

QUADRO UE-USA IN MATERIA DI PROTEZIONE DEI DATI

DOMANDE FREQUENTI PER LE IMPRESE EUROPEE ⁽¹⁾

Adottato il 16 luglio 2024

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

⁽¹⁾ In tale contesto, per imprese europee s'intendono le imprese dello Spazio economico europeo che trasferiscono o possono trasferire dati personali a imprese degli Stati Uniti certificate ai sensi del DPF.

Indice

D1. Cos'è il quadro UE-USA in materia di protezione dei dati?	3
D2. Quali imprese statunitensi sono ammissibili al quadro UE-USA in materia di protezione dei dati?	3
D3. Cosa fare prima di trasferire i dati personali a un'impresa negli Stati Uniti che è, o dichiara di essere, certificata ai sensi del quadro UE-USA in materia di protezione dei dati?.....	4
D4. Dove posso trovare orientamenti in merito alla certificazione delle filiali statunitensi di imprese europee?.....	7

D1. COS'È IL QUADRO UE-USA IN MATERIA DI PROTEZIONE DEI DATI?

Il quadro UE-USA in materia di protezione dei dati («DPF») è un meccanismo di autocertificazione per le imprese negli USA. Le imprese che si sono autocertificate come aderenti al DPF devono rispettarne i principi, le norme e gli obblighi relativi al trattamento dei dati personali degli interessati nello Spazio economico europeo (SEE). Per maggiori informazioni su questi impegni, cfr. i [principi del quadro in materia di protezione dei dati](#) ⁽²⁾.

La Commissione europea ha ritenuto che i trasferimenti di dati personali dal SEE a imprese certificate ai sensi del DPF godano di un livello di protezione adeguato ⁽³⁾. Di conseguenza, i dati personali possono essere trasferiti liberamente a società degli Stati Uniti certificate, senza la necessità di porre in essere ulteriori garanzie o di ottenere un'autorizzazione. Di seguito sono riportati alcuni link utili per ulteriori informazioni:

- Commissione europea: [Domande e risposte:quadro in materia di protezione dei dati](#) ⁽⁴⁾
- [Il sito web del quadro in materia di protezione dei dati gestito dal Dipartimento del Commercio degli Stati Uniti](#) ⁽⁵⁾
- [La decisione della Commissione europea sull'adeguato livello di protezione dei dati personali nell'ambito del quadro UE-USA in materia di protezione dei dati](#) ⁽⁶⁾.

Il DPF si applica a qualsiasi tipo di dati personali trasferiti dal SEE agli Stati Uniti, compresi i dati personali trattati per scopi commerciali o sanitari e i dati sulle risorse umane acquisiti nel contesto di un rapporto di lavoro (di seguito: «dati sulle risorse umane»), a condizione che la società destinataria negli Stati Uniti sia autocertificata nell'ambito del DPF per trattare questo tipo di dati ⁽⁷⁾.

D2. QUALI IMPRESE STATUNITENSIS SONO AMMISSIBILI AL QUADRO UE-USA IN MATERIA DI PROTEZIONE DEI DATI?

Per essere abilitata all'autocertificazione del DPF, un'impresa statunitense deve essere soggetta ai poteri di indagine e di esecuzione della Commissione federale del Commercio degli USA («FTC») o del Dipartimento dei Trasporti degli USA («DoT»). In futuro potrebbero essere previsti altri organi statutari degli Stati Uniti ⁽⁸⁾.

²[https://www.dataprivacyframework.gov/program-articles/Participation-Requirements-Data-Privacy-Framework-\(DPF\)-Principles](https://www.dataprivacyframework.gov/program-articles/Participation-Requirements-Data-Privacy-Framework-(DPF)-Principles)

⁽³⁾ La decisione sull'adeguatezza del quadro in materia di protezione dei dati è stata adottata dalla Commissione europea il 10 luglio 2023. È stata concepita dalla Commissione europea e dal Dipartimento del Commercio degli Stati Uniti per sostituire la decisione (UE) 2016/1250 sullo «scudo per la privacy», dichiarata invalida dalla Corte di giustizia dell'UE

il 16 luglio 2020 nella causa C-311/18, *Data Protection Commissioner c. Facebook Ireland Limited e Maximilian Schrems (Schrems II)*.

⁴ https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752

⁵ <https://www.dataprivacyframework.gov/s/>

⁶https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf

⁽⁷⁾ Si noti che non tutte le autocertificazioni del DPF riguardano i dati sulle risorse umane. È quindi importante procedere a una verifica in tal senso, ove pertinente. Cfr. anche la domanda D3.

⁽⁸⁾ Cfr. l'allegato I della decisione sull'adeguatezza, Principi del quadro UE-USA in materia di protezione dei dati emanati dal Dipartimento del Commercio degli Stati Uniti, paragrafo I.2.

Ciò significa che, ad esempio, le organizzazioni senza scopo di lucro, le banche, le compagnie di assicurazione e i fornitori di servizi di telecomunicazione (nell'esercizio di attività di vettore pubblico) che non rientrano nella giurisdizione dell'FTC o del DoT non possono avvalersi dell'autocertificazione ai sensi del DPF.

D3. COSA FARE PRIMA DI TRASFERIRE I DATI PERSONALI A UN'IMPRESA NEGLI STATI UNITI CHE È, O DICHIARA DI ESSERE, CERTIFICATA AI SENSI DEL QUADRO UE-USA IN MATERIA DI PROTEZIONE DEI DATI?

Prima di trasferire dati personali a un'impresa negli Stati Uniti che dichiara di essere autocertificata ai sensi del DPF, un esportatore di dati del SEE deve accertarsi che l'impresa negli USA sia titolare di un'autocertificazione valida (le certificazioni devono essere rinnovate annualmente) e che tale certificazione riguardi i dati in questione (in particolare se si tratta, rispettivamente, di dati sulle risorse umane e di dati non relativi alle risorse umane) ⁽⁹⁾.

Per verificare se un'autocertificazione sia valida o meno e applicabile, gli esportatori di dati del SEE devono controllare se l'impresa negli Stati Uniti figura nell'[elenco del quadro in materia di protezione dei dati](#) ⁽¹⁰⁾, pubblicato sul sito web del Dipartimento del Commercio degli Stati Uniti. L'elenco contiene anche un registro delle imprese che sono state cancellate dall'elenco («partecipanti inattivi») unitamente alla motivazione. Un esportatore di dati del SEE non può avvalersi del DPF per i trasferimenti di dati personali verso dette imprese. Si noti che le imprese cancellate dall'elenco del quadro in materia di protezione dei dati devono continuare ad applicare i principi di tale quadro ai dati personali ricevuti nel corso dell'adesione al DPF per tutto il periodo tempo in cui li conservano.

Per il trasferimento di dati personali a imprese negli Stati Uniti che non sono (o non sono più) autocertificate ai sensi del DPF, è possibile avvalersi di altre basi di cui al capo V del regolamento generale sulla protezione dei dati, come le norme vincolanti d'impresa o le clausole contrattuali tipo.

Il fatto che l'impresa destinataria negli Stati Uniti sia autocertificata nell'ambito del DPF consentirà agli esportatori di dati del SEE di rispettare il capo V del regolamento generale sulla protezione dei dati, ma restano applicabili tutti gli altri requisiti di tale regolamento e qualsiasi altra normativa nazionale in materia di protezione dei dati.

3.1. Trasferimenti a filiali statunitensi di imprese certificate ai sensi del quadro UE-USA in materia di protezione dei dati.

Nel caso di trasferimenti a imprese statunitensi che sono filiali di un'impresa madre certificata ai sensi del DPF, gli esportatori di dati del SEE sono tenuti a verificare se la certificazione dell'impresa madre riguarda anche la filiale.

⁽⁹⁾ Cfr. la definizione di «dati sulle risorse umane» alla domanda D1.

¹⁰ <https://www.dataprivacyframework.gov/list>

Ulteriori informazioni su come verificare l'ambito dell'autocertificazione di un'organizzazione, compresa l'eventuale copertura di altre entità statunitensi o filiali statunitensi, sono disponibili [qui](#) ⁽¹¹⁾.

3.2. Trasferimenti a un'impresa negli Stati Uniti che agisce in qualità di titolare del trattamento

Prima di trasferire i dati personali a un titolare del trattamento negli Stati Uniti, un esportatore di dati nel SEE deve assicurare che il trasferimento sia conforme a tutte le disposizioni pertinenti del regolamento generale sulla protezione dei dati. Come primo passo, l'esportatore di dati può condividere i dati personali con un'impresa negli Stati Uniti solo se esiste una base giuridica per il trattamento (articolo 6 del regolamento generale sulla protezione dei dati). Devono inoltre essere soddisfatti tutti gli altri requisiti previsti dal regolamento generale sulla protezione dei dati (ad esempio la limitazione della finalità, la proporzionalità, l'accuratezza e gli obblighi di informazione nei confronti degli interessati). Si noti che, quando i dati devono essere trasferiti a un'impresa autocertificata negli Stati Uniti, l'esportatore di dati del SEE, a norma degli articoli 13 e 14 del regolamento generale sulla protezione dei dati, deve informare gli interessati in merito all'identità dei destinatari dei loro dati e al fatto che il trasferimento è disciplinato dalla decisione sull'adeguatezza del quadro UE-USA in materia di protezione dei dati.

3.3. Trasferimenti a un'impresa negli Stati Uniti che agisce in qualità di responsabile del trattamento

Quando un titolare del trattamento del SEE trasferisce dati a un responsabile del trattamento negli Stati Uniti, il titolare del trattamento e il responsabile del trattamento sono obbligati a concludere un accordo relativo al trattamento dei dati ai sensi dell'articolo 28 del regolamento generale sulla protezione dei dati (di seguito: accordo sul trattamento dei dati), indipendentemente dal fatto che il responsabile del trattamento abbia o non abbia un'autocertificazione ai sensi del DPF.

Per ulteriori informazioni sui requisiti contrattuali per i trasferimenti a un responsabile del trattamento negli Stati Uniti, si rimanda a questa [pagina](#) ⁽¹²⁾.

La conclusione di un accordo relativo al trattamento dei dati è necessaria per garantire che il responsabile del trattamento statunitense si impegni a:

- trattare i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento dei dati, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
- garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo statutario di riservatezza;

¹¹[https://www.dataprivacyframework.gov/program-articles/How-to-Verify-an-Organization-s-Privacy-Data-Privacy-Framework-\(DPF\)-Commitments](https://www.dataprivacyframework.gov/program-articles/How-to-Verify-an-Organization-s-Privacy-Data-Privacy-Framework-(DPF)-Commitments)

¹²<https://www.dataprivacyframework.gov/program-articles/Contract-Requirements-for-Data-Transfers-to-a-Processor>

- attuare adeguate misure tecniche e organizzative per garantire un livello di sicurezza commisurato al rischio, in linea con quanto disposto dall'accordo relativo al trattamento dei dati (derivante dall'articolo 32 del regolamento generale relativo alla protezione delle persone dei dati personali) e con le sezioni 4 e 10 del DPF;
- rispettare le condizioni di cui all'accordo relativi al trattamento dei dati (derivante dall'articolo 28, paragrafi 2 e 4, del regolamento generale sulla protezione dei dati) e alla sezione II.3.B del DPF per il coinvolgimento di un altro responsabile del trattamento;
- in considerazione della natura del trattamento, assistere il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del regolamento generale sulla protezione dei dati;
- assistere il titolare del trattamento nel garantire il rispetto dei propri obblighi di cui agli articoli da 32 a 36 del regolamento generale sulla protezione dei dati, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- su scelta del titolare del trattamento, cancellare tutti i dati personali o restituirli al titolare del trattamento dopo che è terminata la prestazione dei servizi relativi al trattamento, e cancellare le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati personali; e
- mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'articolo 28 del regolamento generale sulla protezione dei dati e consentire gli audit dando contributi, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro revisore da questi incaricato. Per quanto riguarda quest'ultimo punto, il responsabile del trattamento informa immediatamente il titolare del trattamento se, a suo parere, un'istruzione viola il DPF.

Se il responsabile del trattamento statunitense incarica un altro responsabile del trattamento («sub-responsabile») di svolgere specifiche attività di trattamento per conto del titolare del trattamento del SEE, il responsabile del trattamento deve garantire che siano soddisfatti i requisiti di cui alla sezione II.3.B del DPF. Ciò include la garanzia che il sub-responsabile del trattamento fornisca lo stesso livello di protezione dei dati personali richiesto nel DPF e gli stessi obblighi in materia di protezione dei dati stabiliti nell'accordo relativo al trattamento dei dati. Qualora un sub-responsabile del trattamento non adempia ai propri obblighi in materia di protezione dei dati, il responsabile statunitense iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi di tale sub-responsabile.

D4. DOVE POSSO TROVARE ORIENTAMENTI IN MERITO ALLA CERTIFICAZIONE DELLE FILIALI STATUNITENSIS DI IMPRESE EUROPEE?

Le filiali statunitensi di imprese del SEE possono autocertificare l'adesione al DPF se sono soggette alla giurisdizione della Commissione federale del commercio (FTC) o del Dipartimento dei Trasporti degli Stati Uniti (DoT).

Maggiori informazioni sui requisiti di idoneità sono disponibili [qui](#) ⁽¹³⁾ e una guida al processo di autocertificazione è consultabile [qui](#) ⁽¹⁴⁾.

¹³[https://www.dataprivacyframework.gov/program-articles/U-S-Subsidiaries-of-European-Businesses-Participation-in-the-Data-Privacy-Framework-\(DPF\)-Program](https://www.dataprivacyframework.gov/program-articles/U-S-Subsidiaries-of-European-Businesses-Participation-in-the-Data-Privacy-Framework-(DPF)-Program)

¹⁴[https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-\(DPF\)-Program-\(part%E2%80%93\)](https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(part%E2%80%93))