

1. Trasferimento dei dati all'estero¹

L'architettura delle norme sui trasferimenti internazionali non ha subito modifiche rilevanti rispetto quella della direttiva 95/46/CE ora abrogata: il GDPR tende a chiarirne l'impiego, formalizza e amplia il numero di strumenti di trasferimento alternativi, come le clausole contrattuali tipo e le norme vincolanti d'impresa, affinché con il trasferimento risultino impregiudicati i livelli di protezione delle persone fisiche garantite dal GDPR (art.44).

Scopo di questo documento è offrire un quadro d'insieme dei fattori da prendere in considerazione nell'effettuare un trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, assicurando una continuità del livello di protezione associata ai dati ("attaccata" ai dati, *sticky regulation*) anche a seguito di qualsiasi ulteriore successivo trasferimento, avendo presente che i trasferimenti verso paesi esteri non sono consentiti, in linea di principio, a meno che intervengano specifiche garanzie che il regolamento elenca in ordine gerarchico, dalle decisioni di adeguatezza alle deroghe in specifiche situazioni.

Occorre quindi tenere presente che i trasferimenti verso paesi esteri è sempre soggetto al rispetto di almeno una delle regole di cui al Capo V del GDPR.

1.1 Definizioni utili

- a) **Paese terzo:** è uno Stato non appartenente all'UE o allo Spazio Economico Europeo comprendente anche la Norvegia, l'Islanda e il Liechtenstein.
- b) **Organizzazione internazionale:** ai sensi dell'art.4.26) del GDPR, è un'organizzazione o un organismo di diritto internazionale pubblico a essa subordinato o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.
- c) **Paese estero:** un paese terzo o un'organizzazione internazionale.
- d) **Trasferimento:** è un trattamento ed avviene se i dati del Titolare, soggetto alle disposizioni del GDPR, sono oggetto di un qualsiasi trattamento in un paese terzo o sono destinati ad esserlo dopo il trasferimento verso un titolare, responsabile o destinatario stabilito fuori dell'ambito di applicazione del GDPR. Un ulteriore chiarimento del termine è riportato in fondo al paragrafo.
- e) **Trasferimento occasionale e non ripetitivo:** si configurano tali quei trattamenti che:
 - i. Possono ripetersi ma: solo in circostanze non ordinarie e a intervalli di tempo arbitrari
 - ii. Sono conseguenti al manifestarsi di condizioni casuali o ignote e pertanto non hanno sicuramente cadenza regolare
- f) **Trattamento:** è definito dall'art. 4.2) GDPR come qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- g) **Comunicazione:** è definita dal comma 4 dall'art. 2-ter del D.Lgs. 196/2003 come il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
- h) **Diffusione:** è definita dal comma 4 dall'art. 2-ter del D.Lgs. 196/2003 come il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
- i) **Adeguatezza:** nel caso dei trasferimenti, indica che non possa esigersi che un paese terzo assicuri un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione ma che tale paese assicuri effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello

¹ Testi principali utilizzati oltre il GDPR: "il Regolamento privacy europeo" Bolognini-Pelino-Bistolfi ed. Giuffrè; Linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679 EDPB; Comunicazione della Commissione Europea n.43 del 24.1.2018; direttiva 95/46/CE; doc.WP114 25.11.2005 Gruppo WP29; sentenza CGUE 6 ottobre 2015 su causa C-362/14 (Schrems); sentenza CGUE 6 novembre 2003 Lindquist; Doc WP 47 5061/01/IT/def Gruppo WP29

di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito all'interno dell'Unione.

- j) **Decisione di adeguatezza:** è la decisione della Commissione Europea, assunta a valle di una valutazione dell'adeguatezza del livello di protezione dei dati, che un paese terzo, un territorio, uno o più settori all'interno di un territorio o un'organizzazione internazionale garantiscono un livello di protezione adeguato per il trattamento dei dati personali.
- k) **Registro:** un documento (scritto, in formato cartaceo o elettronico) in cui sono annotati con regolarità determinati elementi o particolari, oppure un elenco ufficiale riportante una serie di nomi o elementi (Merriam Webster Dictionary, Oxford dictionary 2018)

Per comprendere meglio la definizione di trasferimento, che il GDPR non fornisce direttamente, risultano utili alcune considerazioni che la Corte di Giustizia UE espresse in relazione al caso Lindqvist dove, tra altri punti, fu chiamata a stabilire se l'inserimento su una pagina internet di dati personali costituisse trasferimento di dati verso un paese terzo per il solo fatto di rendere tali dati accessibili a persone che si trovano in paesi terzi.

La conclusione fu che l'inserimento di dati personali in una pagina web di un fornitore di servizi (web provider) stabilito in uno Stato membro, effettuato da parte di una persona che si trova in uno Stato membro, non costituisce trasferimento di dati personali ai sensi dell'art. 44 del GDPR, il che induce a ritenere che si configuri un trasferimento di dati nell'ipotesi in cui il fornitore sia stabilito in un paese terzo.

Si noti come venga ampliata temporalmente la protezione del dato nel caso di trasferimenti all'estero perché, secondo le previsioni all'art. 44, per configurarsi un trasferimento di dati verso paesi terzi non è necessario che essi vengano trattati contemporaneamente al trasferimento: è sufficiente che essi siano destinati a trattamenti in fase successiva al trasferimento, compresi gli eventuali trasferimenti successivi verso un altro paese terzo o organizzazione internazionale.

Alcune condizioni per il trasferimento, come si vedrà, si applicano solo a quelli caratterizzabili come "occasional" o "non ripetitivi"; a solo titolo d'esempio, non possono considerarsi occasionali i trasferimenti di dati personali da un Titolare ad un importatore nell'ambito di un rapporto stabile o quando l'importatore possa accedere direttamente alla banca dati mediante un'interfaccia applicativa, indipendentemente da quante volte la utilizzi.

Alcune Organizzazioni internazionali sono totalmente autonome e indipendenti nello scenario internazionale ed il loro operato non è riferibile ad alcuno stato in particolare: per questo motivo sono stati considerati equiparabili ai paesi terzi, nella nuova normativa, così da poter garantire agli interessati diritti azionabili e mezzi di ricorso effettivi anche in tali trasferimenti.

1.2 Adempimenti

Il trasferimento di dati personali, come ogni trattamento, deve essere innanzitutto conforme alle disposizioni generali inerenti la protezione dei dati personali, in relazione alle finalità per cui viene effettuato, quindi:

- deve essere fondato su una base giuridica tra quelle previste all'art. 6 del GDPR;
- deve essere eseguito nel pieno rispetto dei principi elencati all'art.5 del GDPR e, in generale, di tutte le disposizioni pertinenti del GDPR e delle altre normative applicabili ai trattamenti di dati personali;
- deve essere inserito nel Registro dei trattamenti, riportando i paesi terzi od organizzazioni internazionali a cui i dati personali sono stati o saranno comunicati, la valutazione del rischio effettuata e la descrizione delle garanzie attuate per il trasferimento, in relazione ai rischi valutati, affinché l'interessato benefici di un adeguato livello di protezione dei suoi dati personali sia nel trasferimento dei dati verso un paese terzo sia nell'eventuale ulteriore trasferimento da questi ad altro paese terzo, secondo le disposizioni al Capo V del GDPR;
- deve essere inserito nell'informativa per l'interessato, riportando quali siano i paesi terzi o organizzazioni internazionali destinatarie e le motivazioni per cui ha luogo il trasferimento. Devono essere inoltre riportate le valutazioni del Titolare in merito alla scelta dello strumento di garanzia adottato, tra quelli previsti dal GDPR, in caso di assenza di una decisione di adeguatezza.

La valutazione dell'adeguatezza della tutela offerta da un paese terzo va considerata in funzione di **tutte** le circostanze relative ad un trasferimento o ad una categoria di trasferimenti, che riguardano anche la modalità, la frequenza, la durata e il contesto del trasferimento.

Sia nella valutazione del rischio sia nelle garanzie attuabili, il Titolare deve prestare attenzione anche ai trasferimenti che potrebbero subentrare tra l'importatore dei dati e un successivo sub-incaricato, in virtù di un subcontratto dell'importatore.

1.3 Condizioni per la legittimità del trasferimento

I dati possono essere trasferiti solo in presenza di **almeno una** delle seguenti condizioni, ovvero una delle relative sotto-casistiche, che saranno dettagliate nei successivi paragrafi:

1. **Decisione di adeguatezza:** se la Commissione Europea ha deciso che il Paese terzo, un territorio o uno o più settori specifici all'interno del Paese terzo, o l'organizzazione internazionale in questione, garantiscono un livello di protezione dei Dati Personali adeguato il trasferimento è possibile senza altre autorizzazioni specifiche.
2. **Garanzie adeguate:** qualora non vi sia decisione di adeguatezza, il trasferimento può essere effettuato in presenza di garanzie adeguate e in forza di condizioni per le quali gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi. Esse sono costituite da (alternativamente):
 - a. uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici;
 - b. le norme vincolanti d'impresa (BCR) in conformità dell'art. 47 GDPR;
 - c. le clausole contrattuali tipo o standard di protezione dei dati, adottate dalla Commissione Europea secondo la procedura d'esame di cui all'art. 93, par. 2 GDPR;
 - d. le clausole contrattuali tipo o standard di protezione dei dati, adottate da un'Autorità di Controllo e approvate dalla Commissione Europea secondo la procedura d'esame di cui all'art. 93, par. 2 GDPR;
 - e. un Codice di Condotta (CC) approvato a norma dell'art. 40 GDPR, unitamente all'impegno vincolante ed esecutivo da parte del Titolare del trattamento o del Responsabile del trattamento nel Paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli Interessati;
 - f. un Meccanismo di Certificazione (MC) approvato a norma dell'art. 42 GDPR, unitamente all'impegno vincolante ed esigibile da parte del Titolare del trattamento o del Responsabile del trattamento nel Paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli Interessati;
 - g. (con l'autorizzazione dell'Autorità di Controllo competente) le Clausole Contrattuali tra il Titolare del trattamento o il Responsabile del trattamento e il Titolare del trattamento, il Responsabile del trattamento o il destinatario dei Dati Personali nel Paese terzo o nell'organizzazione internazionale;
 - h. (con l'autorizzazione dell'Autorità di Controllo competente) le disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli Interessati.
 - i. le autorizzazioni rilasciate da uno Stato membro o dal GDPR in base alla precedente direttiva 95/46/CE, che restano valide fino a quando non vengono modificate, sostituite o revocate dalla medesima autorità di controllo (art.46.5).
3. **Deroghe in specifiche situazioni:** in mancanza di una delle precedenti condizioni di legittimità, è possibile trasferire i Dati Personali solo se si verifica una delle seguenti situazioni vincolanti, che sono da considerare residuali nel loro utilizzo rispetto quelle riportate in precedenza e che, per il loro utilizzo da parte dell'Università o Pubblica amministrazione, richiedono la concomitante presenza di altri fattori, come nel seguito schematizzato. Le condizioni sono, in alternativa:
 - a. che l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate;
 - b. che il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;
 - c. che il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'Interessato;
 - d. che il trasferimento sia necessario per importanti motivi di interesse pubblico;
 - e. che il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
 - f. che il trasferimento sia necessario per tutelare gli interessi vitali dell'Interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
 - g. che il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri;

- h. se non è ripetitivo, se riguarda un numero limitato di interessati, se è necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgono gli interessi o i diritti e le libertà dell'Interessato; il titolare del trattamento deve aver valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione ha fornito garanzie adeguate relativamente alla protezione dei Dati Personali. Il titolare del trattamento informa del trasferimento l'Autorità di Controllo. In aggiunta alla fornitura di informazioni di cui agli artt. 13 e 14 GDPR, il titolare del trattamento informa l'Interessato del trasferimento e degli interessi legittimi cogenti perseguiti ⁽²⁾.

Ad esse si aggiunge la condizione prevista all'art. 28, paragrafo 3.a, per la quale il Responsabile del trattamento può effettuare il trasferimento dei dati verso un paese estero, pur non avendolo tra le istruzioni del Titolare, quando lo prevede il diritto dell'UE o dello Stato membro cui è soggetto. In tal caso ne informa il Titolare, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.

1.3.1 Decisione di adeguatezza

La novità del GDPR riguarda la possibilità che la decisione di adeguatezza della CE possa essere adottata anche su un territorio o uno o più settori specifici all'interno di un paese estero e non necessariamente sull'interezza di questo. Ulteriore elemento di novità è la possibilità che la decisione possa essere revocata tramite un meccanismo di riesame periodico - almeno ogni 4 anni - tenendo conto degli sviluppi che in tali paesi potrebbero incidere sul funzionamento delle decisioni già adottate

La Commissione deve difatti valutare l'adeguatezza di un paese per un trasferimento di dati personali, tenendo conto innanzitutto dello stato di diritto e del rispetto dei diritti umani e delle libertà fondamentali, della pertinente legislazione generale e settoriale, anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale, accesso delle autorità pubbliche ai dati personali e norme inerenti il trasferimento successivo dei dati personali verso un altro paese estero, osservate nel paese terzo o organizzazione internazionale.

Il concetto di adeguatezza è finalizzato anche ad escludere il ricorso a trattamenti in paesi terzi diretti ad eludere la normativa UE, richiedendo che le misure adottate nel paese terzo o organizzazione internazionale siano basate sui medesimi principi Ue di protezione dei dati e dimostrino un'efficacia verificabile: il che dovrà includere la presenza di un impianto sanzionatorio adeguato per la loro eventuale violazione e la disponibilità per l'interessato di diritti azionabili e mezzi di ricorso effettivi, in sede amministrativa e giudiziaria, quali quelli garantiti nell'ambito territoriale di applicazione del GDPR.

Sono considerate equiparate a tali decisioni quelle adottate dalla Commissione in base all'art.25 paragrafo 6 della direttiva 95/46/CE e che continuano ad essere valide fino a quando non sono modificate, sostituite o abrogate da una decisione della Commissione adottata mediante atti di esecuzione, al pari delle decisioni adottate sulla base del GDPR. Difatti esse venivano assunte sulla base di una procedura di valutazione, fondata sul parere di un comitato di supporto alla Commissione prevista all'art. 31 paragrafo 2 della stessa direttiva, con una procedura assimilabile a quella attualmente prevista per gli atti di esecuzione.

Tutte le decisioni sono pubblicate sul sito della Commissione (e anche del Garante); alla pagina https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_it è descritta la modalità con la quale l'UE determina se un paese terzo sia o meno adeguato.

1.3.2 Approfondimenti sulle Garanzie adeguate

Secondo il principio della non tassatività e in linea con l'*accountability* del titolare, in assenza di decisioni di adeguatezza è possibile ricorrere a garanzie adeguate, descritte all'art. 46 e precedentemente riportate, in alcuni casi con la necessità di autorizzazione specifica da parte di un'Autorità di controllo.

Le garanzie previste all'art. 46 mirano a rendere disponibili agli Interessati diritti azionabili e mezzi di ricorso effettivi. Tra queste, come si è accennato, continuano a rimanere valide le autorizzazioni rilasciate da uno Stato membro o dall'autorità di controllo in base all'art.26, paragrafo 2 della direttiva 95/46/CE fino a quando non vengano modificate, sostituite o abrogate dalla medesima autorità di controllo.

² Questa condizione rappresenta un'alternativa molto residuale rispetto le altre riportate ed è applicabile in condizioni particolari. Nelle linee guida EDPB sui trasferimenti è riferita come condizione al comma 2 art. 49 paragrafo 1, nella versione ufficiale del R. UE 679/2016 italiana è riportata dopo la lettera g) dello stesso paragrafo.

Continuano pertanto ad essere valide le autorizzazioni nazionali emesse dal Garante, anche in conseguenza di decisioni di adeguatezza della Commissione adottate sulla precedente normativa, riportate all'indirizzo <http://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-internazionale/trasferimento-dei-dati-verso-paesi-terzi#1>.

Si noti bene che le sentenze di un'autorità giurisdizionale e le decisioni di un'autorità amministrativa di un paese terzo, che dispongano il trasferimento di dati personali da parte di un titolare o responsabile del trattamento, possono essere riconosciute o assumere un carattere esecutivo **soltanto se** basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro, fatti salvi gli altri presupposti al trasferimento di cui al capo V del GDPR (art.48 e c115). E' questo il caso, ad esempio, dell'Accordo tra Unione europea e Stati Uniti in materia di estradizione del 25 giugno 2015 e di altri accordi presenti sulla pagina del Ministero della giustizia – Atti internazionali. Questo perché la presenza di un accordo internazionale (o anche di mutua collaborazione giudiziaria) in vigore tra lo Stato membro e il paese terzo fornisce una garanzia, da parte di questi, di tutela dei principi, dei diritti e delle libertà fondamentali dell'UE; diversamente, la mera applicazione extraterritoriale di leggi, regolamenti e atti normativi del paese terzo potrebbe creare una situazione contraria al diritto della protezione dati.

Rivedendo l'elenco delle garanzie adeguate, si può aggiungere che:

- a. strumenti giuridici vincolanti ed esecutivi tra soggetti pubblici: per avere validità, gli accordi internazionali stipulati tra soggetti pubblici europei e dei paesi esteri non devono incidere sul diritto dell'UE o sul GDPR, ossia contraddirli o limitarne la portata. Inoltre devono essere conclusi da autorità pubbliche o organismi pubblici, devono essere giuridicamente vincolanti e avere efficacia esecutiva sia nel paese terzo sia nei territori dell'UE.
- b. norme vincolanti d'impresa (BCR): requisito fondamentale per attingere a tale strumento è l'appartenenza della società "importatrice" ed "esportatrice" al medesimo gruppo societario (anche se situate in due paesi diversi). Non sono pertanto applicabili in ambito universitario.
- c. clausole contrattuali tipo: sono testi contrattuali standard sottoscritti da ambo le parti, solitamente allegati ai contratti di servizio. Esistono:
 - i) Clausole tipo della Commissione Europea: le più recenti sono state approvate dalla Commissione a febbraio 2010 e sono considerate ancora valide in base all'art.46.5 e il C106. Sono di due tipi: una per trasferimenti da un titolare ad un titolare fuori UE, l'altra per trasferimenti da un titolare ad un responsabile fuori UE. Sono tutte riportate nelle Clausole contrattuali standard all'indirizzo: <https://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-internazionale/trasferimento-dei-dati-verso-paesi-terzi#2>;
 - ii) Clausole tipo adottate dalla DPA nazionale (novità): esse possono essere comunicate come "decisione di adozione" da parte del GDPD al Comitato per la protezione dati (EDPB), secondo l'art. 64.1.d, e approvate dalla Commissione europea secondo atti d'esecuzione, al fine di garantire un'omogenea applicazione della normativa all'interno di ciascuno stato membro e dell'UE.
 - iii) Clausole contrattuali ad hoc tra le parti: questa condizione di garanzia esplicita un requisito precedentemente più vago e, nel caso in cui le *model clause* siano stipulate tra il titolare o responsabile (esportatore) e l'importatore (altro titolare o responsabile extra UE), impone che tali contratti, anche di natura privata, siano sottoposti al GDPD. Questi ha il compito di autorizzarne la validità (art. 58 paragrafo 3.h) e di comunicare tale decisione al Comitato³ perché possa emettere un parere, secondo il principio di coerenza di cui all'art.63.

Le clausole-tipo di protezione dati non ammettono emendamenti e devono essere sottoscritte dalle parti. Solitamente riguardano solo gli aspetti inerenti la protezione dei dati⁴, pertanto vengono incorporate in un contratto più generale di Data Transfer e vi si possono aggiungere clausole ulteriori purché non in conflitto, direttamente o indirettamente, con quanto approvato dalla Commissione europea.

- d. Contratto di diritto amministrativo tra autorità o organismi pubblici: sono considerate garanzie adeguate le disposizioni inserite in accordi amministrativi tra tali soggetti pubblici se comprendono diritti effettivi e azionabili per gli interessati. Un esempio può essere rappresentato dal Memorandum d'intesa che, pur non

³ Comitato europeo per la protezione dei dati, di cui alla sezione 3 del GDPR

⁴ Ad esempio la Decisione 2010/87/CE per le clausole contrattuali tipo da Titolare a Responsabile prevede misure di sicurezza tecniche ed organizzative che il Responsabile è tenuto ad attuare, consente all'interessato di far valere contro il Titolare gli obblighi previsti nelle clausole o, qualora il Titolare sia scomparso o abbia cessato di esistere giuridicamente, di rivalersi contro il Responsabile, prevedendo la mediazione e giurisdizione di un terzo indipendente o autorità di controllo.

essendo un vero e proprio contratto, è un documento giuridico che esprime una convergenza di interessi fra le parti, indicando una comune linea di azione prestabilita e comune per i diritti effettivi ed azionabili degli interessati. Sempre per il principio di coerenza, anche in questo caso va subordinato ad autorizzazione del GDPR (art. 58 paragrafo 3.i) e deve seguire l'iter indicato al punto c.iii).

Da notare che l'ultimo capoverso del C109 invita i Titolari del Trattamento e i Responsabili del Trattamento a fornire garanzie *supplementari* attraverso impegni contrattuali che integrino le Clausole tipo di protezione dati. Allo stesso modo, i Codici di condotta (art. 40) e i Meccanismi di Certificazione (art. 42) costituiscono strumenti validi se accompagnati da un impegno vincolante ed esecutivo, assunto dalla parte stabilita nel paese extra UE, ad attuare garanzie adeguate rispetto ai principi di protezione dati, che prevedano sanzioni e meccanismi di esercizio dei diritti da parte degli interessati.

1.4 Trasferimento effettuato in base a deroghe

1.4.1 Deroghe e necessità

Scopo del GDPR è garantire agli interessati la disponibilità di diritti azionabili e mezzi di ricorso effettivi attraverso una serie di strumenti giuridici tipici per cui è consentito ricorrere al meccanismo delle deroghe, previste all'art. 49, **solo** eccezionalmente.

I trasferimenti fondati su una deroga non necessitano di alcuna autorizzazione preventiva del GDPR e presentano quindi rischi maggiori per i diritti e le libertà degli interessati; devono quindi essere interpretate in maniera restrittiva, rimanere un'eccezione e non una regola nei trasferimenti del Titolare.

Quando i trasferimenti avvengono nell'ambito della normale attività o prassi commerciale, devono essere messe in atto garanzie adeguate ai sensi dell'art. 46 piuttosto che ricorrere alle deroghe.

Con le Linee guida 2/2018 l'EDPB, basandosi sul documento WP 114 del gruppo WP29, ha fornito una serie di orientamenti per l'applicazione del meccanismo delle deroghe ai trasferimenti verso paesi terzi o organizzazioni internazionali, tenendo conto del C111 e ponendo, come presupposto di fondo per il ricorso alle deroghe, la "necessità" del trasferimento dei dati per una determinata finalità.

1.4.2 Test di necessità

Le deroghe di cui all'art.49 paragrafo 1 lettere da b) a f) prevedono che "il trasferimento sia necessario..". Tale condizione deve essere verificata mediante un test di necessità da parte del Titolare, volto ad evidenziare il nesso stretto e specifico tra i dati personali oggetto del trasferimento e le finalità del trattamento della specifica deroga che ritiene di applicare.

Il trasferimento può avvenire solo se le finalità sono necessarie, concrete e non presunte, o possibili, e i dati strettamente pertinenti e necessari allo scopo.

1.4.3 Quali rischi

Il gruppo di lavoro della Commissione Europea, già nel 1998⁵, riteneva che fra le categorie di trasferimenti che rappresentano una minaccia particolare per la vita privata e meritano quindi particolare attenzione siano comprese le seguenti:

- trasferimenti riguardanti le categorie particolari di dati;
- trasferimenti che comportano rischi di perdite finanziarie (ad esempio pagamenti con carta di credito attraverso Internet);
- trasferimenti che comportano rischi per la sicurezza personale;
- trasferimenti finalizzati all'adozione di una decisione particolarmente importante per la persona interessata (assunzioni, promozioni, concessione di un credito, ecc.);
- trasferimenti che rischiano di causare un grave imbarazzo a una persona o di lederne la reputazione;
- trasferimenti che possono condurre ad azioni specifiche che costituiscono un'ingerenza grave nella vita privata della persona;
- trasferimenti ripetuti che riguardano grandi volumi di dati (per es. dati su transazioni elaborati su reti di telecomunicazioni, Internet, ecc.);
- trasferimenti che comportano la raccolta di dati per mezzo di nuove tecnologie secondo modalità particolarmente occulte o clandestine (per es. i cosiddetti "cookies" di Internet), cui potrebbe oggi aggiungersi

⁵ Commissione europea, Gruppo di lavoro "Tutela delle persone fisiche con riguardo al trattamento dei dati personali" DG XV D/5025/98 WP 12

l'utilizzo diffuso di servizi in cloud anche per la gestione dei dati dei lavoratori o per lo scambio di dati per attività di lavoro e ricerca.

I rischi per i diritti e le libertà delle persone fisiche, di cui tenere conto, sono ulteriormente elencati ai considerando 75 e 76 del GDPR.

1.4.4 Matrice di applicazione delle deroghe

Di seguito viene riportata una schematizzazione delle condizioni di applicazione delle deroghe di cui al paragrafo 1 art.49 che, come già detto, sono da considerare residuali nel loro utilizzo, sottolineando che anche le deroghe non espressamente limitate ai trasferimenti "occasionalmente" e "non ripetitivi" devono essere interpretate come eccezionali rispetto alla regola.

	Eccezioni per la PA	Applicabile solo per Trasferimenti occasionali	Cosa aggiungere nell'informativa o al Registro dei trattamenti	Riferimenti e annotazioni
a. che l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'Interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate;	Non utilizzabile nell'esercizio di pubblici poteri (art.49.3)		Consenso come base giuridica, che deve essere esplicito, informato e specifico, indicando i paesi di destinazione, i destinatari o le categorie di destinatari, i possibili rischi derivanti dall'assenza, nel paese terzo, di un'autorità di controllo e la possibilità che non siano previsti principi di legittimità del trattamento e diritti per l'interessato mancando un parere di adeguatezza	Essendo possibile la revoca in qualsiasi momento non è utilizzabile per trasferimenti di lungo periodo. Il consenso deve essere <u>esplicito</u> , dopo minuziosa informazione dei possibili rischi, e nel pieno rispetto delle condizioni agli artt.4.11, 7, 13 e 14, dei C32, C33, C42 e C44 GDPR e delle linee guida sul consenso WP259 del WP29. La specificità impone che il consenso valga solo per quel trasferimento specifico di cui è informato e le circostanze del trasferimento non siano modificate dopo la prestazione del consenso.
b. che il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;	Non utilizzabile nell'esercizio di pubblici poteri (art.49.3)	SI	Occasionalità del trasferimento e quale sia il nesso stretto e significativo tra il trasferimento dei dati, i dati trasferiti e le finalità del contratto.	Non utilizzabile per trasferimenti di dati aggiuntivi, non strettamente necessari per l'esecuzione del contratto o delle misure precontrattuali. Nel caso di trasferimenti ripetuti devono essere utilizzate le misure di garanzie art.46.
c. che il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'Interessato;	Non utilizzabile nell'esercizio di pubblici poteri (art.49.3)	SI	Come per b)	Come per b)

d. che il trasferimento sia necessario per importanti motivi di interesse pubblico;	Cfr terzo capoverso 1.3.2 nel caso di richieste da paesi terzi, art.48			<p>In continuità con l'art.26.1.d della direttiva 95/46/CE il trasferimento può avvenire solo qualora sia necessario o prescritto dalla legge per la salvaguardia di un interesse pubblico rilevante, deducibile dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento, anche in virtù della reciprocità per la cooperazione internazionale sottoscritta tramite accordo o convenzione internazionale. Nel wp114 del 25 novembre 2015 il WP29 afferma che "questa deroga può essere utilizzata solo se il trasferimento è nell'interesse delle autorità stesse di uno Stato membro dell'Ue e non unicamente nell'interesse di una o più autorità di un paese terzo".</p> <p>Il requisito essenziale è nell'indicazione di un interesse pubblico, non nella natura dell'organizzazione che trasferisce o riceve i dati, che può essere anche privata (C111, C112)</p>
e. che il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;		SI		<p>Poiché il trasferimento deve essere effettuato nell'ambito del procedimento, è necessario un nesso stretto tra i dati trasferiti e il procedimento specifico relativo alla situazione in questione, non la mera possibilità che occorranza a tale scopo. I procedimenti devono avere un fondamento giuridico e possono includere la fase preprocessuale, l'apertura di un contenzioso o la richiesta di approvazione di una fusione. Nel diritto nazionale di alcuni Stati esistono i "blocking statutes" che impediscono o limitano i trasferimenti di dati personali verso autorità giudiziarie o talvolta organismi pubblici di paesi terzi. Occorrerebbe prima verificare se possano essere utilizzati dati anonimi o pseudonimizzati</p>
f. che il trasferimento sia necessario per tutelare gli interessi vitali dell'Interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;	SOLO quando l'interessato è nell'incapacità fisica o giuridica di prestare il consenso			<p>Se c'è capacità decisionale ed è possibile dare il consenso la deroga non è applicabile. Il trasferimento deve essere correlato all'interesse individuale dell'interessato o di un'altra persona e, nel caso di dati sanitari, deve essere necessario ai fini di una diagnosi essenziale. E' esclusa p.e. la ricerca medica che produrrà risultati solo in futuro. Il grave rischio imminente deve essere superiore rispetto le preoccupazioni connesse alla protezione dei dati</p>

<p>g. che il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può essere consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri;</p>				<p>La deroga si applica a dati contenuti in registri aventi la finalità di trasmettere informazioni al pubblico, non ai registri privati. Si tratta di registri che possono essere consultati dal pubblico, in generale, o da chiunque sia in grado di dimostrare un legittimo interesse (registri delle imprese, di condanne penali o casellario giudiziale, registri catastali, pubblici registri automobilistici ...). Non può riguardare la totalità dei dati né intere categorie di dati personali contenuti nel registro. Se il registro è costituito per legge per essere consultato da persone che hanno un legittimo interesse, il trasferimento può avvenire <u>su loro richiesta</u> o se ne sono destinatarie (quindi non tramite pubblicazione <i>erga omnes</i>), tenendo conto degli interessi e dei diritti fondamentali dell'interessato.</p>
---	--	--	--	--

<p>h. se non è ripetitivo, se riguarda un numero limitato di interessati, se è necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'Interessato; il titolare del trattamento deve aver valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei Dati Personali. Il titolare del trattamento informa del trasferimento l'Autorità di Controllo. In aggiunta alla fornitura di informazioni di cui agli artt. 13 e 14 GDPR, il titolare del trattamento informa l'Interessato del trasferimento e degli interessi legittimi cogenti perseguiti.</p>	<p>Non utilizzabile nell'esercizio di pubblici poteri (art.49.3) (è la condizione dal secondo capoverso lettera g, che nel testo originale è il secondo comma par.1)</p>	<p>SI</p>	<p>Il titolare deve informare l'interessato. Vanno descritti i legittimi interessi cogenti e i seri motivi per i quali non è stato possibile tutelare il trasferimento con garanzie adeguate o alcuna delle altre deroghe previste, inserendo i paesi destinatari. Devono essere indicate nel Registro dei trattamenti sia la valutazione delle circostanze relative al trasferimento sia le garanzie adeguate fornite a seguito della valutazione.</p>	<p>E' prevista come extrema ratio, applicabile solo nel caso in cui non è possibile basare il trasferimento su una disposizione art. 45 o 46 né su alcuna delle deroghe sopra elencate; ai sensi del C113, deve riguardare un numero limitato di interessati ed è subordinato alla concomitante sussistenza delle condizioni espressamente elencate nell'intero capoverso riportato dopo la lettera g) paragrafo 1 art.49. L'interesse legittimo deve essere cogente poiché non vi rientrano tutti i possibili interessi di cui all'art.6, paragrafo 1.f); deve esserne informato il GDPR</p>
--	--	-----------	---	---

Il paragrafo 5 dell'art.49 pone una deroga alle deroghe, lasciando possibilità all'Unione o agli Stati membri, in assenza di una decisione di adeguatezza, di fissare limiti al trasferimento di categorie specifiche di dati verso paesi esteri per importanti motivi di interesse pubblico, notificandolo alla Commissione.

1.5 Brexit

Dal 12 febbraio 2019 è stata diffusa una nota dell'EDPB con la quale si informa che, in assenza di un accordo fra i Paesi dello Spazio Economico Europeo (ossia UE + Norvegia, Liechtenstein, Islanda) e il Regno Unito, questi diverrà un Paese terzo. Conseguentemente, il trasferimento di dati personali verso il Regno Unito dovrà basarsi su uno degli strumenti giuridici finora indicati e secondo l'ordine di garanzia preferibile e riportato:

- Clausole-tipo di protezione dati o clausole ad-hoc;
- Norme vincolanti d'impresa;
- Codici di condotta e meccanismi di certificazione;
- Deroghe.

Nella stessa comunicazione si consiglia di iniziare a provvedere a 5 step di adeguamento a tale situazione, consistenti nell'individuare tra i trattamenti effettuati quali siano quelli che richiedono trasferimenti di dati verso il Regno Unito, individuare quali tra gli strumenti prima elencati possa essere applicato, implementare tale strumento provvedendo ad aggiornare i documenti interni (p.e. Registro dei trattamenti) e modificare le informative.

1.6 Sanzioni

Le sanzioni amministrative per le violazioni degli artt. da 44 a 49 sono previste all'art.83.5.c) e comportano, fatti salvi i principi di proporzionalità, importi fino a 20.000.000 € e da uno a tre anni di reclusione in base all'art.167 comma 3 D.Lgs. 196/2003.

2. Una casistica: il programma Erasmus+ extra UE

Il programma Erasmus+ è istituito con Regolamento(UE) 1288/2013 del Parlamento Europeo e del Consiglio dell'11 dicembre 2013 quale programma dell'Unione per l'istruzione, la formazione, la gioventù e lo sport. Esso contribuisce al conseguimento di vari obiettivi⁶, tra cui quelli in materia di istruzione, formazione e promozione dei valori europei, attraverso molteplici "azioni chiave". Tra queste, alcune sono volte sostenere la mobilità degli studenti e del personale per esperienze di apprendimento e/o professionali in altri paesi, anche tramite partenariati strategici transnazionali.

La responsabilità ultima del regolare funzionamento del Programma Erasmus+ spetta alla Commissione europea, che ne gestisce il bilancio e ne stabilisce costantemente priorità, obiettivi e criteri.

A livello europeo, l'Agenzia esecutiva per l'istruzione, gli audiovisivi e la cultura (Agenzia esecutiva) è responsabile in particolare dell'attuazione delle azioni centralizzate del Programma Erasmus+. Molte altre azioni sono decentrate e, in particolare, la Commissione europea affida le funzioni di esecuzione del bilancio alle Agenzie nazionali: per l'Italia, è l'Agenzia Indire.

Le Agenzie nazionali promuovono e realizzano il Programma a livello nazionale e fungono da tramite tra la Commissione europea e le organizzazioni partecipanti a livello locale, regionale e nazionale. Di norma, i partecipanti ai progetti Erasmus+ devono risiedere in uno dei paesi aderenti al Programma, tra cui ci sono anche paesi esterni all'UE.

Nell'ambito del programma Erasmus, gli accordi di cooperazione interuniversitaria e di mobilità possono essere quindi stipulati anche con atenei collocati in paesi terzi per:

- a) Scambio di visite di docenti e ricercatori impegnati nell'attività di ricerca o organizzazione congiunta d'incontri, seminari, corsi di formazione e attività di docenza;
- b) Scambio di dottorandi, dottori di ricerca, assegnisti di ricerca e giovani ricercatori;
- c) Scambio di studenti;
- d) Altre forme di cooperazione: progetti comuni di ricerca, sostegno all'avvio di una struttura di ricerca o progetti di sviluppo, etc.

Tali accordi possono avere la forma di "accordi quadro" all'interno dei quali stipulare, di volta in volta, accordi inerenti una delle specifiche situazioni tra quelle appena citate.

⁶ https://ec.europa.eu/programmes/erasmus-plus/programme-guide/part-a/objectives-and-important-features/general-objective_it

Venendo alle finalità di approfondimento del trasferimento dei dati, dalle modalità di istituzione del programma consegue che i trattamenti sono effettuati ai sensi dell'art. 6 lettera e) del GDPR ossia "il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento" - e ai sensi dell'art.6 lettera c), anche per gli obblighi derivanti dall'adesione dell'Ateneo al programma Erasmus+.

I trattamenti dei dati dei candidati al programma avvengono sia da parte degli Atenei che da parte dell'Agenzia nazionale o di quella esecutiva; questi ultimi, sono descritti all'indirizzo https://ec.europa.eu/programmes/erasmus-plus/programme-guide/part-c/important-contractual-provisions/data-protection_it⁷ e integrano i trattamenti dei dati effettuati dall'Ateneo in conseguenza della candidatura dello studente, per i quali è dovuta l'informativa.

Come avviene per altre tipologie di contratti o convenzioni, l'individuazione degli Atenei contraenti come Titolari autonomi o Contitolari dipende dall'impostazione data sulle finalità e modalità dei trattamenti che sono oggetto dell'accordo. In ogni caso, **salvo** la presenza di una decisione di adeguatezza inerente il Paese dell'Ateneo estero, occorre seguire una delle seguenti strade:

- a) Aggiungere all'accordo la sottoscrizione di una clausola contrattuale tipo adottata in base alla Decisione della Commissione europea, ad esempio quella del 27 dicembre 2004 (2004/915/CE) - che modifica la decisione 2001/497/CE - per il trasferimento di dati personali a titolare stabilito in un paese estero. Essendo state adottate prima dell'entrata in vigore del GDPR, occorre intervenire nella terminologia (Titolare, dati particolari,.. al posto di Responsabile, dati sensibili,..) oltre alla specifica di quanto necessario per l'applicazione al caso concreto e che, in ogni caso, non dovrà essere incompatibile con il contenuto delle clausole.

Il documento che riporta in allegato la clausola, composta da tre elementi, è rinvenibile ai seguenti indirizzi, rispettivamente per la lingua italiana, inglese, francese e spagnola:

<https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32004D0915&from=IT>
<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32004D0915&from=EN>
<https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32004D0915&from=FR>
<https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32004D0915&from=ES>

Può essere utilizzata anche la clausola contrattuale adottata con decisione 2001/497/CE, che è stata modificata e affiancata, ma non sostituita, da quella appena proposta.

- b) Utilizzare la base di garanzia prevista all'art. 46 paragrafo 3 lettera b), ossia "disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli Interessati", che possono essere predisposte dall'Ateneo ma devono essere sottoposte all'autorizzazione preventiva del Garante.

Nel caso di singoli accordi, da ritenersi comunque nell'eccezionalità alla regola, non è escludibile il ricorso alla deroga del consenso, di cui all'art.49 paragrafo 1 lettera a), ferme restando le condizioni già descritte per lo specifico caso.

3. Conclusione

Il trasferimento verso paesi terzi è considerato un trattamento ad alto rischio per le libertà e i diritti fondamentali e pertanto può avere luogo solo nel rispetto delle condizioni di cui al Capo V che sono state qui riportate, sia che riguardino progetti di ricerca, mobilità del personale e degli studenti, richieste di dati provenienti da paesi terzi, p.e. inerenti curriculum di laureati o dipendenti dell'ateneo, l'utilizzo di piattaforme che non garantiscono la collocazione dei datacenter su territorio UE e altre casistiche anche frequenti in ambito universitario. Con il GDPR le decisioni di adeguatezza possono essere revocate e, in condizioni particolari, anche in tempi molto brevi per cui, nei casi di movimenti della scena politica del paese di destinazione che potrebbero inficiare i presupposti di adeguatezza, su cui si fonda una decisione esistente, e siano già osservabili al momento di avviare un trasferimento, si potrebbe preferire il ricorso a garanzie specifiche anzi descritte. In questo caso infatti il trasferimento troverebbe una base di legittimità che prescinde dalla presenza della decisione stessa e quindi dalla sua eventuale revoca.

Solo come annotazione finale, riguardo i trasferimenti in USA⁸, l'Edpb ha recentemente ribadito, nella sesta riunione plenaria di fine gennaio, le preoccupazioni sull'accordo per lo scambio di dati personali fra UE e USA, *cd.* 'Privacy Shield', che ha sostituito il precedente Safe Harbour, inibito da una sentenza della Corte UE. Nonostante i progressi fatti dagli

⁷ L'indirizzo riporta il riferimento al Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati, ora sostituito dal Regolamento UE 1725/2018

⁸ <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5306161>

USA nel garantire gli impegni presi con l'UE, mancano ancora garanzie concrete e verificabili rispetto ad una raccolta indiscriminata di dati personali, attuata p.e. per motivi di sicurezza. Inoltre il Comitato non può attualmente ritenere che il mediatore (Ombudsperson) sia dotato di poteri sufficienti per porre rimedio alle non conformità e fa notare che i controlli relativi al rispetto sostanziale dei principi dello Scudo per la privacy non sono sufficientemente forti.