trasferimento in questione (ad esempio nel settore normativo specifico; con riguardo alla categoria cui appartiene l'importatore di dati; ecc.);

(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 ricevute dall'importatore in un determinato

periodo di tempo ([93]), in particolare nei settori di cui al punto 1), fra cui informazioni sulle richieste ricevute, sui dati richiesti, sull'organismo richiedente, sulla base giuridica ai fini della comunicazione e sulla misura in cui l'importatore ha ottemperato alla richiesta di dati ([94]);

specificare se e in quale misura all'importatore sia proibito per legge fornire le informazioni di cui ai punti da 1) a 5).

107. Tali informazioni potrebbero essere fornite mediante questionari strutturati che l'importatore dovrebbe compilare e firmare e che sarebbero integrati dall'obbligo contrattuale dell'importatore di segnalare entro un intervallo determinato eventuali modifiche a tali informazioni, come è prassi corrente per i processi di *due diligence*.

108. Condizioni di efficacia:

- L'importatore deve essere in grado di fornire all'esportatore questo tipo di informazioni al meglio delle proprie conoscenze e dopo essersi adoperato al massimo per ottenerle.
- 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. Ciò consentirà quindi all'esportatore di desistere dalla conclusione del contratto o, se le informazioni cambiano successivamente alla stipula, 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 del SEE. Il rispetto di tale obbligo non può tuttavia giustificare la comunicazione dei dati personali da parte dell'importatore, né far presumere che non vi saranno ulteriori richieste di accesso.

***

109. 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) il diritto 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 ([95]).

110. Condizioni di efficacia:

- L'esistenza di una legislazione o di politiche governative che impediscono agli importatori di comunicare le informazioni in questione può rendere inefficace tale clausola. L'importatore

([93]) Tale lasso di tempo 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 del perfezionamento dello strumento di esportazione dei dati con l'esportatore di dati.
([94]) Il rispetto di questo obbligo non equivale, in quanto tale, alla prestazione di un livello di protezione adeguato. Al tempo stesso, qualsiasi comunicazione impropria che sia effettivamente avvenuta porta alla necessità di attuare misure supplementari.
([95]) Questa clausola è importante per garantire un adeguato livello di protezione dei dati personali trasferiti e dovrebbe essere richiesta in via routinaria.

non sarà quindi in grado di stipulare il contratto o dovrà comunicare all'esportatore la sua incapacità di continuare a rispettare gli impegni contrattuali.

- Il contratto deve includere sanzioni e/o la possibilità per l'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 aziendali manipolati o l'obbligo di attuare uno di essi o non informi tempestivamente l'esportatore non appena venga a conoscenza della loro esistenza.
- Nel caso in cui l'importatore di dati abbia comunicato dati personali trasferiti violando gli impegni previsti dallo strumento di trasferimento, il contratto potrebbe altresì prevedere un risarcimento da parte dell'importatore di dati a beneficio dell'interessato per i danni materiali e immateriali subiti.

***

111. L'esportatore potrebbe rafforzare il suo potere di effettuare verifiche ([96]) o ispezioni delle strutture di trattamento dei dati dell'importatore, in loco e/o da remoto, per verificare se i dati siano stati comunicati alle autorità pubbliche e a quali condizioni (accesso non oltre quanto necessario e proporzionato in una società democratica), ad esempio prevedendo un breve preavviso e meccanismi che garantiscano il rapido intervento degli organismi ispettivi e rafforzino l'autonomia dell'esportatore nella scelta degli stessi.

112. Condizioni di efficacia:

- Per essere pienamente efficace, l'ambito della verifica deve includere giuridicamente e tecnicamente qualsiasi trattamento dei dati personali trasmessi nel paese terzo che sia svolto da parte dei (sub)responsabili del trattamento operanti per l'importatore.
- I registri di accesso e altri registri simili dovrebbero essere a prova di manomissione (per esempio dovrebbero essere resi inalterabili per mezzo di tecniche di cifratura conformi allo stato dell'arte, come l'hashing, ed essere inoltre trasmessi sistematicamente e periodicamente all'esportatore) in modo che i soggetti incaricati delle verifiche possano trovare evidenze di eventuali comunicazioni. I registri di accesso e altri registri simili dovrebbero inoltre distinguere tra gli accessi dovuti a regolari operazioni commerciali e gli accessi dovuti a ordini o richieste di accesso.

***

113. Qualora a seguito della valutazione iniziale del diritto e delle prassi del paese terzo dell'importatore si sia ritenuta la sussistenza di 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, ove la situazione si modifichi, dell'impossibilità di rispettare gli impegni contrattuali

([96]) 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.

e di conseguenza lo standard richiesto di «sostanziale equivalenza» del livello di protezione dei dati ([97]).

114. Tale impossibilità può derivare da cambiamenti nella legislazione o nelle prassi del paese terzo ([98]). 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, della loro portata e dell'efficacia delle misure adottate per opporvisi dovrebbero fornire all'esportatore indicazioni sufficienti per adempiere all'obbligo di sospendere o terminare il trasferimento e/o risolvere il contratto.

115. Condizioni di efficacia:

- La notifica deve avvenire prima di consentire l'accesso ai dati. 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 norme di tale paese terzo che eccedono quanto è consentito in base al livello di protezione dei dati previsto dal diritto dell'Unione. La notifica può comunque servire a prevenire future violazioni e a consentire all'esportatore di adempiere all'obbligo di sospendere il trasferimento dei dati personali verso il paese terzo e/o di rescindere il contratto.
- L'importatore di dati deve monitorare qualsiasi sviluppo giuridico o politico che potrebbe comportare l'incapacità di adempiere agli obblighi rispettivamente incombenti e informare tempestivamente l'esportatore di tali sviluppi, se possibile prima della loro realizzazione, in modo da consentire all'esportatore di recuperare i 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 ([99]) 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 attraverso sanzioni per l'importatore e/o il potere dell'esportatore di sospendere il trasferimento e/o di rescindere immediatamente il contratto.

***

([97]) Clausola 5, lettera a) e lettera d), punto i) della decisione 2010/87/UE relativa alle clausole contrattuali tipo.
([98]) 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».
([99]) Tale soglia dovrebbe garantire che gli interessati continuino a godere di un livello di protezione equivalente a quello garantito all'interno del SEE.

116. Nella misura consentita dalla legislazione nazionale del paese terzo, il contratto potrebbe rafforzare gli obblighi di trasparenza dell'importatore prevedendo il ricorso al cosiddetto «Warrant Canary», per cui l'importatore si impegna a pubblicare regolarmente (ad esempio, almeno ogni 24 ore) un messaggio firmato in forma cifrata con cui informa l'esportatore che fino a una certa data e ora non ha ricevuto alcun ordine di rivelare dati personali o simili. Il mancato aggiornamento di questa comunicazione indicherà all'esportatore che l'importatore potrebbe aver ricevuto un ordine in tal senso.

117. 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 warrant canary.
- L'importatore di dati deve garantire la conservazione sicura della sua chiave privata per la firma del warrant canary e che la legislazione del paese terzo non possa obbligarlo a emettere falsi warrant canary. A tal fine, potrebbe essere utile prevedere l'apposizione di più firme da parte di persone diverse e/o l'emissione del warrant canary da parte di una persona non soggetta alla giurisdizione del paese terzo.

Obblighi di intraprendere azioni specifiche

118. L'importatore potrebbe impegnarsi a verificare, in base al diritto del paese di destinazione, la legalità di eventuali ordini di comunicazione dei dati, in particolare se essi eccedano i poteri riconosciuti all'autorità pubblica richiedente, e a contestare tali ordini se, dopo un'attenta valutazione, conclude che vi sono motivi per farlo in base al diritto del paese di destinazione. Nel contestare un ordine, l'importatore di dati dovrebbe chiedere misure provvisorie atte a sospendere gli effetti dello stesso fino a quando l'autorità giudiziaria non si sarà pronunciata nel merito. L'importatore avrà l'obbligo di non comunicare i dati personali richiesti fino a quando non sia tenuto a farlo in base alle norme applicabili. L'importatore si impegnerà inoltre a fornire la quantità minima consentita di informazioni in risposta all'ordine, sulla base di un'interpretazione ragionevole dello stesso.

119. Condizioni di efficacia:

- L'ordinamento giuridico del paese terzo deve offrire vie legali efficaci per contestare gli ordini di comunicazione dei dati.
- Questa clausola offrirà sempre una protezione aggiuntiva molto limitata, poiché un ordine di comunicare i 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 del diritto 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 comunicazione dei dati.
- L'importatore dovrà essere in grado di documentare e dimostrare all'esportatore le azioni che ha intrapreso, adoperandosi al massimo delle proprie possibilità, per adempiere a questo impegno.

***

120. Nella 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 ([100]) 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.

121. Condizioni di efficacia:

- Le informazioni sulla protezione conferita dal diritto dell'Unione e sul conflitto di obblighi dovrebbero avere un qualche effetto giuridico nell'ordinamento del paese terzo per potenziare la protezione dei dati, come ad esempio provocare un riesame in sede giudiziaria o amministrativa dell'ordine o della richiesta di accesso, rendere necessario un mandato giudiziario e/o imporre una sospensione temporanea dell'ordine.
- 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, adoperandosi al massimo delle proprie possibilità, per adempiere a questo impegno.

Consentire agli interessati di esercitare i loro diritti

122. Il contratto potrebbe consentire l'accesso ai dati personali trasmessi in chiaro nel corso della normale attività commerciale (anche in contesti di supporto) solo previo accordo espresso o implicito dell'esportatore e/o dell'interessato, con riguardo a uno specifico accesso ai dati.

123. Condizioni di efficacia:

- Questa clausola potrebbe essere efficace in quelle situazioni in cui gli importatori ricevono richieste di cooperazione su base volontaria da parte delle autorità pubbliche, in contrapposizione, ad esempio, all'accesso ai dati da parte delle autorità pubbliche effettuato 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 prestare un consenso che soddisfi tutte le condizioni stabilite dal diritto dell'Unione (libero, specifico, informato e inequivocabile) (ad esempio nel caso di lavoratori dipendenti) ([101]).

---

[100] 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.
([101]) Articolo 4, paragrafo 11, del RGPD.

- Eventuali normative o prassi nazionali che obblighino l'importatore a non divulgare l'ordine di accesso possono rendere inefficace questa clausola, a meno di rafforzarla prevedendo tecnicamente la necessità di un intervento dell'esportatore o dell'interessato affinché i dati in chiaro siano resi accessibili. Tali misure tecniche volte a limitare l'accesso possono essere previste in particolare se l'accesso è consentito solo in casi specifici relativi ad attività di supporto o di servizio, ma i dati in quanto tali sono conservati nel SEE.

***

124. 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, così da consentire all'interessato di chiedere informazioni e di esperire un mezzo di ricorso effettivo (ad esempio presentando un reclamo all'autorità di controllo competente e/o all'autorità giudiziaria e dimostrando la propria legittimazione attiva dinanzi alle autorità giudiziarie del paese terzo), con la possibilità di prevedere un risarcimento da parte dell'importatore di dati per tutti i danni materiali e immateriali subiti dell'interessato a causa della comunicazione dei dati personali trasferiti per mezzo dello strumento di trasferimento prescelto in violazione degli impegni da quest'ultimo previsti.

125. Condizioni di efficacia:

- Questa comunicazione potrebbe allertare l'interessato rispetto a 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 contribuire a risolvere alcune delle difficoltà che un interessato può incontrare nel dimostrare la propria legittimazione attiva (locus standi) dinanzi alle autorità giudiziarie di paesi terzi per contestare l'accesso ai propri dati da parte delle autorità pubbliche.
- Le normative e le politiche nazionali possono vietare questa comunicazione all'interessato. L'esportatore e l'importatore potrebbero tuttavia impegnarsi a informare l'interessato non appena le restrizioni alla suddetta comunicazione siano revocate e a compiere ogni sforzo possibile per ottenere la deroga al divieto di comunicazione. Come minimo, l'esportatore o l'autorità di controllo competente potrebbero comunicare all'interessato la sospensione o la cessazione del trasferimento dei suoi dati personali a causa dell'impossibilità per l'importatore di adempiere ai suoi impegni contrattuali a seguito della ricezione di una richiesta di accesso.

***

126. Il contratto potrebbe impegnare l'esportatore e l'importatore ad assistere l'interessato nell'esercizio dei suoi diritti nel paese terzo mediante appositi meccanismi di ricorso e consulenza legale.

127. Condizioni di efficacia:

- Alcune normative nazionali potrebbero non consentire all'importatore di dati di prestare questo tipo di assistenza direttamente agli interessati, benché possano permettergli di procurare tale assistenza a loro beneficio.

- Le normative e le prassi nazionali possono imporre condizioni tali da compromettere l'efficacia degli appositi meccanismi di ricorso 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 la prestazione di 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 del SEE. 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 mezzi di ricorso dinanzi alle autorità giudiziarie nazionali, o che esista un meccanismo di ricorso apposito, anche contro le misure di sorveglianza.

2.3 Misure organizzative

128. Ulteriori misure organizzative possono consistere in politiche interne, metodi organizzativi e standard che i titolari 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 in tali frangenti. 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 del SEE.

129. La valutazione delle misure più idonee deve essere effettuata caso per caso, tenendo presente che i titolari 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. L'elenco non è esaustivo e possono essere appropriate anche altre misure.

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

130. Adozione di adeguate politiche interne con una chiara attribuzione delle responsabilità per il trasferimento dei dati, canali di segnalazione e procedure operative standard in caso di richieste formali o informali di accesso ai dati da parte di autorità pubbliche. Soprattutto in caso di trasferimenti tra gruppi di imprese, tali politiche possono includere, tra l'altro, la nomina di un team specifico, composto da esperti in materia di informatica e legislazione in materia di protezione dei dati e privacy, per gestire le richieste che riguardano dati personali trasferiti dal SEE; 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.

131. 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.

132. 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 ([102]). Quando la richiesta è incompatibile, tali politiche non sarebbero sufficienti a garantire un livello equivalente di protezione dei dati personali e, come già indicato, i trasferimenti devono essere interrotti o devono essere messe in atto misure supplementari adeguate per evitare l'accesso.

Misure a fini di trasparenza e responsabilizzazione

133. 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 quale sia stata 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.

134. Condizioni di efficacia:

- La legislazione nazionale del paese terzo può vietare la divulgazione delle richieste o delle informazioni di merito e quindi rendere inefficace questa prassi. L'importatore di dati dovrebbe informare l'esportatore dell'impossibilità di fornire tali documenti e registrazioni, offrendogli così la possibilità di sospendere i trasferimenti se ciò comportasse la mancanza di un livello di protezione adeguato.

***

135. La pubblicazione regolare di relazioni sulla trasparenza o di sintesi riguardanti le richieste governative di accesso ai dati e la tipologia delle risposte fornite, nella misura in cui tale pubblicazione è consentita dalla legislazione nazionale.

136. 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.

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

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

137. Anche i requisiti organizzativi già esistenti in base al principio di responsabilizzazione, quali l'adozione di politiche di accesso ai dati e di riservatezza rigorose e granulari, e migliori pratiche basate sulla rigorosa applicazione del principio di necessità ("need to know"), monitorate regolarmente e attuate- con l'aiuto di misure disciplinari, possono risultare utili in un contesto di trasferimento dei dati. 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 (si veda il caso di un accesso remoto ai dati SEE, come nelle attività di supporto, quando è previsto un accesso limitato anziché 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).

138. Condizioni di efficacia:

- Dovrebbero essere previste verifiche regolari e misure disciplinari importanti 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 (*multi-party computation*) sicuri e la disseminazione di set di dati cifrati tra più soggetti fiduciari può impedire, fin dalla progettazione, che un eventuale accesso unilaterale comporti la divulgazione di dati identificabili.

***

139. Sviluppo di migliori prassi per coinvolgere in modo appropriato e tempestivo e informare il responsabile della protezione dei dati, se esistente, e i servizi legali e di revisione interna su questioni relative ai trasferimenti internazionali di dati personali.

140. 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 normative del paese terzo applicabili e le garanzie che l'importatore si è impegnato ad attuare.

Adozione di standard e migliori prassi

141. 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.

Altre

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

***

143. L'impegno dell'importatore di dati a non effettuare trasferimenti successivi dei dati personali all'interno dello stesso paese o verso 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 sostanzialmente equivalente a quello garantito all'interno del SEE ([103]).

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

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

144. 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, ivi comprese le normative e le prassi applicabili all'importatore stesso e ai dati trasferiti. Voi e l'importatore potete fare riferimento a varie fonti di informazione, come quelle elencate di seguito in modo non esaustivo e in ordine di preferenza:

- giurisprudenza della Corte di giustizia dell'Unione europea (CGUE) e della Corte europea dei diritti dell'uomo (Corte CEDU) ([104]), come indicato nelle raccomandazioni relative alle garanzie essenziali europee ([105]);
- decisioni di adeguatezza nel paese di destinazione se il trasferimento si basa su una base giuridica diversa ([106]);
- risoluzioni e relazioni di organizzazioni intergovernative, quali il Consiglio d'Europa ([107]), altri organismi regionali ([108]) e organi e agenzie dell'ONU [ad esempio il Consiglio dei diritti umani delle Nazioni Unite ([109]) o il Comitato dei diritti umani ([110])];
- relazioni e analisi a cura di reti di regolamentazione competenti come la Global Privacy Assembly (GPA) ([111]);
- giurisprudenza nazionale o decisioni adottate da autorità giudiziarie o amministrative indipendenti competenti in materia di privacy e di protezione dei dati di paesi terzi;
- relazioni pubblicate da organi parlamentari o di vigilanza indipendenti;
- relazioni pubblicate da soggetti attivi nello stesso settore dell'importatore basate sull'esperienza pratica relativa a casi pregressi di richieste di comunicazione da parte di autorità pubbliche, o all'assenza di tali richieste;
- warrant canary di altri soggetti che trattano dati nello stesso settore dell'importatore;
- relazioni prodotte o commissionate da camere di commercio, associazioni commerciali, professionali e di categoria, agenzie diplomatiche governative, commerciali e di investimento dell'esportatore o di altri paesi terzi che esportano nel paese terzo verso cui viene effettuato il trasferimento;

([104]) Si veda la scheda della giurisprudenza della Corte CEDU sulla sorveglianza di massa: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

([105]) 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.

([106]) 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

[107] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

([108]) Cfr., ad esempio, i rapporti sui paesi della Commissione interamericana dei diritti dell'uomo (IACHR), https://www.oas.org/en/iachr/reports/country.asp..

([109]) Cfr. https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx.

([110]) Cfr. https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5.

([111]) Cfr. per esempio https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf.

- relazioni di istituzioni accademiche e organizzazioni della società civile (ad esempio ONG);
- relazioni di fornitori privati di business intelligence in materia di rischi finanziari, normativi e reputazionali per le aziende;
- warrant canary dell'importatore stesso ([112]);
- relazioni sulla trasparenza, a condizione che menzionino espressamente il fatto che non sono pervenute richieste di accesso. Le relazioni sulla trasparenza che si limitino a tacere sul punto non sarebbero sufficientemente probanti, poiché il più delle volte riferiscono delle richieste di accesso pervenute da autorità giudiziarie e di polizia e forniscono dati solo su questo aspetto, mentre tacciono in merito a richieste di accesso ricevute per scopi di sicurezza nazionale. Ciò non significa che non siano pervenute richieste di accesso, ma piuttosto che queste informazioni non possono essere condivise ([113]).
- dichiarazioni interne o registri dell'importatore che indicano espressamente che non sono pervenute richieste di accesso per un periodo sufficientemente lungo, preferibilmente dichiarazioni e registri che impegnano la responsabilità dell'importatore e/o che sono prodotti da funzioni interne dotate di margini di autonomia quali revisori interni, responsabili della protezione dei dati, ecc. ([114])

([112]) Cfr. le condizioni per tenere conto dell'esperienza pratica documentata dell'importatore rispetto a casi pregressi e pertinenti di richieste di accesso pervenute da autorità pubbliche nel paese terzo di cui al paragrafo 47.
([113]) *Ibid.*
([114]) *Ibid.*