Linee Guida

Linee guida 7/2022 sulla certificazione come strumento per i trasferimenti

Versione 2.0

Adottate il 14 febbraio 2023

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

CRONOLOGIA DELLE VERSIONI

Versione 1.0	14 giugno 2022	Adozione delle linee guida per la consultazione pubblica
Versione 2.0	14 febbraio 2023	Adozione delle linee guida dopo la consultazione pubblica

SINTESI

L'articolo 46 del regolamento generale sulla protezione dei dati (GDPR) impone agli esportatori di dati di fornire garanzie adeguate per i trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali. A tal fine, il GDPR diversifica le garanzie adeguate che possono essere utilizzate dagli esportatori di dati a norma dell'articolo 46 per inquadrare i trasferimenti verso paesi terzi introducendo, tra l'altro, la certificazione come nuovo meccanismo per i trasferimenti (articolo 42, paragrafo 2, e articolo 46, paragrafo 2, lettera f), GDPR).

Le presenti linee guida forniscono orientamenti relativi all'applicazione dell'articolo 46, paragrafo 2, lettera f), GDPR ai trasferimenti di dati personali verso paesi terzi o verso organizzazioni internazionali sulla base della certificazione. Il documento è strutturato in quattro sezioni, con un allegato.

La prima parte del presente documento ("ASPETTI GENERALI") precisa che le linee guida integrano le linee guida 1/2018 relative alla certificazione, già esistenti e di carattere generale, e tratta i requisiti specifici di cui al capo V GDPR per i casi in cui la certificazione è utilizzata come strumento di trasferimento. In virtù dell'articolo 44 GDPR, qualunque trasferimento di dati personali verso paesi terzi o organizzazioni internazionali deve soddisfare le condizioni previste dalle altre disposizioni del GDPR, oltre a rispettare il capo V GDPR. Di conseguenza, in primo luogo, è necessario garantire la conformità alle disposizioni generali del GDPR e, in secondo luogo, deve essere rispettato quanto disposto dal capo V GDPR. Sono descritti i soggetti coinvolti e i loro principali ruoli in tale contesto, con un'attenzione particolare al ruolo dell'importatore di dati cui sarà rilasciata una certificazione e dell'esportatore di dati che la utilizzerà come strumento per inquadrare i suoi trasferimenti (tenendo conto del fatto che la responsabilità del rispetto del trattamento dei dati continua a ricadere sull'esportatore di dati). In tale contesto, la certificazione può anche comprendere misure che integrano gli strumenti di trasferimento al fine di garantire la conformità con il livello unionale di protezione dei dati personali. La prima parte delle linee guida contiene altresì informazioni sulla procedura per l'ottenimento di una certificazione da utilizzare come strumento per i trasferimenti.

La seconda parte delle presenti linee guida ("ORIENTAMENTI DI ATTUAZIONE RELATIVI AI REQUISITI DI ACCREDITAMENTO") ricorda che i requisiti per l'accreditamento di un organismo di certificazione vanno ricercati nella ISO 17065, come pure nell'interpretazione delle linee guida 4/2018 relative all'accreditamento degli organismi di certificazione a norma dell'articolo 43 GDPR e relativo allegato alla luce del contesto del capo V. Tuttavia, nell'ambito di un trasferimento, le presenti linee guida illustrano ulteriormente alcuni dei requisiti di accreditamento applicabili all'organismo di certificazione.

La terza parte delle presenti linee guida ("CRITERI DI CERTIFICAZIONE SPECIFICI") fornisce orientamenti sui criteri di certificazione già illustrati nelle linee guida 1/2018 e stabilisce criteri specifici aggiuntivi che dovrebbero essere compresi in un meccanismo di certificazione da utilizzare come strumento per i trasferimenti verso paesi terzi. Tali criteri riguardano la valutazione della legislazione del paese terzo, gli obblighi generali degli esportatori e degli importatori, le norme sui trasferimenti successivi, le misure di ricorso e attuazione, le procedure e gli interventi per le situazioni in cui le pratiche e la legislazione nazionali impediscono il rispetto degli impegni presi nel contesto della certificazione nonché le richieste di accesso ai dati da parte di autorità di paesi terzi.

La quarta parte delle presenti linee guida ("IMPEGNI VINCOLANTI E AZIONABILI DA ATTUARE") illustra gli elementi che dovrebbero essere presi in considerazione negli impegni vincolanti e azionabili che i titolari del trattamento o i responsabili del trattamento non soggetti al GDPR dovrebbero assumere

per fornire garanzie adeguate ai dati trasferiti verso paesi terzi. Tali impegni, che possono essere definiti in vari strumenti, anche contrattuali, prevedono segnatamente una garanzia riguardo al fatto che l'importatore non ha motivo di ritenere che le norme e le pratiche del paese terzo applicabili al trattamento in esame, ivi compresi eventuali requisiti riguardanti la comunicazione di dati personali o misure che autorizzano l'accesso da parte delle autorità pubbliche, gli impediscano di adempiere ai suoi impegni nel quadro della certificazione.

L'ALLEGATO delle presenti linee guida contiene alcuni esempi di misure supplementari in linea con quelle illustrate nell'allegato II delle raccomandazioni 01/2020 (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) nel contesto dell'utilizzo di una certificazione come strumento per i trasferimenti. Gli esempi sono concepiti nell'ottica di portare l'attenzione a situazioni critiche.

INDICE

Il Comitato europeo per la protezione dei dati

visto l'articolo 70, paragrafo 1, lettera e), del 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),

visto l'accordo SEE, in particolare l'allegato XI e il protocollo 37, modificati dalla decisione del Comitato misto SEE n. 154/2018 del 6 luglio 2018[1],

visti gli articoli 12 e 22 del proprio regolamento interno,

HA ADOTTATO LE SEGUENTI LINEE GUIDA

1 ASPETTI GENERALI

1.1 Scopo e ambito di applicazione

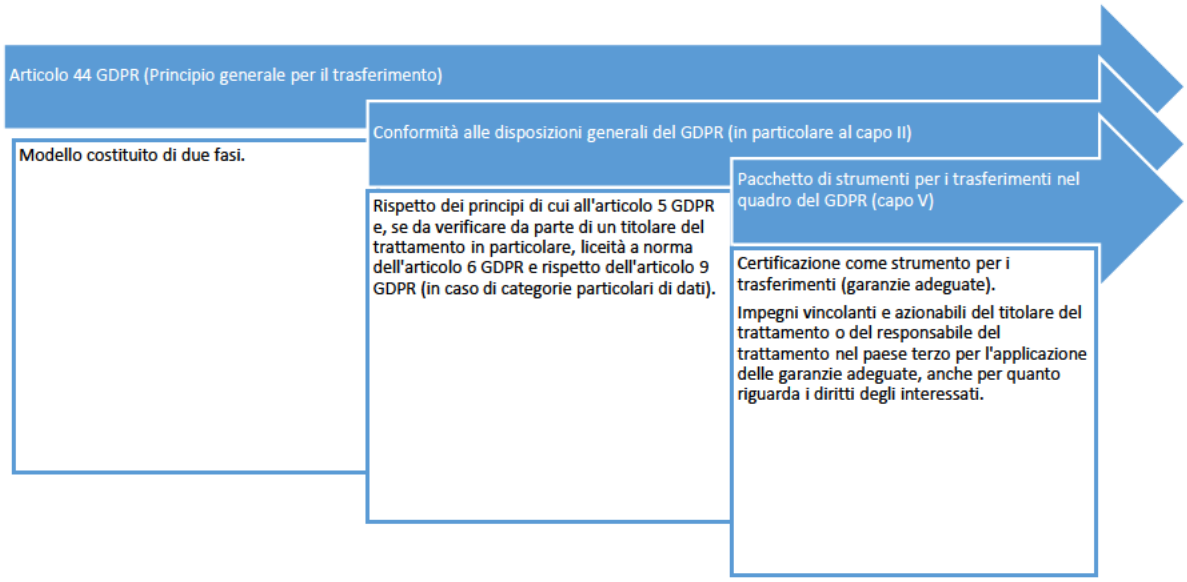
1. Il presente documento intende fornire orientamenti relativi all'applicazione dell'articolo 46, paragrafo 2, lettera f), del regolamento generale sulla protezione dei dati (GDPR) ai trasferimenti di dati personali verso paesi terzi o verso organizzazioni internazionali sulla base della certificazione. Il Comitato europeo per la protezione dei dati (EDPB) ha già pubblicato orientamenti generali in materia di certificazione[2] e accreditamento[3] nel quadro del GDPR. Tali nuove linee guida riguardano pertanto solo gli aspetti specifici relativi alla certificazione come strumento per i trasferimenti. Precisano l'applicazione dell'articolo 46, paragrafo 2, lettera f), e dell'articolo 42, paragrafo 2, GDPR, fornendo orientamenti pratici a tale proposito e introducendo elementi nuovi rispetto alle linee guida già pubblicate.

2. L'EDPB valuterà il funzionamento delle presenti linee guida alla luce dell'esperienza acquisita nella loro applicazione pratica e fornirà ulteriori orientamenti per chiarire l'applicazione degli elementi illustrati di seguito, ivi compreso il ruolo dell'accordo di certificazione per quanto concerne gli impegni vincolanti e azionabili di cui all'articolo 46, paragrafo 2, lettera f), GDPR.

1.2 Norme generali applicabili ai trasferimenti internazionali

3. In virtù dell'articolo 44 GDPR, qualunque trasferimento di dati personali verso paesi terzi[4] o organizzazioni internazionali deve soddisfare le condizioni previste dalle altre disposizioni del GDPR, oltre a rispettare il capo V GDPR. Di conseguenza, ciascun trasferimento deve rispettare, tra l'altro, i principi sulla protezione dei dati di cui all'articolo 5 GDPR, essere lecito in conformità dell'articolo 6 GDPR e ottemperare all'articolo 9 GDPR in caso di categorie particolari di dati. Deve pertanto essere applicata una verifica composta di due fasi. In primo luogo, è necessario garantire la conformità alle disposizioni generali del GDPR e, in secondo luogo, deve essere rispettato quanto disposto nel capo V GDPR.

[1] Nel presente documento con il termine "Stati membri" si intendono gli "Stati membri del SEE".
[2] Linee guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione in conformità degli articoli 42 e 43 del regolamento (UE) 2016/679.
[3] Linee guida 4/2018 relative all'accreditamento degli organismi di certificazione a norma dell'articolo 43 del regolamento generale sulla protezione dei dati (regolamento (UE) 2016/679).
[4] Linee guida 05/2021 sull'interazione tra l'applicazione dell'articolo 3 e le disposizioni sui trasferimenti internazionali a norma del capo V GDPR, pagina 4.



4. All'articolo 46, il GDPR precisa che "in mancanza di una decisione ai sensi dell'articolo 45, paragrafo 3, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi". A norma dell'articolo 46, paragrafo 2, lettera f), GDPR, tali garanzie adeguate possono essere previste da un meccanismo di certificazione approvato 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.

5. Di conseguenza, l'esportatore di dati potrebbe decidere di basarsi sulla certificazione ottenuta da un importatore di dati quale elemento per dimostrare l'adempimento dei suoi obblighi, ad esempio in conformità dell'articolo 24, paragrafo 3, o dell'articolo 28, paragrafo 5, GDPR. L'importatore di dati potrebbe decidere di chiedere la certificazione per dimostrare che sono predisposte garanzie adeguate.

6. Entrambi, l'esportatore di dati e l'importatore di dati, possono svolgere ruoli diversi (ad esempio quello di titolare del trattamento o di responsabile del trattamento)[5], a seconda del trattamento di cui al capo V, con conseguenti responsabilità diverse:

7. Oltre all'utilizzo della certificazione o di qualsiasi altro meccanismo o strumento di trasferimento di cui agli articoli 45 e 46, l'articolo 49 GDPR prevede per un numero limitato di situazioni specifiche che i

[5] Cfr. di seguito: ORIENTAMENTI DI ATTUAZIONE RELATIVI AI CRITERI DI CERTIFICAZIONE.

trasferimenti di dati internazionali siano ammessi nei casi in cui non è rispettato alcun altro meccanismo di cui al capo V[6]. Tuttavia, come illustrato negli orientamenti precedentemente pubblicati dall'EDPB, le deroghe di cui all'articolo 49 GDPR devono essere interpretate in senso restrittivo e riguardano principalmente attività di trattamento che sono occasionali e non ripetitive[7].

1.3 Quali sono i soggetti coinvolti e qual è il loro ruolo per la certificazione come strumento per i trasferimenti?

8. All'**EDPB** è conferito il potere di approvare criteri di certificazione validi per tutto il SEE (sigillo europeo per la protezione dei dati) e di fornire pareri sui progetti di decisione delle autorità di controllo riguardo ai criteri di certificazione e ai requisiti di accreditamento degli organismi di certificazione al fine di garantire la coerenza. È altresì competente a raccogliere in un registro tutti i meccanismi di certificazione e i sigilli e i marchi di protezione dei dati nonché a renderli pubblici[8].

9. Le **autorità di controllo** approvano i criteri per la certificazione quando il meccanismo di certificazione non è un sigillo europeo per la protezione dei dati[9]. Potrebbero altresì accreditare l'organismo di certificazione, elaborare i criteri di certificazione e rilasciare la certificazione se previsto dal diritto nazionale del loro Stato membro[10].

10. L'**organismo nazionale di accreditamento** può accreditare organismi di certificazione terzi ricorrendo alla ISO 17065 e ai requisiti di accreditamento aggiuntivi delle autorità di controllo, che dovrebbero essere in linea con la sezione 2 delle presenti linee guida. In alcuni Stati membri, l'accreditamento può essere offerto anche dall'autorità di controllo competente nonché essere effettuato da un organismo nazionale di accreditamento o da entrambi.

11. Il **proprietario dello schema** è un'organizzazione che ha stabilito criteri di certificazione e i requisiti metodologici in base ai quali deve essere valutata la conformità. L'organismo che effettua le valutazioni potrebbe essere la stessa organizzazione che ha sviluppato lo schema e ne è proprietaria, ma potrebbero sussistere accordi in base ai quali un'organizzazione è proprietaria dello schema e un'altra (o più di un'altra) effettua le valutazioni in qualità di organismo di certificazione.

12. A seconda del diritto nazionale, in alternativa alle autorità di controllo, l'**organismo di certificazione** accreditato come sopra descritto può rilasciare le certificazioni[11]. Potrebbe elaborare i criteri per la certificazione e, pertanto, costituire il proprietario dello schema (cfr. paragrafo 11 sopra) e deve essere stabilito nel SEE, in particolare al fine di consentire l'esercizio effettivo dei poteri correttivi di cui all'articolo 58, paragrafo 2, lettera f), GDPR. L'organismo di certificazione potrebbe però affidare in subcontratto le attività a esperti locali o stabilimenti al di fuori del SEE che svolgeranno le attività di verifica per suo conto[12]. Tuttavia, l'organismo di certificazione non affida in subcontratto la decisione di rilasciare o meno una certificazione.

---

[6] Per maggiori informazioni sull'articolo 49 e sulla sua interazione con l'articolo 46 in generale, cfr. le linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679.
[7] Linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679, pagina 5.
[8] Articolo 42, paragrafo 8, GDPR.
[9] Linee guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione in conformità degli articoli 42 e 43 del regolamento (UE) 2016/679, sezione 2.2.
[10] Articolo 42, paragrafo 5, e articolo 43, paragrafo 1, GDPR.
[11] Articolo 42, paragrafo 5, GDPR.
[12] Gli organismi di certificazione devono valutare i loro esperti locali in conformità della norma ISO 17065 e dei requisiti aggiuntivi per l'accreditamento stabiliti dall'autorità di controllo (articolo 43, paragrafo 1, lettera b), GDPR).

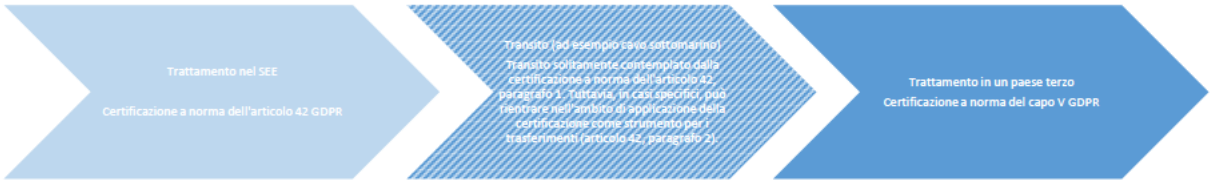
13. L'**importatore di dati** è l'entità (titolare del trattamento o responsabile del trattamento) nel paese terzo che riceve i dati da un esportatore di dati.

14. L'**esportatore di dati** è l'entità (titolare del trattamento o responsabile del trattamento) che trasferisce i dati dal SEE verso un importatore di dati. L'esportatore di dati deve garantire il rispetto del capo V.

1.4 Quali sono l'ambito di applicazione e l'oggetto della certificazione come strumento per i trasferimenti?

15. Un meccanismo di certificazione come strumento per il trasferimento a norma dell'articolo 42, paragrafo 2, deve essere finalizzato ad assicurare garanzie adeguate per il trattamento dei dati personali ai sensi dell'articolo 46, paragrafo 2, lettera f). La certificazione dimostra l'esistenza di garanzie adeguate fornite dai titolari del trattamento o dai responsabili del trattamento al di fuori del SEE o che costituiscono un'organizzazione internazionale che riceve dati da titolari del trattamento o responsabili del trattamento nel SEE per contrastare i rischi specifici del trasferimento di dati personali.

16. In generale, l'operazione di trasferire dati personali da uno Stato membro verso un paese terzo costituisce, in quanto tale, un trattamento di dati personali ai sensi dell'articolo 4, punto 2, GDPR, effettuato nel territorio di uno Stato membro[13] e pertanto certificabile a norma dell'articolo 42, paragrafo 1, GDPR. Tuttavia, a seconda del contesto, in alcune situazioni il transito potrebbe rientrare nell'ambito di applicazione della certificazione come strumento per i trasferimenti. Di conseguenza, l'oggetto della certificazione (che coincide con l'oggetto della valutazione durante la certificazione[14]) dovrebbe generalmente essere il trattamento dei dati ricevuti dal SEE da parte dell'importatore di dati nel paese terzo e il transito, se sotto il controllo dell'importatore.



17. L'oggetto della certificazione può essere un singolo trattamento o una serie di trattamenti. Tra questi possono rientrare i processi di governance intesi come misure organizzative e quindi come parti integranti di un trattamento[15].

18. L'entità che effettua la richiesta sarebbe pertanto l'importatore di dati nel paese terzo in relazione al suo oggetto della certificazione.

---

[13] Sentenza della Corte di giustizia dell'Unione europea nella causa C-311/18, Data Protection Commissioner contro Facebook Ireland Ltd e Maximillian Schrems, punto 83.
[14] Linee guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione in conformità degli articoli 42 e 43 del regolamento (UE) 2016/679, pagina 17.
[15] Linee guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione in conformità degli articoli 42 e 43 del regolamento (UE) 2016/679, pagina 16 (ad esempio meccanismo di gestione dei reclami).

1.5 Quale dovrebbe essere il ruolo dell'esportatore nell'utilizzo della certificazione come strumento per i trasferimenti?

19. Generalmente, il trasferimento da parte dell'esportatore di dati in quanto tale rientra direttamente nel quadro del GDPR. Ciò significa che l'esportatore è tenuto ad adempiere ai propri obblighi in forza del GDPR e segnatamente a garantire che i dati siano trasferiti in modo sicuro conformemente all'articolo 32 e al capo V al fine di assicurare che il livello di protezione delle persone fisiche garantito da tale regolamento non sia pregiudicato (articolo 44 GDPR)[16]. Ciò può essere ovviamente certificato a norma dell'articolo 42, paragrafo 1.

20. Inoltre, l'esportatore di dati che desidera ricorrere a una certificazione quale garanzia adeguata in base all'articolo 46, paragrafo 2, lettera f), GDPR è in particolare tenuto a verificare se la certificazione cui intende fare affidamento è efficace alla luce delle caratteristiche del trattamento previsto. A tale scopo, l'esportatore di dati deve controllare la certificazione rilasciata al fine di verificare se il certificato è valido e non scaduto, se contempla il trasferimento specifico da effettuare e se il transito di dati personali rientra nell'ambito di applicazione della certificazione, come pure se sono previsti trasferimenti successivi ed è fornita una documentazione adeguata su questi ultimi. L'esportatore deve inoltre controllare che l'organismo di certificazione che rilascia la certificazione sia accreditato da un organismo nazionale di accreditamento o un'autorità di controllo competente. L'esportatore di dati dovrebbe altresì fare riferimento all'utilizzo della certificazione come strumento di trasferimento nel contratto relativo al trattamento dei dati a norma dell'articolo 28 GDPR in caso di trasferimenti dal titolare del trattamento al responsabile del trattamento o in un contratto sulla condivisione dei dati con l'importatore di dati in caso di trasferimenti tra titolari del trattamento.

21. Tenendo conto del fatto che è responsabile dell'applicazione di tutte le disposizioni di cui al capo V, l'esportatore deve altresì valutare se la certificazione su cui intende fare affidamento come strumento per i trasferimenti è efficace alla luce delle normative e delle pratiche in vigore nel paese terzo pertinenti per il trasferimento in esame. Ai fini di tale valutazione e quale elemento significativo attraverso cui dimostrare l'adempimento delle proprie responsabilità, l'esportatore di dati può fare affidamento sulla verifica effettuata dall'organismo di certificazione della valutazione documentata dell'importatore delle normative e delle pratiche del paese terzo.

22. Qualora la valutazione dell'importatore avesse rivelato che quest'ultimo e/o l'esportatore di dati può essere tenuto a fornire misure supplementari previste dalla certificazione per garantire un livello di protezione sostanzialmente equivalente a quello fornito nel SEE, l'esportatore di dati deve verificare le misure supplementari fornite dall'importatore di dati in possesso di una certificazione e se è in grado di dare seguito alle misure tecniche e (se del caso) supplementari richieste dall'importatore di dati.

---

[16] A tale proposito, è importante notare che l'articolo 44 GDPR prevede chiaramente che un trasferimento possa essere svolto non solo da un titolare del trattamento ma anche da un responsabile del trattamento. Si verificherà pertanto un trasferimento qualora un responsabile del trattamento invii dati a un altro responsabile del trattamento o persino a un titolare del trattamento in un paese terzo su istruzione del suo titolare del trattamento (articolo 28, paragrafo 3, lettera a), GDPR). In tali casi, il responsabile del trattamento agisce da esportatore di dati per conto del titolare del trattamento ed è tenuto a garantire il rispetto di quanto disposto nel capo V per il trasferimento in esame sulla base delle istruzioni del titolare del trattamento, ivi compreso il fatto che sia utilizzato uno strumento adeguato per il trasferimento. Siccome il trasferimento è un'attività di trattamento effettuata per conto del titolare del trattamento, quest'ultimo è anche competente e potrebbe essere responsabile a norma del capo V ed è pure tenuto a garantire che il responsabile del trattamento fornisca garanzie sufficienti a norma dell'articolo 28.

23. Se tali requisiti non sono soddisfatti, l'esportatore di dati dovrà chiedere all'importatore di attuare misure supplementari adattate o stabilirle autonomamente.

1.6 Qual è la procedura per la certificazione come strumento per i trasferimenti?

24. La certificazione è facoltativa, ma quando richiesta deve essere rilasciata attraverso una procedura trasparente basata su norme imperative. Il GDPR pone una fiducia considerevole nei meccanismi di certificazione privati quali "autoregolamentazione regolamentata". Di conseguenza, tali meccanismi devono garantire che i certificati soddisfino sostanzialmente i requisiti sulle garanzie adeguate di cui all'articolo 46 GDPR.

25. La certificazione deve pertanto basarsi sulla valutazione dei criteri di certificazione conformemente a una metodologia di verifica vincolante. Tali criteri saranno approvati dalle autorità di controllo nazionali o dall'EDPB secondo quanto illustrato nell'articolo 42, paragrafo 5, GDPR. I criteri per la certificazione comprendono i requisiti per una valutazione del trattamento effettuato dall'importatore di dati, ivi compresi i trasferimenti successivi, nonché del quadro giuridico pertinente del paese terzo, onde evitare che le norme e le pratiche del paese terzo impediscano all'importatore di adempiere agli obblighi che incombono su quest'ultimo in forza della certificazione.

26. Durante il processo di certificazione, l'oggetto della valutazione è controllato conformemente ai criteri di certificazione da un organismo di certificazione accreditato dall'organismo nazionale di accreditamento o dall'autorità di controllo competente[17].

27. In base all'articolo 43, paragrafo 1, GDPR, gli organismi di certificazione in possesso del livello adeguato di competenze riguardo alla protezione dei dati rilasciano e rinnovano la certificazione, dopo averne informato l'autorità di controllo al fine di consentire alla stessa di esercitare i suoi poteri a norma dell'articolo 58, paragrafo 2, lettera h), GDPR, ove necessario.

28. In base all'articolo 43, paragrafo 5, GDPR, gli organismi di certificazione trasmettono alle autorità di controllo competenti i motivi del rilascio o della revoca della certificazione richiesta. Ciò non significa che l'organismo di certificazione abbia bisogno dell'autorizzazione dell'autorità di controllo per il rilascio della certificazione. L'organismo di certificazione monitorerà il rispetto dei criteri di certificazione da parte dei suoi clienti.

29. L'autorità di controllo dispone del potere correttivo di revocare una certificazione o di ingiungere di ritirare una certificazione rilasciata a norma degli articoli 42 e 43 GDPR oppure di ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono più soddisfatti.

30. Un sigillo europeo per la protezione dei dati per i trasferimenti di dati internazionali può fungere da strumento per contemplare i trasferimenti verso paesi terzi unitamente a impegni vincolanti e azionabili[18].

31. Tuttavia, le certificazioni da utilizzare come strumento per i trasferimenti possono essere altresì rilasciate in base a schemi di certificazione approvati nazionali negli Stati del SEE. In quanto tali, sono

[17] Linee guida 4/2018 relative all'accreditamento degli organismi di certificazione a norma dell'articolo 43 del regolamento generale sulla protezione dei dati (regolamento (UE) 2016/679), pagina 9.
[18] Cfr. l'articolo 42, paragrafo 5, GDPR e il paragrafo 35 delle linee guida 1/2018 dell'EDPB relative alla certificazione e all'identificazione di criteri di certificazione in conformità degli articoli 42 e 43 del regolamento (UE) 2016/679.

valide solo per i trasferimenti verso paesi terzi da parte degli esportatori nello Stato membro del SEE in cui lo schema di certificazione è stato approvato, in quanto non sussiste alcun reciproco riconoscimento delle certificazioni dei diversi Stati del SEE. Le autorità di controllo di Stati del SEE diversi hanno tuttavia la facoltà di approvare il medesimo meccanismo di certificazione per i trasferimenti[19].

2 ORIENTAMENTI DI ATTUAZIONE RELATIVI AI REQUISITI DI ACCREDITAMENTO

32. I requisiti di accreditamento di un organismo di certificazione per quanto riguarda le certificazioni come strumento per i trasferimenti vanno ricercati nella ISO 17065 e nell'interpretazione delle linee guida 4/201820 alla luce del contesto del capo V, come sotto illustrato.

33. A parere dell'EDPB, i requisiti aggiuntivi di accreditamento elaborati sulla base delle linee guida 4/2018 e della ISO 17065 adottati conformemente all'articolo 64, paragrafo 1, lettera c), GDPR comprendono già i requisiti specifici necessari per l'accreditamento di un organismo di certificazione per quanto riguarda le certificazioni come strumento per i trasferimenti. Tuttavia, nel contesto dei trasferimenti, alcuni requisiti necessitano di qualche miglioria in termini di interpretazione e note esplicative.

34. In relazione ai requisiti per le risorse (cfr. allegato 1, requisito 6, delle linee guida 4/2018), l'organismo di certificazione garantisce di disporre delle risorse necessarie per essere in grado di verificare che, secondo quanto previsto dai criteri di certificazione, l'importatore abbia svolto debitamente e correttamente la necessaria valutazione della situazione giuridica e delle pratiche del/i paese/i terzo/i in cui è stabilito oppure opera[21]. Tale valutazione dovrebbe essere svolta in relazione alle attività di trattamento da certificare nel contesto dell'oggetto della valutazione per quanto riguarda le garanzie adeguate di cui all'articolo 46 GDPR e, ove necessario, comprende le misure supplementari individuate e attuate dall'importatore. Ciò comprende anche, ad esempio, una conoscenza significativa delle normative e delle pratiche locali pertinenti, come pure competenze linguistiche adeguate in relazione al/i paese/i terzo/i.

35. Per quanto riguarda i requisiti di processo (cfr. allegato 1, requisito 7, delle linee guida 4/2018), l'organismo di certificazione garantisce che il processo di certificazione possa essere coadiuvato da possibili verifiche in loco, sia svolto in relazione al trattamento che avverrà nel/i paese/i terzo/i e che la valutazione riguardi anche l'attuazione pratica delle normative e delle politiche vigenti nel/i paese/i terzo/i.

36. Per quanto concerne i requisiti relativi alle modifiche che influenzano la certificazione (cfr. allegato 1, requisito 7.10, delle linee guida 4/2018), l'organismo di certificazione monitora le modifiche nella legislazione e/o nella giurisprudenza del paese terzo che possono influire sul trattamento che rientra nell'ambito di applicazione dell'oggetto della valutazione.

---

[19] Se un'autorità di controllo guida l'adozione dei criteri di certificazione X nel quadro della sua iniziativa nazionale e, successivamente, tenendo conto dei criteri dello schema e delle normative nazionali specifiche applicabili, altri paesi desiderano adottare i medesimi criteri di certificazione, tali paesi possono adottarli senza richiedere un parere dell'EDPB a norma dell'articolo 64 GDPR e basarsi sul parere fornito alla prima autorità di controllo, conformemente all'articolo 64, paragrafo 3, GDPR [cfr. a tale proposito, Orientamenti – Addendum (Allegato delle linee guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione in conformità degli articoli 42 e 43 del regolamento (UE) 2016/679), paragrafo 66].

[20] Linee guida 4/2018 relative all'accreditamento degli organismi di certificazione a norma dell'articolo 43 del regolamento generale sulla protezione dei dati e relativo allegato.

[21] Cfr. il precedente paragrafo 12.

3 CRITERI DI CERTIFICAZIONE SPECIFICI

37. Nel contesto dell'esame dei criteri di certificazione specifici, le presenti linee guida si basano sulle linee guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione in conformità degli articoli 42 e 43 del regolamento (UE) 2016/679 (versione 3. 0), sul rispettivo allegato 2 relativo al riesame e alla valutazione dei criteri di certificazione di cui all'articolo 42, paragrafo 5, nonché sull'addendum degli orientamenti sulla valutazione dei criteri di certificazione.

38. A parere dell'EDPB, i criteri di certificazione elaborati sulla base dell'allegato 2 delle linee guida 1/2018 nonché dell'addendum degli orientamenti sulla valutazione dei criteri di certificazione comprendono già la maggior parte dei criteri di certificazione che devono essere presi in considerazione nell'elaborazione di uno schema di certificazione da utilizzare come strumento per i trasferimenti. Tuttavia, potrebbe essere necessario precisare ulteriormente alcuni di tali criteri vigenti per adeguarli al contesto specifico di un trasferimento (cfr. paragrafo 3.1). Potrebbe inoltre essere necessario formulare criteri aggiuntivi ai fini dell'applicazione delle garanzie adeguate, anche per quanto riguarda i diritti degli interessati (cfr. paragrafo 3.2).

3.1 ORIENTAMENTI DI ATTUAZIONE RELATIVI AI CRITERI DI CERTIFICAZIONE

39. Per quanto concerne l'ambito di applicazione del meccanismo di certificazione e l'oggetto della valutazione (cfr. allegato 2, sezione 2, lettera a), dovrebbero essere chiaramente descritti nella documentazione pertinente, anche in relazione al trasferimento di dati personali verso un paese terzo oppure se devono contemplare anche il loro transito.

40. Per quanto concerne l'ambito di applicazione del meccanismo di certificazione e l'oggetto della valutazione (cfr. allegato 2, sezione 2, lettera b), la documentazione pertinente dovrebbe descrivere concretamente per quale tipo di soggetto (ad esempio, titolare del trattamento e/o responsabile del trattamento) è applicabile il meccanismo di certificazione.

41. In relazione all'ambito di applicazione del meccanismo di certificazione e all'oggetto della valutazione (cfr. allegato 2, sezione 2, lettera f), i criteri dovrebbero richiedere che l'oggetto della valutazione sia definito in modo concreto al fine di evitare equivoci, indicando almeno quanto segue.

42. Il/i trattamento/i, anche nel caso in cui siano previsti trasferimenti successivi;

    a) l'obiettivo;

    b) il tipo di soggetto (ad esempio, titolare del trattamento e/o responsabile del trattamento);

    c) il tipo di dati trasferiti tenendo conto dell'eventualità che siano interessate categorie particolari di dati personali ai sensi dell'articolo 9 GDPR;

    d) le categorie di interessati;

    e) i paesi in cui avviene il trattamento dei dati.

43. Per quanto riguarda la trasparenza e i diritti degli interessati (cfr. allegato 2, sezione 8), i criteri di certificazione dovrebbero:

    a) richiedere che le informazioni sulle attività di trattamento siano fornite agli interessati, anche, se del caso, sul trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale (cfr. articoli 12, 13 e 14 GDPR);

b) richiedere che agli interessati siano garantiti diritti di accesso, rettifica, cancellazione, limitazione, notifica in caso di rettifica, cancellazione o limitazione, opposizione al trattamento, nonché di non essere sottoposti a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, sostanzialmente equivalenti a quelli previsti dagli articoli da 15 a 19, 21 e 22 GDPR;
c) richiedere la definizione di una procedura adeguata di gestione dei reclami da parte dell'importatore di dati in possesso di una certificazione al fine di garantire l'effettiva attuazione dei diritti degli interessati;
d) richiedere di valutare se e in quale misura tali diritti sono azionabili per gli interessati nel paese terzo pertinente, nonché eventuali misure adeguate aggiuntive che può essere necessario predisporre per farli valere, ad esempio richiedendo che l'importatore accetti di sottoporsi alla giurisdizione dell'autorità di controllo competente per gli esportatori (uno o più) e di cooperare con quest'ultima in qualsiasi procedura finalizzata a garantire l'osservanza di tali diritti nonché, in particolare, accetti di dare seguito alle indagini, sottoporsi a verifiche e rispettare le misure adottate dall'autorità di controllo sopraccitata, ivi comprese le misure compensative e correttive.

44. Per quanto riguarda le misure organizzative e tecniche che garantiscono la protezione (allegato 2, sezione 10, lettera q)), i criteri di certificazione dovrebbero richiedere che l'importatore segnali all'esportatore e, se l'importatore agisce in qualità di titolare del trattamento, all'autorità di controllo nel SEE competente per gli esportatori di dati (uno o più) eventuali violazioni dei dati, come pure che le comunichi agli interessati qualora la violazione sia suscettibile di presentare un rischio elevato per i loro diritti e libertà, in linea con quanto richiesto nell'articolo 34 GDPR.

3.2 CRITERI DI CERTIFICAZIONE SPECIFICI AGGIUNTIVI

45. Alla luce delle garanzie individuate per altri strumenti di trasferimento nel quadro dell'articolo 46 GDPR (ad esempio le norme vincolanti d'impresa o i codici di condotta), nonché al fine di garantire un livello coerente di protezione e tenendo conto della sentenza Schrems II della Corte di giustizia, l'EDPB ritiene che il meccanismo di certificazione da utilizzare come strumento per i trasferimenti verso paesi terzi dovrebbe comprendere anche i criteri sotto riportati.

1. Valutazione della legislazione dei paesi terzi

a) I criteri richiedono che l'importatore abbia valutato le norme e le pratiche del paese terzo in cui opera e l'eventualità che queste gli impediscano di adempiere ai suoi impegni nel quadro della certificazione?
b) I criteri richiedono all'importatore di documentare la valutazione delle norme e delle pratiche del paese terzo in cui opera e di tenere la documentazione disponibile per l'organismo di certificazione e, su richiesta, l'autorità di controllo nel SEE competente per l'esportatore di dati, come pure per quest'ultimo?
c) I criteri richiedono che l'importatore abbia individuato e attuato le misure tecniche e organizzative atte a fornire le garanzie adeguate di cui all'articolo 46 GDPR tenendo conto delle 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?
d) I criteri richiedono che l'importatore documenti le misure tecniche e organizzative effettivamente attuate per fornire le garanzie adeguate di cui all'articolo 46 GDPR e mantenga la documentazione disponibile per l'organismo di certificazione nonché, su richiesta, le autorità di protezione dei dati competenti e l'esportatore di dati?

e) I criteri richiedono che l'importatore abbia individuato e attuato le misure tecniche e organizzative atte a garantire la sicurezza dei dati personali trasferiti, tenendo conto delle 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 se il transito rientra nell'ambito di applicazione della certificazione come strumento per i trasferimenti?
f) I criteri richiedono una garanzia all'organismo di certificazione e all'esportatore riguardo al fatto che l'importatore non ha motivo di ritenere che la legislazione e le pratiche ad esso applicabili possano impedirgli di adempiere ai suoi obblighi nel quadro della certificazione?

2. Obblighi generali degli esportatori e degli importatori

a) I criteri richiedono di definire in accordi contrattuali (ad esempio in un contratto di servizi esistente) tra gli esportatori e gli importatori una descrizione del trasferimento specifico a cui si applica la certificazione e che agli interessati in esame sono riconosciuti diritti di terzo beneficiario?

b) Nella misura in cui i criteri richiedano un contenuto specifico per tali strumenti o accordi contrattuali e sia fornito un modello, i criteri richiedono che siano anch'essi oggetto della valutazione?

3. Norme sui trasferimenti successivi

a) I criteri richiedono che i trasferimenti successivi siano soggetti a garanzie specifiche in linea con i requisiti di cui al capo V GDPR in modo tale da assicurare che il livello di protezione garantito nel SEE non sia compromesso e richiedono che una documentazione adeguata sia mantenuta a disposizione dell'organismo di certificazione e dell'autorità di controllo nel SEE competente per gli esportatori di dati (uno o più) nonché dell'esportatore di dati su richiesta?

4. Ricorso e attuazione

a) I criteri prevedono che gli interessati possano far valere i propri diritti come terzo beneficiario nei confronti dell'importatore di dati dinanzi all'organo giurisdizionale del SEE della residenza abituale dell'interessato o a un'organizzazione internazionale, anche per compensare i danni subiti dall'interessato in caso di non conformità da parte dell'importatore allo schema di certificazione pertinente?
b) I criteri consentono una valutazione adeguata del fatto che un importatore è responsabile nel SEE dei danni subiti dall'interessato in caso di non conformità allo schema di certificazione pertinente?
c) I criteri richiedono che gli interessati possano presentare un reclamo nei confronti dell'importatore a un'autorità di controllo nel SEE, in particolare nello Stato del SEE della loro residenza abituale, del loro luogo di lavoro o competente per gli esportatori di dati (uno o più)?
d) I criteri richiedono che l'importatore cooperi con l'autorità di controllo nel SEE competente per gli esportatori di dati (uno o più) e accetti di essere sottoposto a verifiche e ispezioni da parte loro, nonché tenga conto del loro parere e rispetti le loro decisioni?

5. Procedura e interventi per le situazioni in cui la legislazione nazionale impedisce di adempiere agli impegni presi nel contesto della certificazione

a) I criteri richiedono un impegno in base al quale laddove un'organizzazione internazionale o l'importatore di dati in un paese terzo avesse motivo di ritenere che modifiche nella legislazione e nelle pratiche a esso applicabili possano impedirgli di adempiere agli obblighi che gli incombono in forza della certificazione lo comunicherà quanto prima all'organismo di certificazione e all'esportatore di dati affinché quest'ultimo possa valutare se interrompere immediatamente i trasferimenti?
b) I criteri richiedono una descrizione delle misure da adottare (comprese la notifica all'esportatore nel SEE e l'adozione di misure aggiuntive adeguate) se l'importatore di dati viene a conoscenza di normative o pratiche di un paese terzo che impediscono l'adempimento degli obblighi nel quadro della certificazione, come pure delle misure da adottare in caso di richieste di informazioni da parte di autorità di un paese terzo (ivi compreso l'obbligo di riesaminare e, se del caso, contestare la legalità della richiesta e ridurre al minimo le eventuali informazioni comunicate)?

6. Trattare le richieste di accesso ai dati da parte di autorità di paesi terzi

a) I criteri richiedono che l'importatore di dati informi quanto prima l'esportatore di dati in caso di richieste di accesso da parte delle autorità di paesi terzi e adotti misure aggiuntive adeguate?
b) I criteri richiedono che non si proceda al trasferimento in caso di richieste di accesso sproporzionate da parte di autorità pubbliche di paesi terzi, in particolare di richieste volte a trasferimenti indiscriminati e sostanziali di dati personali?

7. Garanzie aggiuntive riguardanti l'esportatore

46. I criteri richiedono che, ove previsto, l'importatore di dati garantisca, anche attraverso requisiti vincolanti a tale proposito per l'esportatore di dati, che le misure supplementari che ha individuato siano accompagnate da misure supplementari corrispondenti da parte dell'esportatore di dati, tenendo conto delle raccomandazioni 01/2020 dell'EDPB e dei casi di utilizzo, al fine di garantire un'attuazione efficace delle misure supplementari dell'importatore?

4 IMPEGNI VINCOLANTI E AZIONABILI DA ATTUARE

47. L'articolo 42, paragrafo 2, GDPR, impone ai titolari del trattamento e ai responsabili del trattamento non soggetti al GDPR che aderiscono a un meccanismo di certificazione destinato ai trasferimenti di assumere altresì l'impegno vincolante e azionabile, mediante strumenti contrattuali o altri strumenti giuridicamente vincolanti[22], di applicare le garanzie adeguate previste dal meccanismo di certificazione, anche per quanto riguarda i diritti degli interessati.

[22] Tale strumento giuridicamente vincolante non è un altro strumento di cui al capo V (ad esempio le clausole contrattuali tipo), in quanto tali impegni vincolanti e azionabili di cui all'articolo 46, paragrafo 2, lettera f), devono essere concepiti per garantire che l'importatore rispetti i criteri di certificazione.

48. Come specificato dal GDPR, tali impegni possono essere assunti mediante la stipula di un contratto, che sembra la soluzione più semplice. Si potrebbero usare anche altri strumenti, purché i titolari/responsabili del trattamento che aderiscono al meccanismo di certificazione siano in grado di dimostrare il carattere vincolante e azionabile di questi altri mezzi.

49. Il carattere vincolante e azionabile deve in ogni caso essere garantito a norma del diritto dell'UE e gli impegni dovrebbero essere vincolanti e azionabili da parte degli interessati come terzi beneficiari.

50. Una semplice alternativa consisterebbe nell'inclusione degli impegni vincolanti e azionabili nel contratto tra l'esportatore di dati e l'importatore di dati. In pratica, le parti potrebbero ricorrere a un contratto esistente (ad esempio un accordo di servizi tra l'esportatore di dati e l'importatore di dati, il contratto riguardante l'accordo al trattamento dei dati in conformità dell'articolo 28 GDPR tra titolari del trattamento e responsabili del trattamento o un accordo sulla condivisione dei dati tra vari titolari del trattamento) nel quale potrebbero essere inseriti gli impegni vincolanti e azionabili. Tali impegni dovrebbero essere chiaramente distinti da qualsiasi altra clausola. Un'altra soluzione potrebbe essere quella di affidarsi a un contratto separato, ad esempio aggiungendo al meccanismo di certificazione destinato ai trasferimenti un contratto tipo che dovrebbe essere poi firmato dai titolari/responsabili del trattamento nel paese terzo e da tutti i loro esportatori.

51. Dovrebbe essere garantita una certa flessibilità nella scelta dell'opzione più adeguata a seconda della situazione specifica.

52. Quando il meccanismo di certificazione deve essere utilizzato per i trasferimenti e i trasferimenti successivi da un responsabile del trattamento a sub-responsabili del trattamento, nell'accordo stipulato tra il responsabile del trattamento e il suo titolare del trattamento occorre anche fare un riferimento al meccanismo di certificazione e allo strumento che prevede impegni vincolanti e azionabili.

Esempio di impegni vincolanti e azionabili compresi nel contratto tra l'esportatore di dati e l'importatore di dati:

53. In generale il contratto o altro strumento giuridico vincolante deve indicare che il titolare/responsabile del trattamento in possesso di una certificazione che agisce in qualità di importatore si impegna a rispettare le norme specificate nella certificazione destinata ai trasferimenti durante il trattamento dei dati pertinenti ricevuti dal SEE e garantisce di non aver motivo di ritenere che le normative e le pratiche nel paese terzo applicabili al trattamento in esame, ivi compresi eventuali requisiti in materia di comunicazione dei dati personali o possibili misure che autorizzano l'accesso da parte delle autorità pubbliche, gli impediscano di adempiere ai suoi impegni nel quadro della certificazione, nonché che comunicherà all'esportatore eventuali modifiche pertinenti nella legislazione o nella pratica a tale proposito.

54. Il contratto o altro strumento deve altresì prevedere meccanismi che consentano di far rispettare tali impegni in caso di non conformità alle norme nel quadro della certificazione da parte del titolare/responsabile del trattamento che agisce in qualità di importatore, segnatamente per quanto riguarda i diritti degli interessati i cui dati sono trasferiti a norma della certificazione.

55. Più in particolare, il contratto o altro strumento dovrebbe riguardare:

- l'esistenza di un diritto per gli interessati i cui dati sono trasferiti in virtù della certificazione di far valere come terzi beneficiari gli impegni presi dall'importatore di dati certificato nel contesto della certificazione;
- la questione della responsabilità in caso di non conformità alle norme nel quadro della certificazione da parte di un importatore di dati in possesso di una certificazione al di fuori del SEE. Gli interessati hanno la possibilità, in caso di non conformità alle norme nel quadro della certificazione da parte di un importatore di dati in possesso di una certificazione al di fuori del SEE, di presentare un reclamo invocando il loro diritto di terzo beneficiario, anche per un risarcimento, contro tale entità dinanzi a un'autorità di controllo del SEE e all'organo giurisdizionale del SEE della residenza abituale dell'interessato. L'importatore in possesso di una certificazione accetta la decisione dell'interessato. Qualora la non conformità da parte dell'importatore possa comportare una responsabilità dell'esportatore di dati, gli interessati hanno anche la possibilità di presentare un reclamo nei confronti dell'esportatore di dati dinanzi all'autorità di controllo o all'organo giurisdizionale del luogo di stabilimento dell'esportatore di dati o della residenza abituale dell'interessato23. L'importatore e l'esportatore di dati dovrebbero anche accettare che l'interessato possa essere rappresentato da un organismo, un'organizzazione o un'associazione senza scopo di lucro alle condizioni stabilite nell'articolo 80, paragrafo 1, GDPR;
- l'esistenza di un diritto per l'esportatore da far valere nei confronti dell'importatore di dati in possesso di una certificazione le norme nel quadro della certificazione come terzo beneficiario;
- l'esistenza di un obbligo dell'importatore di dati in possesso di una certificazione di comunicare all'esportatore e all'autorità di controllo dell'esportatore di dati eventuali misure adottate dall'organismo di certificazione a seguito della rilevazione di una non conformità rispetto alle norme della certificazione da parte del medesimo importatore di dati.

[23] Tale responsabilità non dovrebbe pregiudicare i meccanismi da attuare a norma della certificazione e l'organismo di certificazione deve anche poter prendere provvedimenti contro i titolari/responsabili del trattamento certificati conformemente alla certificazione, imponendo misure correttive.

ALLEGATO

A. ESEMPI DI MISURE SUPPLEMENTARI CHE L'IMPORTATORE DEVE ATTUARE QUALORA IL TRANSITO SIA CONTEMPLATO NELL'AMBITO DI APPLICAZIONE DELLA CERTIFICAZIONE

Caso d'uso 1: conservazione dei dati per il backup e per altri scopi che non richiedono l'accesso ai dati in chiaro

È necessario stabilire criteri relativi alle norme di cifratura e alla sicurezza della chiave di decifrazione, segnatamente criteri riguardanti la situazione giuridica nel paese terzo. Se l'importatore può essere obbligato a trasmettere le chiavi di decifrazione, la misura aggiuntiva non può essere considerata efficace[24].

Caso d'uso 2: trasferimento di dati pseudonimizzati

In caso di dati pseudonimizzati, sono stabiliti criteri relativi alla sicurezza delle informazioni aggiuntive necessarie per attribuire i dati trasferiti a un soggetto identificato o identificabile, in particolare:

- criteri riguardanti la situazione giuridica nel paese terzo. Se l'importatore può essere obbligato ad accedere o ricorrere a dati aggiuntivi al fine di attribuire i dati a un soggetto identificato o identificabile, la misura non può essere considerata efficace[25];

- criteri relativi alla definizione delle informazioni aggiuntive a disposizione di autorità di paesi terzi che potrebbero essere sufficienti per attribuire i dati a un soggetto identificato o identificabile.

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

In caso di dati cifrati, sono compresi eventuali criteri per la sicurezza del transito. Se l'importatore può essere obbligato a trasmettere le chiavi di cifratura per la decifrazione o l'autenticazione oppure a modificare un componente utilizzato per il transito in modo tale che le sue proprietà di sicurezza siano compromesse, la misura aggiuntiva non può essere considerata efficace[26].

Caso d'uso 4: destinatario protetto

In caso di destinatari protetti, devono essere definiti criteri per i limiti del privilegio. Il trattamento dei dati deve rimanere nei limiti del privilegio legale. Ciò vale anche per il trattamento da parte di (sub-)responsabili del trattamento e i trasferimenti successivi, i cui destinatari devono anch'essi disporre di privilegi[27].

[24] Allegato 2 delle 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, Caso d'uso 1: conservazione dei dati per il backup e per altri scopi che non richiedono l'accesso ai dati in chiaro, paragrafo 85; https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_it_0.pdf

[25] Cfr. supra, paragrafi 86-89.

[26] Cfr. supra, paragrafo 90.

[27] Cfr. supra, paragrafo 91.

B. ESEMPI DI MISURE SUPPLEMENTARI QUALORA IL TRANSITO NON SIA CONTEMPLATO DALLA CERTIFICAZIONE E L'ESPORTATORE LE DEBBA GARANTIRE

Caso d'uso 2: trasferimento di dati pseudonimizzati

Sono previsti criteri riguardanti le informazioni aggiuntive a disposizione di autorità di paesi terzi che potrebbero essere sufficienti per attribuire i dati a un soggetto identificato o identificabile.

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

Sono previsti criteri riguardanti l'attendibilità dell'infrastruttura o autorità di certificazione della chiave pubblica utilizzata, la sicurezza delle chiavi di cifratura utilizzate per l'autenticazione o la decifrazione e l'affidabilità della gestione delle chiavi, nonché l'utilizzo di software senza vulnerabilità note sottoposti a una corretta manutenzione.

Se l'importatore può essere obbligato a comunicare chiavi di cifratura adatte per la decifrazione o l'autenticazione oppure a modificare un componente utilizzato per il transito al fine di comprometterne le proprietà di sicurezza, la misura non può essere considerata efficace[28].

Caso d'uso 4: destinatario protetto

In caso di destinatari protetti, devono essere definiti i criteri per i limiti del privilegio. Il trattamento dei dati deve rimanere nei limiti del privilegio legale. Ciò vale anche per il trattamento da parte di (sub-)responsabili del trattamento e i trasferimenti successivi, i cui destinatari devono anch'essi disporre di privilegi[29].

[28] Cfr. supra, raccomandazioni, paragrafo 90.
[29] Cfr. supra, raccomandazioni, paragrafo 91.