RISERVATO

Transfer Impact Assessment – Flussi verso gli Stati Uniti

Wibo Discover – versione 1.3 del 13 ottobre 2026 (sostituisce la versione 1.2 del 13 ottobre 2026)

Voce	Contenuto
Esportatore	EntertainmentLabs S.r.l. (Wibo) – Torino – C.F./P.IVA 12215420014
Ruolo dell'esportatore	Responsabile del trattamento per conto dei Clienti-Titolari
Ambito	Trasferimenti verso sub-responsabili negli Stati Uniti d'America
Metodologia	Raccomandazioni EDPB 01/2020 v.2.0; CGUE C-311/18 (Schrems II)

Premessa

La presente valutazione d'impatto sul trasferimento ("TIA") esamina l'adeguatezza dei trasferimenti di dati personali verso gli Stati Uniti effettuati da EntertainmentLabs S.r.l. ("Wibo") nell'erogazione del servizio Wibo Discover, in qualità di Responsabile del trattamento per conto dei Clienti-Titolari. La TIA ha carattere generale, si applica trasversalmente ai flussi USA del servizio comuni a tutti i clienti ed è richiamata dal modello di DPA (art. 1.8).

1. Identificazione del trasferimento (Step 1)

Voce	Contenuto
Importatori	Replit, Inc. – hosting dell'applicazione e database applicativo (infrastruttura negli Stati Uniti; il database è gestito per conto di Replit dal suo sub-responsabile Neon, LLC, negli Stati Uniti); Anthropic, PBC (contraente Anthropic Ireland, Ltd.) – modelli linguistici; OpenAI, LLC (contraente OpenAI Ireland Ltd.) – trascrizione vocale; Plus Five Five, Inc. (Resend) – email transazionali; Cal.com, Inc. – prenotazione delle sessioni.
Base del trasferimento	Clausole contrattuali tipo (Decisione di esecuzione (UE) 2021/914), modulo da responsabile a sub-responsabile, quale base

	primaria per tutti gli importatori; Data Privacy Framework (Decisione di esecuzione (UE) 2023/1795) quale base rafforzativa per i fornitori certificati. Alla verifica del 30 settembre 2026, aggiornata al 13 ottobre 2026, risulta certificato Resend; non risultano certificati Replit, Anthropic, OpenAI e Cal.com, per i quali la base è costituita dalle clausole contrattuali tipo con le misure supplementari della presente TIA. I trasferimenti successivi da Replit ai propri sub-responsabili negli Stati Uniti avvengono all'interno dello stesso Paese terzo e restano soggetti agli obblighi assunti da Replit con le clausole contrattuali tipo (clausola 8.8).
Categorie di dati	Identificativi e di contatto professionali; ruolo, dipartimento, relazioni gerarchiche; data e ora delle sessioni; contenuti dichiarati nelle interviste (descrizione di attività e processi lavorativi); testi delle conversazioni; risultati dell'analisi; log di accesso. Nessuna categoria particolare (art. 9) né dato relativo a reati (art. 10).
Categorie di interessati	Dipendenti e collaboratori dei Clienti-Titolari.
Volume e frequenza	Variabile in funzione dei progetti; flussi continuativi per la durata del servizio; conservazione nel database per la durata del contratto con il Cliente e per non oltre 6 mesi dalla sua cessazione, salvo cancellazione anticipata richiesta dal Titolare.
Finalità	Erogazione del servizio: hosting e conservazione dei dati applicativi, agente di intervista e analisi, trascrizione vocale, invio di email transazionali, prenotazione delle sessioni.

2. Mappatura dei flussi (Step 1)

Flusso	**Importatore**	**Dati trasferiti**	**Base**
Hosting dell'applicazione e database applicativo	Replit (database gestito da Neon per conto di Replit)	Anagrafiche, testi delle conversazioni, risultati, log; dati applicativi in transito	SCC

		ed elaborazione	
Agente di intervista e analisi	Anthropic (Claude)	Testi delle conversazioni, tassonomia dei ruoli	SCC
Trascrizione vocale	OpenAI (Whisper)	Contenuti audio convertiti in testo	SCC
Email transazionali	Resend	Indirizzi email, contenuto dei report	DPF + SCC
Prenotazione sessioni	Cal.com	Nome, email, data e ora della sessione	SCC

I dati persistenti (anagrafiche, testi delle conversazioni, output) risiedono nel database applicativo fornito da Replit negli Stati Uniti. Agli altri importatori sono trasmessi i soli dati necessari alla rispettiva funzione. Non è conservata alcuna registrazione audio.

3. Strumento di trasferimento (Step 2)

Lo strumento primario sono le clausole contrattuali tipo di cui alla Decisione (UE) 2021/914, modulo da responsabile a sub-responsabile, scelte per la loro stabilità, indipendente da decisioni di adeguatezza soggette a impugnazione. In via rafforzativa e cumulativa, per i fornitori certificati (Resend) si valorizza l'adesione al Data Privacy Framework, che costituisce autonomo titolo di adeguatezza ai sensi dell'art. 45 GDPR. Data di sottoscrizione delle clausole e data di verifica della certificazione per ciascun importatore sono riportate nell'elenco dei sub-responsabili.

4. Valutazione della legge del Paese terzo (Step 3)

4.1 Quadro normativo sulla sorveglianza. L'ordinamento statunitense prevede, in materia di accesso ai dati per finalità di intelligence, in particolare la Section 702 del Foreign Intelligence Surveillance Act (FISA §702) e l'Executive Order 14086 del 2022, con l'istituzione del Data Protection Review Court a presidio dei principi di necessità e proporzionalità e dei rimedi per gli interessati UE, alla base della decisione di adeguatezza. La §702, riautorizzata dal RISAA del 2024 fino all'aprile 2026 e poi prorogata a breve termine, è giunta a scadenza il 12 giugno 2026 senza riautorizzazione; alla data della presente TIA la raccolta prosegue sulla base delle certificazioni del Foreign Intelligence Surveillance Court in essere, operative fino a marzo 2027, mentre il Congresso discute la riautorizzazione. La riforma del 2024 ha inoltre ampliato la nozione di electronic communication service provider, estendendo potenzialmente l'ambito dei soggetti, inclusi i fornitori cloud, assoggettabili alle direttive §702. Le garanzie dell'Executive Order 14086 si applicano alle attività di intelligence statunitensi indipendentemente dalla certificazione del singolo importatore.
4.2 Elementi fattuali. Conformemente all'approccio EDPB (§43 Racc. 01/2020), la valutazione si incentra sulla concreta probabilità di accesso in relazione alla natura dei dati. I dati trasferiti sono identificativi e professionali e descrivono attività e processi lavorativi; non comprendono categorie particolari, dati giudiziari, comunicazioni interpersonali di contenuto sensibile né dati

con valore intrinseco per finalità di intelligence. La finalità (rilevazione di attività e processi di lavoro, formazione, analisi di automazione) è estranea agli ambiti tipicamente attinti dalla sorveglianza per sicurezza nazionale. Il fornitore di hosting e database opera in un settore potenzialmente raggiungibile dalla nozione ampliata di service provider: ciò accresce l'astratta raggiungibilità ma non muta la probabilità concreta, che resta bassa. La conservazione stabile dei dati presso un importatore statunitense estende l'esposizione dai dati in transito ai dati conservati; essa è presidiata dalle clausole contrattuali tipo, dalla cifratura a riposo, dalla segregazione per cliente e dalla durata di conservazione legata al contratto. Non risultano, per la tipologia di dati e di servizio, evidenze di richieste di accesso.

4.3 Rimedi per l'interessato. Il Data Privacy Framework prevede per i residenti UE un meccanismo di ricorso dinanzi al Data Protection Review Court e al Civil Liberties Protection Officer. L'effettività di tali rimedi è oggetto del ricorso pendente dinanzi alla Corte di giustizia (causa C-703/25 P, Latombe), proposto contro la sentenza del Tribunale UE del 3 settembre 2025 che ha confermato la validità della decisione di adeguatezza.

4.4 Esito dello Step 3. La normativa statunitense non assicura, in astratto, un livello di protezione integralmente equivalente a quello UE, quanto all'accesso per finalità di sicurezza nazionale e all'effettività dei rimedi. Per la specifica tipologia di dati e di trattamento, tuttavia, la probabilità concreta di un accesso pregiudizievole è bassa. Ne consegue la necessità di misure supplementari per mantenere il rischio residuo entro una soglia accettabile.

5. Misure supplementari (Step 4)

5.1 Misure tecniche. Cifratura dei dati in transito (TLS 1.2 o superiore) e a riposo (AES-256 sul database; connessioni al database solo cifrate); minimizzazione dei dati trasmessi a ciascun importatore; istruzioni all'assistente di IA di non richiedere né approfondire dati di categorie particolari o informazioni sulla vita privata; assenza di conservazione delle registrazioni audio, che transitano in memoria per il solo tempo della trascrizione; segregazione logica dei dati per cliente; aggregazione dei risultati per il Titolare con accorpamento dei gruppi con meno di 30 persone; token monouso per il rilascio dei report individuali.

5.2 Misure contrattuali. Clausole contrattuali tipo integrate da: impegno di non addestramento dei modelli sui dati del Cliente, sia presso i fornitori di modelli di IA sia presso il fornitore di hosting e database, e conservazione limitata presso i fornitori di modelli di IA; obblighi di riservatezza e di trattamento su sola istruzione; impegni di notifica all'esportatore delle richieste di accesso delle autorità e di impugnazione di quelle eccedenti il necessario e proporzionato, nei limiti consentiti dalla legge; limitazione della conservazione presso l'importatore.

5.3 Misure organizzative. Selezione di fornitori che offrano garanzie adeguate e, ove possibile, certificati Data Privacy Framework; tenuta e aggiornamento dell'elenco dei sub-responsabili con verifica periodica della certificazione per entità; procedura di gestione delle violazioni; istruzioni agli autorizzati e formazione; riesame periodico del presente documento.

5.4 Matrice rischio – misure – rischio residuo.

Rischio	**Misure**	**Efficacia**	**Rischio residuo**
Accesso governativo ex §702 a dati in transito	Cifratura in transito; minimizzazione; natura non sensibile	Media-alta	Basso

	dei dati		
Accesso governativo ai dati conservati nel database USA	Clausole contrattuali tipo; cifratura a riposo; segregazione per cliente; natura non sensibile dei dati; conservazione legata al contratto con possibilità di cancellazione anticipata per rilevazione	Media	Medio-basso
Richieste mirate all'importatore	Clausole contrattuali, obblighi di notifica e impugnazione, trasparenza	Media	Medio-basso
Conservazione o uso secondario presso i fornitori	Conservazione limitata; non addestramento; nessuna conservazione audio	Media-alta	Basso
Incertezza normativa (§702 e Data Privacy Framework)	Clausole contrattuali tipo come base primaria per tutti gli importatori; riesame periodico; piano di contingenza (art. 1.8 del DPA)	Media	Medio

6. Step procedurali (Step 5)

Sottoscrizione delle clausole contrattuali tipo con ciascun importatore e archiviazione dei relativi accordi; implementazione delle misure supplementari; verifica della certificazione Data Privacy Framework per entità; aggiornamento dell'informativa agli interessati a cura del Titolare (artt. 13-14 GDPR); aggiornamento del registro dei trattamenti (art. 30, lett. e) GDPR); formazione degli autorizzati.

7. Revisione periodica (Step 6)

La presente TIA è riesaminata almeno annualmente e a ogni mutamento rilevante, in particolare: esito della riautorizzazione della §702 e modifiche al quadro di sorveglianza statunitense; esito della causa C-703/25 P e ogni pronuncia sulla validità del Data Privacy Framework; modifiche dei sub-responsabili o dei flussi, inclusa l'eventuale migrazione del database su un'istanza in una regione UE; nuove decisioni di adeguatezza o linee guida EDPB. In caso di sopravvenuta

invalidità del Data Privacy Framework i trasferimenti proseguono sulla base delle clausole contrattuali tipo e delle misure supplementari, secondo l'art. 1.8 del DPA.

8. Esito complessivo

Alla luce della natura dei dati trasferiti (identificativi e professionali, privi di valore per finalità di intelligence, senza categorie particolari), della bassa probabilità concreta di accesso pregiudizievole, dell'adozione di clausole contrattuali tipo con tutti gli importatori e, per i fornitori certificati, del Data Privacy Framework, nonché delle misure supplementari tecniche, contrattuali e organizzative descritte, i trasferimenti verso gli Stati Uniti oggetto della presente valutazione presentano un rischio residuo accettabile e possono essere effettuati. L'esito è subordinato al mantenimento delle misure e alla revisione periodica di cui al punto 7.