



noyb – European Center for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Vienna
AUSTRIA

Garante per la Protezione dei Dati Personali

Piazza Venezia 11
00187 – Roma
Italy
Via e-mail: [REDACTED]

Vienna, 27 Ottobre 2026

Numero di pratica *noyb*: **C109-04**

reclamante:



Rappresentata ex articolo
80(1) GDPR da:

noyb – European Center for Digital Rights
Goldschlagstraße 172/4/3/2, 1140 Vienna, Austria

Convenuto:

Scale AI, Inc.,
650 Townsend Street,
San Francisco
Stati Uniti

Riguardante:

Violazione degli articoli 5(1)(c), 12(3), 15, 25(1) e 28,
(1) del GDPR e dell'articolo 122(1) del Codice in ma-
teria di protezione dei dati personali

RECLAMO

1. MANDATO

1. *noyb* – il Centro Europeo per i Diritti Digitali è un’organizzazione senza scopo di lucro attiva nel campo della tutela dei diritti e delle libertà degli interessati, con sede legale in Goldschlagstraße 172/4/3/2, 1140 Vienna, Austria, registrata con numero ZVR: 1354838270 (di seguito: «*noyb*») (**Allegato 1**).
2. *noyb* rappresenta la reclamante ai sensi dell’articolo 80(1) GDPR (**Allegato 2**).

2. CONTESTO

3. Il lavoro mediante piattaforme digitali è una forma di occupazione che coinvolge centinaia di milioni di persone, di cui almeno 43 milioni in Europa. Il loro numero è più che raddoppiato dal 2022 e si prevede che cresca in modo esponenziale (di seguito «Platform Work»).
4. Platform work comprende, tra le altre categorie, alcuni corrieri, i cosiddetti autisti «uberizzati» e gli annotatori di dati, che si occupano della moderazione e dell’addestramento dei sistemi di intelligenza artificiale. Con riguardo agli annotatori, si tratta di una categoria il cui numero è cresciuto in modo particolarmente rapido negli ultimi tempi. Questa ultima categoria rappresenta l’oggetto del presente reclamo.
5. Platform Work comporta generalmente una particolare vulnerabilità rispetto ad altri lavori. In primo luogo, i lavoratori sono spesso — erroneamente — considerati lavoratori autonomi, il che li esclude dalle prestazioni sociali associate allo status di dipendente. Inoltre, più della metà di queste persone *«guadagna meno del salario minimo orario netto nel paese in cui lavora»*.
6. Inoltre, l’uso di algoritmi nelle operazioni delle piattaforme crea e/o aggrava la discriminazione. Infine, le piattaforme sottopongono i lavoratori a una maggiore sorveglianza digitale.
7. Il legislatore europeo, ben consapevole di queste problematiche, sta attualmente elaborando un quadro giuridico per tutelare questi lavoratori.⁴ Le autorità svolgono un ruolo fondamentale nell’indagare sulle pratiche delle piattaforme e nel garantire il rispetto dei diritti degli interessati. Il Garante e l’autorità olandese, ad esempio, hanno recentemente inflitto sanzioni a Glovo e Uber in relazione a processi decisionali automatizzati illegali.⁵

¹<https://www.consilium.europa.eu/it/infographics/digital-platform-workers/>, consultato il 20.10.2026.

²<https://www.consilium.europa.eu/it/infographics/digital-platform-workers/>, consultato il 20.10.2026.

³Garante per la protezione dei dati personali, n. 675 del 13 novembre 2024, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10074601>.

⁴<https://www.consilium.europa.eu/it/infographics/digital-platform-workers/>, consultato il 20.10.2026.

⁵Garante, Decisione n. 10074601, del 13 novembre 2024, Data Protection Authority olandese: <https://autoriteitpersoonsgegevens.nl/actueel/uber-krijgt-boete-van-bijna-825-miljoen-euro-voor-geautomatiseerd-blokkeren-van-chauffeurs>, consultato il 20.10.2026.

3. I FATTI

3.1. Il convenuto

8. Scale AI (di seguito: “il titolare del trattamento” o “il convenuto”) è una società con sede a San Francisco, negli Stati Uniti, che, tra le altre attività, agisce in qualità di titolare del trattamento dei dati per Outlier, una piattaforma di annotazione dei dati (di seguito la “Piattaforma”).⁶
9. Attraverso la Piattaforma, il Convenuto organizza il lavoro di centinaia di migliaia di persone che annotano i dati e addestrano i sistemi di IA per clienti quali Meta, OpenAI o X.ai.⁷
10. Il lavoro viene generalmente svolto secondo il seguente processo. Un cliente invia i dati al convenuto, il quale (utilizzando algoritmi) assegna a una persona un compito relativo a tali dati — ad esempio, ordinare o etichettare i dati secondo determinati criteri, oppure rispondere a prompt per migliorare i modelli linguistici di grandi dimensioni (LLM). La Piattaforma esamina quindi eventuali errori e assegna a un'altra persona il compito di correggerli e di confermare la qualità del lavoro.

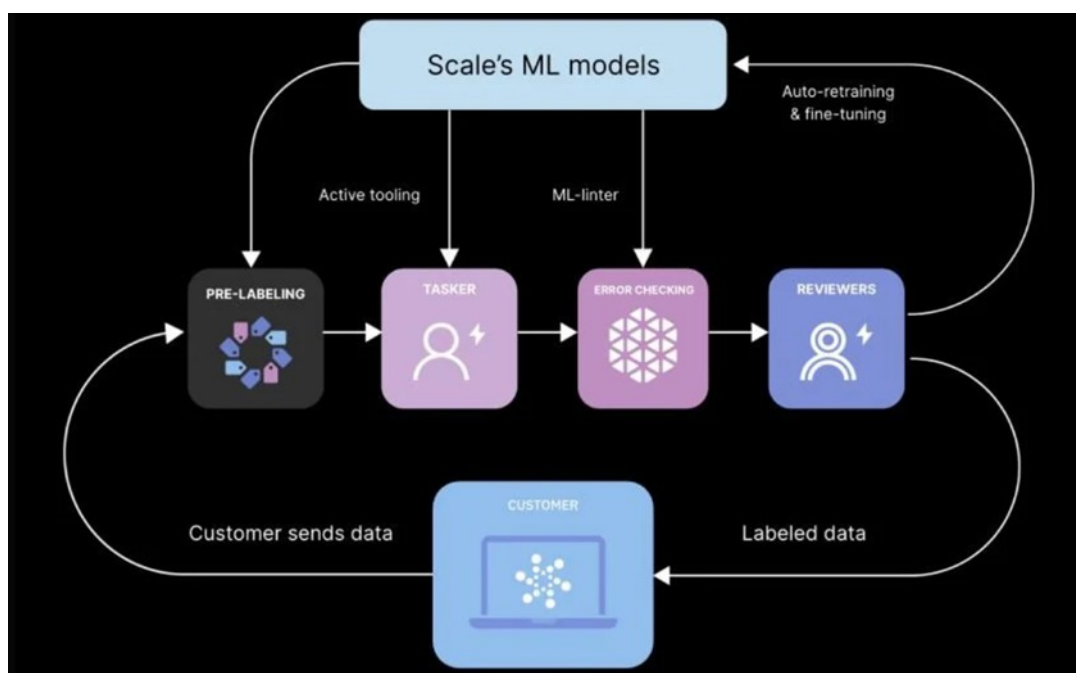


Figura 1: Schema di Scale AI (fonte: <https://www.leadrpro.com/blog/what-is-scale-ai-a-comprehensive-overview/>)

11. I lavoratori vengono assunti come collaboratori autonomi, non come dipendenti. Ricevono una notifica non appena viene loro assegnato un compito e hanno a disposizione un tempo limitato per completarlo; trascorso tale tempo, la tariffa oraria di-

⁶<https://outlier.ai/legal/privacy-policy>, consultato il 20.10.2026.

⁷<https://www.inc.com/sam-blum/leaked-scale-ai-database-offers-new-details-into-projects-for-meta-google-and-x-ai/91176016>, consultato il 20.10.2026.

minuisce (per informazioni sulle condizioni di lavoro all'interno della Piattaforma, si veda l'**Allegato 3**).

12. Da un'analisi dell'informativa sulla privacy del convenuto, disponibile sul suo sito web⁸, emerge che il convenuto effettua il trattamento di una quantità significativa di dati relativi ai propri lavoratori, inclusa una categoria di dati personali raccolti automaticamente (i "Dati raccolti automaticamente"). Tale categoria comprende l'identificativo univoco del dispositivo utilizzato, l'indirizzo IP, le informazioni raccolte tramite cookies o pixel (non identificati nel documento) e il sito web visitato prima di accedere alla Piattaforma. Il convenuto effettua il trattamento di questi dati per varie finalità, tra cui il proprio «*interesse legittimo alla gestione della piattaforma*» (**Allegato 4**).
13. Il convenuto afferma inoltre di effettuare il trattamento dei Dati raccolti automaticamente per il proprio interesse legittimo a sviluppare i propri servizi e prodotti, nonché a ricercare e testare miglioramenti relativi ai servizi dei propri clienti — vale a dire, per l'addestramento dei propri sistemi di intelligenza artificiale.

3.2. La reclamante

14. Nell'██████ la reclamante ha creato un account sulla Piattaforma. A tal fine, si è sottoposta a una procedura di verifica dell'identità (cfr. Sezione 3.3). Ha completato circa 488 attività fino al 4 febbraio 2025 (**Allegato 5**).
15. Le attività consistono, ad esempio, nel confrontare modelli di IA conversazionale valutando le diverse risposte fornite dall'LLM a un determinato «prompt».

3.3. Trattamento dei dati biometrici

16. Come indicato sopra, per creare il proprio account, la reclamante ha dovuto verificare la propria identità tramite un servizio (Persona) fornito da un terzo (Persona Identities Inc.)⁹. Le è stato chiesto di caricare un documento d'identità e, successivamente, di attivare la fotocamera del proprio telefono o computer per registrare un video di sé stessa. La verifica è stata successivamente ripetuta a intervalli irregolari (**Allegato 6**).
17. L'informativa sulla privacy della Piattaforma conferma che la reclamante è stata sottoposta alle verifiche sopra descritte. Stando all'informativa, la verifica dell'identità avviene tramite una foto o un video "selfie" oppure una registrazione vocale, insieme all'analisi del documento di identità dell'utente. La Piattaforma dichiara inoltre di effettuare il trattamento di questi dati «*per contribuire a preservare l'integrità dei Servizi*

⁸<https://outlier.ai/legal/privacy-policy>, consultato il 20.10.2026.

⁹<https://withpersona.com/legal/idv-privacy-policy?ajs=e34c9eb2-fc5d-42ba-881a-3e4a542d2e57#8-contact-us>, consultato il 20.10.2026.

¹⁰<https://outlier.ai/legal/privacy-policy>, consultato il 20.10.2026.

e combattere le frodi” verificando i requisiti e generando dati di riconoscimento facciale.¹¹

«(...) quando ti registri per utilizzare i Servizi, e successivamente a intervalli regolari, potremmo raccogliere, archiviare e analizzare immagini, nonché registrazioni video o audio che ti ritraggono — inclusi selfie e immagini del tuo documento d'identità ufficiale — e utilizzare tali immagini e registrazioni per verificare i tuoi requisiti o generare informazioni e misurazioni relative al tuo volto (“Dati di verifica”), che potrebbero essere considerati dati “biometrici” o “sensibili” ai sensi delle leggi di alcune giurisdizioni»¹² (traduzione libera, enfasi aggiunta).

18. Persona tratta i dati che le vengono trasmessi in conformità con la propria informativa sulla privacy, alla quale fa riferimento il convenuto. Questo documento descrive il trattamento effettuato da Persona nell'ambito della fornitura del proprio servizio. In particolare, Persona si riserva il diritto di raccogliere dati da un numero illimitato di “terzi” non meglio definiti. A tale riguardo, l'informativa fornisce solo categorie generali di informazioni raccolte tramite un elenco aperto, che “include” solo vari esempi, quali indirizzi IP, informazioni sul dispositivo, dati di geolocalizzazione, identificatori univoci, dati relativi all'indirizzo, dati sul credito al consumo e altri dati:

«Potremmo inoltre raccogliere le seguenti informazioni da voi, nostri clienti, o da terze parti al fine di determinare e fornire il metodo di verifica dell'identità appropriato per la vostra giurisdizione e garantire la conformità alle leggi e ai regolamenti applicabili:

- (...) **Informazioni sul dispositivo**, tra cui indirizzo IP, tipo di dispositivo, sistema operativo del dispositivo, browser, cookies e identificatori del dispositivo, nonché altri software, inclusi tipo, versione, lingua, impostazioni e configurazione;

- (...) **Dati disponibili pubblicamente**, inclusi quelli provenienti da registri pubblici e dai social media;

- (...) **Dati aggiuntivi per la verifica dell'età**: potremmo verificare i vostri dati personali ai fini della verifica dell'età attraverso il nostro network di fonti affidabili di dati di terze parti, tra cui: fonti accessibili al pubblico (come banche dati governative pubblicamente accessibili), registri nazionali e governativi di identità, agenzie di valutazione del merito creditizio dei consumatori, aziende di servizi pubblici, operatori di rete mobile e banche dati di indirizzi postali. I tipi di “dati supplementari per la verifica dell'età” che otteniamo da queste fonti variano a seconda dei controlli di verifica disponibili nel paese in questione”¹³ (traduzione libera, enfasi aggiunta).

19. Persona si avvale attualmente di circa quindici fornitori, tra cui OpenAI, Groqcloud e Anthropic, per varie attività di estrazione e analisi dei dati.¹⁴ Il trattamento dei dati

¹¹““use those images and recordings to check your skills or generate information and measurements about your face (“Verification Data”), which may be considered “biometric” data or “sensitive” data under the laws of some jurisdictions.”, <https://outlier.ai/legal/privacy-policy>, consultato il 20.10.2026.

¹²<https://outlier.ai/legal/privacy-policy>, consultato il 20.10.2026.

¹³<https://withpersona.com/legal/privacy-policy>, consultato il 20.10.2026.

¹⁴<https://withpersona.com/legal/subprocessors>, consultato il 20.10.2026.

avviene tramite infrastrutture con sede negli Stati Uniti, tra cui Amazon Web Services e Google Cloud.¹⁵

20. Sono state inoltre segnalate pratiche di sicurezza discutibili da parte di Persona. Ad esempio, nell'ottobre 2025 degli hackers hanno rubato circa 70.000 foto di documenti d'identità ufficiali archiviati presso Persona. Nel febbraio 2026 è inoltre emerso che il codice sorgente di Persona era accessibile al pubblico.¹⁶ Tale codice ha rivelato, tra l'altro, che (i) per ogni "verifica dell'identità", Persona può eseguire 269 controlli distinti, compresi i confronti tra i dati forniti e i database; e che (ii) Persona filtra i "contenuti mediatici sfavorevoli" in base a 14 categorie (tra cui terrorismo e spionaggio), assegnando punteggi di rischio e di "somiglianza".¹⁷
21. Persona ha confermato queste vulnerabilità di sicurezza.¹⁸ Queste pratiche hanno infatti portato uno dei suoi principali clienti, la piattaforma Discord, a rescindere il contratto con Persona per la verifica dell'età dei propri utenti.¹⁹
22. L'informativa sulla privacy di Persona è stata aggiornata il 9 aprile 2026. La versione precedente, in vigore sin dalla registrazione del reclamante,²⁰ prevedeva la possibilità di trattare i documenti di identità ai fini della «formazione del servizio» al fini di «addestrare il Servizio» («*to train the Service*») tramite i propri sistemi di intelligenza artificiale (vedi screenshot qui sotto).²¹

¹⁵ <https://withpersona.com/legal/subprocessors>, consultato il 20.10.2026.

¹⁶ <https://vmfunc.re/blog/persona>, <https://www.franceinfo.fr/internet/reseaux-sociaux/la-plateforme-discord-repousse-la-verification-d-age-pour-la-fin-2026-apres-des-critiques-sur-la-securite-des-donnees-7829012.html>, consultato il 20.10.2026.

¹⁷ <https://www.malwarebytes.com/blog/news/2026/02/age-verification-vendor-persona-left-frontend-exposed> e <https://vmfunc.re/blog/persona>, consultato il 20.10.2026. <https://www.franceinfo.fr/internet/reseaux-sociaux/la-plateforme-discord-repousse-la-verification-d-age-pour-la-fin-2026-apres-des-critiques-sur-la-securite-des-donnees-7829012.html>

¹⁸ <https://withpersona.com/blog/post-incident-review-source-map-exposure-non-production-subdomain>.

¹⁹ <https://www.franceinfo.fr/internet/reseaux-sociaux/la-plateforme-discord-repousse-la-verification-d-age-pour-la-fin-2026-apres-des-critiques-sur-la-securite-des-donnees-7829012.html>, consultato il 20.10.2026.

²⁰ Si veda, ad esempio, la versione del 12 gennaio 2025: <https://web.archive.org/web/20250112151512/https://withpersona.com/legal/idv-privacy-policy>, consultato il 20.10.2026.

²¹ L'informativa sulla privacy di Persona è disponibile all'indirizzo <https://withpersona.com/legal/idv-privacy-policy>. Consultata il 3 giugno 2026. La versione aggiornata il 9 aprile 2026 è disponibile qui: <https://web.archive.org/web/20260422094923/https://withpersona.com/legal/idv-privacy-policy>. La versione aggiornata l'8 maggio 2025, che include una dichiarazione relativa all'utilizzo da parte del servizio dei documenti caricati dagli utenti per finalità di addestramento, è disponibile qui: <https://web.archive.org/web/20260326065823/https://withpersona.com/legal/idv-privacy-policy>

To improve the Service, develop new features, and conduct research. For example: • We use uploaded images of identity documents to train the Service to accurately verify identity documents (e.g. by learning to distinguish what passports look like in different countries). • We use uploaded images of identity documents and your selfie to identify improvements in the Service (e.g. to determine the best types of image captured to ensure the most accurate image recognition and to assess sufficient image clarity to aid with the verification process)	Uploaded Content Geolocation Data Identifiers and Device Information Usage Data	Necessary for our legitimate interests to improve the Service and use insights to develop new features.
--	---	--

Figura 2: Informativa sulla privacy precedente al 9 aprile 2026

3.4. Analisi del traffico

23. Il [REDACTED], la reclamante ha acquisito il traffico sulla Piattaforma sotto forma di file HAR²² mentre navigava sulla Piattaforma (**Allegati 7, 8 e 9**). L'acquisizione del traffico ha seguito la metodologia descritta nell'**Allegato 10**.
24. Gli **Allegati 7, 8 e 9** mostrano che la Piattaforma utilizza trackers²³ inseriti dalle seguenti terze parti: Fullstory, Sprig, TikTok, Facebook, Posthog, Segment, Quora, Snapchat, Run.app, Twitter Analytics, Google, Recruitics e Amplitude.
25. Un altro interessato ha analizzato il traffico mentre verificava la propria identità con Persona e ha riscontrato la presenza di trackers di Fullstory, Amplitude, Posthog e Datahog HQ.
26. La Figura 3 mostra il numero di richieste identificate per alcune di queste terze parti negli **Allegati 7, 8 e 9**.²⁴ Di seguito sono riportate spiegazioni più dettagliate relative ad alcuni esempi di trackers.

²² Un file HAR (abbreviazione di *HTTP Archive*) è un registro completo delle interazioni tra un browser e i server web durante una sessione di navigazione.

²³ Un tracker è uno strumento — spesso invisibile — che raccoglie informazioni sul comportamento online di una persona. Può registrare i siti web visitati, le pagine visualizzate, il tempo trascorso sui contenuti, la posizione approssimativa dell'utente, il tipo di dispositivo utilizzato e così via. Con riguardo ai pixel di tracciamento, si tratta di «un metodo di tracciamento alternativo ai cookie, tradizionalmente implementato come immagine di 1 pixel per 1 pixel incorporata nel sito web ma invisibile all'utente. Il caricamento di questa immagine, il cui nome contiene un identificatore utente, comunica al server che la ospita che l'utente tracciato ha visitato una pagina o letto un'e-mail» (traduzione libera). Vedi <https://www.cnil.fr/fr/definition/tracking-pixelweb-beacon-ou-pixel-espion>, consultato il 20.10.2026.

²⁴ Una richiesta è una query inviata da un programma o dispositivo a un altro, in attesa di una risposta.

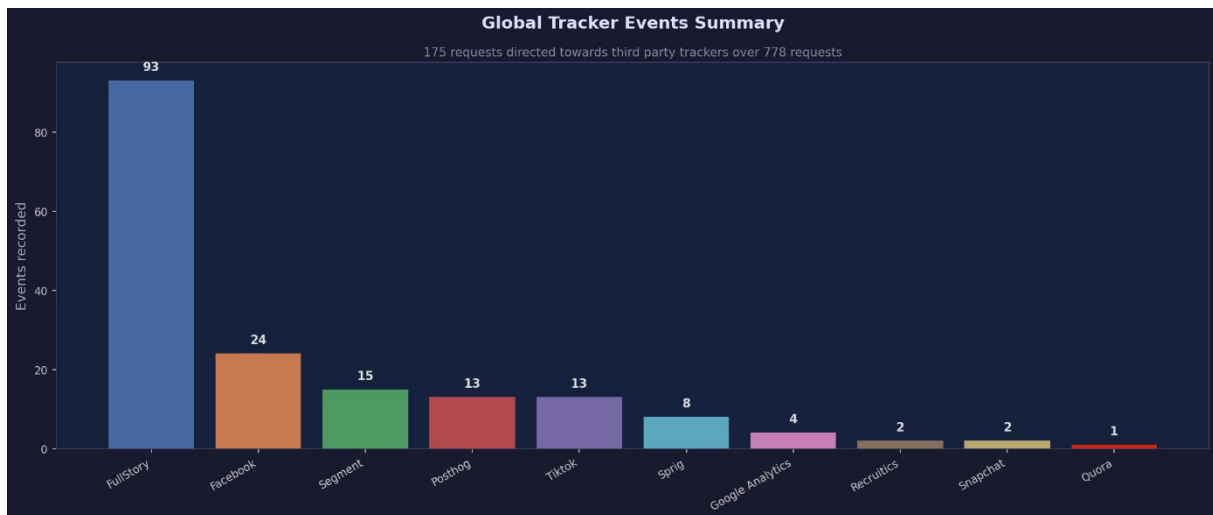


Figure 1: Riepilogo dei trackers nelle Allegati 7, 8 e 9

Esempio 1: Trackers dei “social media”

I file HAR (Allegati 7, 8 e 9) mostrano la presenza di trackers di Facebook, Twitter, Snapchat e TikTok. Il tracker di Twitter, ad esempio, viene solitamente utilizzato per la pubblicità mirata.²⁵

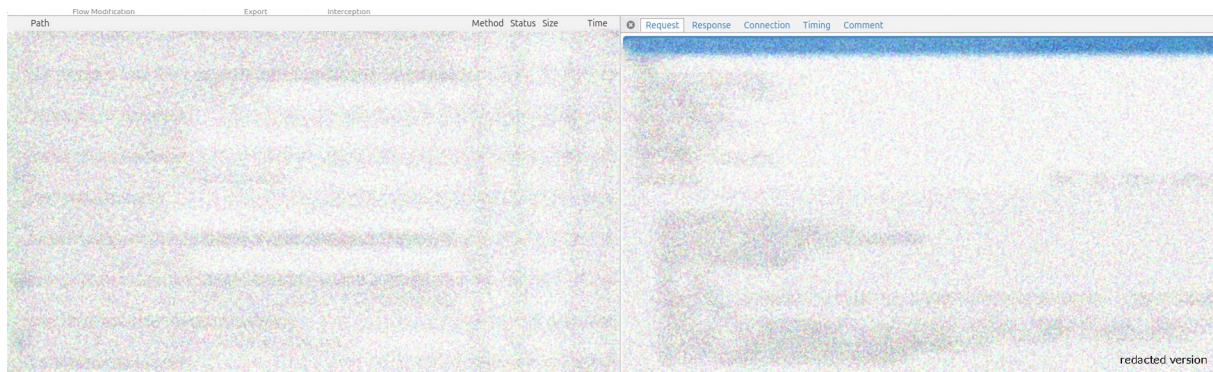


Figure 2: Tracker di Twitter

27. Fullstory offre uno strumento di riproduzione (*session replay*) delle sessioni che registra i movimenti del mouse, i clic, le battute sulla tastiera, ecc.²⁶ In questo caso, il tracker di Fullstory invia una richiesta ogni pochi secondi. Il tracker registra eventi specifici come la pagina che la reclamante sta consultando (vedi Allegati 7, 8 e 9).

Altri esempi

²⁵ <https://pantosource.com/blog/meta-ads-data-quality?>, consultato il 20.10.2026.

²⁶ Vedi la presentazione di Fullstory sul suo servizio: <https://www.youtube.com/watch?v=Q18TO1lZVz8>, consultato il 20.10.2026.

28. Un altro tracker è implementato da Sprig²⁷, che fornisce strumenti di sondaggio interni che un datore di lavoro può somministrare ai propri dipendenti. In questo caso, la reclamante non stava rispondendo a un sondaggio durante l'analisi. Ciononostante, il tracker raccoglie identificatori univoci, informazioni sul dispositivo e la pagina visitata. Per altri interessati, Sprig ha raccolto anche cognome, nome, indirizzo e-mail, numero di telefono e informazione di pagamento.

3.3. La richiesta di accesso

29. Il 17 dicembre 2025 la reclamante ha inviato una richiesta di accesso all'indirizzo e-mail privacy@outlier.ai, come specificato nell'informativa sulla privacy della piattaforma (**Allegato 11**). Con la sua richiesta d'accesso la reclamante chiedeva, tra l'altro, se il convenuto avesse applicato nei suoi confronti un processo decisionale automatizzato.

30. Nonostante un sollecito inviato il 23 gennaio 2026, anch'esso indirizzato a outlier@lionheartssquared.eu, il convenuto non ha ancora risposto a tale richiesta.

31. Il 21 maggio 2026 la reclamante ha inoltre richiesto l'accesso ai propri dati a Persona, la quale, dopo aver confermato la ricezione della richiesta, ha invitato la reclamante a rivolgersi a Outlier (**Allegato 12**).

4. COMPETENZA

32. La reclamante vive e lavora in Italia, mentre il convenuto ha sede negli Stati Uniti, senza una sede principale di attività nell'Unione europea. Il Garante è pertanto competente a trattare il presente reclamo ai sensi dell'articolo 77 del GDPR.

5. MOTIVI DEL RECLAMO

5.1. Violazioni

33. Le pratiche oggetto di esame possono essere suddivise nelle seguenti categorie: (1) l'inserimento di trackers; (2) il trattamento dei dati biometrici; e (3) la richiesta di accesso. Esse violano rispettivamente:

(1.a) l'articolo 5(1)(c), del GDPR, in quanto il trattamento dei dati del reclamante e l'archiviazione di trackers violano il principio di minimizzazione dei dati;

(1.b) l'articolo 5(3) della Direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche (Direttiva ePrivacy), recepito in Italia dall'articolo 122, comma 1, del Codice in materia di protezione dei dati personali, per aver archiviato trackers sul dispositivo della reclamante senza il suo consenso;

²⁷<https://sprig.com/>, consultato il 20.10.2026.

(2) gli articoli 5(1)(c), in combinato disposto con gli articoli 25(1), e 28(1) GDPR, per aver effettuato il trattamento dei dati biometrici della reclamante in violazione del principio di minimizzazione dei dati, della scelta di un responsabile del trattamento adeguato, e del principio di protezione dei dati per impostazione predefinita;

(3) gli articoli 15 e 12(3) del GDPR, per non aver dato seguito alla richiesta di accesso presentata dalla reclamante.

(1.a) Violazione dell'articolo 5(1)(c) GDPR

34. Il principio di minimizzazione dei dati è un'applicazione del principio di proporzionalità, che richiede che qualsiasi interferenza con un diritto fondamentale sia proporzionata.²⁸ In particolare, l'articolo 5(1)(c) GDPR richiede che i dati trattati siano adeguati, pertinenti e limitati a quanto strettamente necessario per le finalità perseguite.
35. Nel caso in esame, come descritto sopra (§13), il convenuto effettua il trattamento di dati raccolti automaticamente quali l'indirizzo IP, il sito web visitato dalla reclamante prima di accedere alla piattaforma, informazioni che identificano in modo univoco il dispositivo, e i trackers di cui sopra (sezione 3.4).
36. Le finalità dichiarate per il trattamento di tali dati includono:
- la fornitura, la gestione e l'amministrazione della Piattaforma;
 - la personalizzazione del servizio;
 - il miglioramento dei prodotti e dei servizi del convenuto; e
 - il miglioramento dei prodotti e dei servizi delle cliente del convenuto²⁹
 - il miglioramento dei prodotti e dei servizi dei clienti del convenuto.³⁰
37. Un altro documento, la *cookie policy* della Piattaforma, fa riferimento anche alle finalità di profilazione e pubblicità mirata.³¹
38. È difficile comprendere come il trattamento di tutti i Dati raccolti automaticamente — compresi quelli raccolti tramite i trackers descritti nella Sezione 3.4 — possa essere strettamente necessario per le finalità citate. Ad esempio, sapere quale sito web sia stato visitato prima della Piattaforma, o condividere il nome degli interessati, non è chiaramente necessario per nessuna di tali finalità.
39. Appare poi sproporzionato che i dati della reclamante- e in particolare quelli trattati tramite trackers, l'indirizzo IP o il sito web visitato prima della Piattaforma - debbano essere trattati ai fini del miglioramento dei prodotti e dei servizi dei clienti del conven-

²⁸CGUE, *NTH Haustechnik GmbH*, C-484/24, par. 95.

²⁹<https://outlier.ai/legal/privacy-policy>, consultato il 20.10.2026.

³⁰<https://outlier.ai/legal/privacy-policy>, consultato il 20.10.2026.

³¹<https://outlier.ai/legal/cookies-policy>, consultato il 20.10.2026.

uto. E ciò, senza contare che tali finalità includono certamente l'addestramento di sistemi di intelligenza artificiale – e sorvolando, oltretutto, sui seri dubbi sulla legittimità di tale finalità.

40. L'analisi del traffico ha inoltre dimostrato che numerosi *trackers* vengono archiviati da piattaforme di social media, società di analisi e vari fornitori di servizi. Come descritto sopra, questi *trackers* trattano dati quali le informazioni di contatto della reclamante, la sua attività sulla Piattaforma, i movimenti del mouse e gli identificatori univoci. Ancora una volta, è difficile comprendere come un trattamento così sistematico e costante, a beneficio di così tanti destinatari, possa essere strettamente necessario per il perseguimento delle finalità dichiarate.
41. Per quanto riguarda le piattaforme di social media, in particolare, le finalità perseguite dalla Piattaforma sono completamente distinte da quelle delle piattaforme di social media. È quindi ancora più difficile stabilire l'utilità del tracciamento, per non parlare della sua necessità.
42. Va inoltre osservato che la Piattaforma dichiara di perseguire tutte le finalità sopra elencate sulla base del proprio interesse legittimo. Ai sensi dell'articolo 6(1)(f) GDPR, secondo l'interpretazione della CGUE e del EDPB, tale base giuridica richiede, in particolare, che i dati siano trattati in conformità al principio di minimizzazione dei dati per essere valida.³² Una violazione del principio di minimizzazione dei dati rende quindi invalida la base giuridica dell'interesse legittimo.
43. Per raggiungere la finalità di migliorare i propri prodotti e servizi, nel rispetto del principio di minimizzazione dei dati, il convenuto avrebbe potuto trattare solo determinati dati relativi al dispositivo — quali il browser utilizzato, la lingua e il tipo di dispositivo utilizzato (cellulare o computer) — oppure trattare determinati dati solo al verificarsi di specifici eventi, quali i «bug». Per quanto riguarda i trackers, il convenuto avrebbe inoltre dovuto rimuovere una serie di trackers e/o limitare i dati che i trackers possono trattare. In particolare, per quanto riguarda gli strumenti di riproduzione delle sessioni, il convenuto avrebbe potuto, come raccomandato dalla CNIL nel suo progetto di raccomandazioni sugli strumenti di riproduzione delle sessioni³³, utilizzare lo strumento solo occasionalmente e in modo casuale, implementare una tecnica di mascheramento o di hashing, oppure evitare di raccogliere identificatori univoci.
44. Il Garante ha già avuto modo di occuparsi dell'installazione di determinati trackers a fini analitici sui dispositivi dei lavoratori. Tali trackers, proprio come nel caso in es-

³²CGUE, C-252/21, *Meta Platforms Inc. contro Bundeskartellamt*, par. 109; C-708/18, *Asociația de Proprietari bloc M5A-ScaraA*, par. 48; C-621/22, *Koninklijke Nederlandse Lawn Tennisbond*, parr. 51–52; Comitato europeo per la protezione dati, *Linee guida 1/2024 sul trattamento dei dati personali basato sull'articolo 6, par. 1, lettera f), del GDPR*, 8 ottobre 2024, punto 29.

³³https://www.cnil.fr/sites/default/files/2026-02/projet_de_recommandation_rejeu_session.pdf, consultato il 20.10.2026.

ame, consentivano il trattamento degli identificatori dei lavoratori, dei loro indirizzi IP, dei dati relativi ai dispositivi, nonché degli indirizzi e-mail e dei numeri di telefono. Il Garante ha qualificato questo trattamento estensivo e la condivisione dei dati con terzi come sorveglianza, in violazione del principio di minimizzazione dei dati.³⁴

45. Alla luce di quanto sopra esposto, i dati del reclamante sono stati trattati in violazione del principio di minimizzazione dei dati ai sensi dell'articolo 5(1)(c) GDPR.

(1.b) Violazione dell'articolo 5(3) della Direttiva ePrivacy e dell'articolo 122(1) del Codice in materia di protezione dei dati personali

46. L'inserimento di pixel e trackers costituisce un'archiviazione di informazioni sul dispositivo dell'utente ed è pertanto disciplinato anche dall'articolo 5(3) della Direttiva ePrivacy.³⁵

47. L'articolo 122(1) del Codice in materia di protezione dei dati personali recepisce l'articolo 5(3) della suddetta Direttiva e prevede quanto segue:

“L'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o l'accesso a informazioni già archiviate sono consentiti unicamente a condizione che il contraente o l'utente abbia espresso il proprio consenso dopo essere stato informato con modalità semplificate. Ciò non vieta l'eventuale archiviazione tecnica o l'accesso alle informazioni già archiviate se finalizzati unicamente ad effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dal contraente o dall'utente a erogare tale servizio. Ai fini della determinazione delle modalità semplificate di cui al primo periodo il Garante tiene anche conto delle proposte formulate dalle associazioni maggiormente rappresentative a livello nazionale dei consumatori e delle categorie economiche coinvolte, anche allo scopo di garantire l'utilizzo di metodologie che assicurino l'effettiva consapevolezza del contraente o dell'utente”.

48. In questo caso, l'analisi del traffico e l'esame dell'informativa sulla privacy (cfr. sopra, sezione 3.1) hanno dimostrato che il convenuto ha archiviato trackers e pixel sul terminale della reclamante.

49. Il convenuto basa l'archiviazione di tali trackers e pixel sul proprio interesse legittimo, in violazione del suddetto Articolo 122(1) che richiede il consenso dell'interessato.

(2) Violazione dell'articolo 5(1)(c), in combinato disposto con gli articoli 25(1) e 28(1) GDPR

50. L'articolo 25(1) GDPR tutela gli interessati imponendo ai titolari del trattamento di attuare misure tecniche e organizzative adeguate per garantire il rispetto di principi quali la minimizzazione dei dati e la liceità.

³⁴Garante, Decisione n. 10074601, del 13 novembre 2024, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10074601>, Sezione 4.11.

³⁵Comitato europeo per la protezione dati, *Orientamenti 2023/02 sull'ambito di applicazione tecnico dell'art. 5, paragrafo 3, della Direttiva ePrivacy*, §50.

51. Il EDPB precisa che i titolari del trattamento non devono scegliere un responsabile del trattamento che non consenta loro di adempiere ai propri obblighi, poiché sono responsabili del rispetto dell'articolo 25 del GDPR.³⁶ In altre parole, le misure adeguate includono la scelta di un responsabile del trattamento adeguato.³⁷
52. Analogamente, anche l'articolo 28(1) GDPR richiede ai titolari del trattamento di selezionare responsabili del trattamento in grado di garantire la conformità al GDPR.
53. Tali misure sono particolarmente rilevanti quando si tratta del trattamento di dati sensibili ai sensi dell'articolo 9 del GDPR, quali i dati biometrici. Il EDPB precisa, a questo proposito, che il trattamento di tali dati costituisce «*di per sé*» una grave violazione della privacy.³⁸ Le misure possono consistere nella pseudonimizzazione o nell'imporre ai responsabili del trattamento di attuare determinate pratiche di minimizzazione dei dati.³⁹
54. Il Garante stesso ha stabilito, in un caso in cui un'azienda richiedeva ai propri lavoratori mediante piattaforma digitale di identificarsi tramite verifica biometrica, che il trattamento di tali dati non fosse essenziale per la fornitura del servizio in questione.⁴⁰
55. È indiscusso che il convenuto effettui il trattamento dei dati biometrici dell'attore ai fini della verifica dell'identità e dell'età. La presente sezione dimostra (i) che il trattamento dei dati biometrici di per sé non è strettamente necessario, in violazione dell'articolo 5(1)(c) GDPR, e (ii) che, anche se lo fosse, il trattamento delegato a Persona è stato comunque effettuato in violazione degli articoli 5(1)(c), in combinato disposto con gli articoli 25(1) e 28(1) GDPR.

(i) *Il trattamento dei dati biometrici non è necessario*

56. In questo caso, il trattamento dei dati biometrici viene effettuato «*per contribuire a preservare l'integrità dei Servizi e contrastare le frodi*».⁴¹ La formulazione vaga suggerisce che la finalità sia quella di garantire che sia effettivamente il lavoratore scelto a svolgere le mansioni. Nel suddetto caso italiano, il titolare del trattamento perseguiva una finalità simile e ha riconosciuto, nel corso del procedimento, che la verifica biometrica non costituisce *di per sé* una misura sufficiente per prevenire il fenomeno di frode, ma funge piuttosto da deterrente. Il Garante ha quindi concluso

³⁶https://www.edpb.europa.eu/documents/guideline/guidelines-42019-on-article-25-data-protection-by-design-and-by-default_it, consultato il 20.10.2026., §96.

³⁷Analogamente, Garante per la protezione dei dati personali, provvedimento 675 del 13 novembre 2024, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10074601>, Sezione 4.11.

³⁸Linee guida 05/2022 sull'uso della tecnologia di riconoscimento facciale nel settore delle attività di contrasto, 17 maggio 2023, §36.

³⁹https://www.edpb.europa.eu/documents/guideline/guidelines-42019-on-article-25-data-protection-by-design-and-by-default_it, consultato il 20.10.2026, §9.

⁴⁰Garante per la protezione dei dati personali, provvedimento 675 del 13 novembre 2024, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10074601>, Sezione 4.7.

⁴¹<https://outlier.ai/legal/privacy-policy>, consultato il 20.10.2026.

che la verifica biometrica non fosse strettamente necessaria.⁴² Questa considerazione si applica *mutatis mutandis* al caso in esame.

57. Infatti, per raggiungere la finalità dichiarata, esistono altri mezzi meno invasivi per autenticare i lavoratori. Ne sono un esempio l'autenticazione a due fattori (2FA) o una chiave fisica che deve essere inserita per effettuare l'accesso alla piattaforma.

*(ii) Quand'anche il Garante ritenesse necessario il trattamento,
lo stesso violerebbe gli articoli 5(1)(c), 25(1) e 28(1) GDPR*

58. In assenza di una risposta alla sua richiesta di accesso, la reclamante può fare affidamento solo sull'informativa sulla privacy di Persona, la quale afferma che Persona confronta i dati che riceve con quelli provenienti da altre banche dati. Ciò corrisponde a una tecnica di identificazione nota come «uno a molti» («one-to-many»), che consiste nel confrontare un volto con altri volti memorizzati in una banca dati. La tecnica «uno a molti» si contrappone alla tecnica di verifica «uno a uno» («one-to-one»), che in questo contesto comporterebbe il confronto di un volto con un documento di identità.

59. La direttiva (UE) 2024/2831 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativa al miglioramento delle condizioni di lavoro nel Platform Work — sebbene non ancora recepita — potrebbe essere utile per valutare la legittimità di questo tipo di verifica. Il Considerando 41 afferma espressamente che, qualora sia necessario effettuare il trattamento dei dati biometrici, si dovrebbe ricorrere al metodo di verifica «uno a uno».

60. In questo caso, il trattamento dei suddetti dati è chiaramente eccessivo rispetto alla finalità perseguita, ovvero la verifica dell'identità.

61. Per rispettare il principio di minimizzazione dei dati, la verifica dovrebbe essere effettuata utilizzando il metodo «uno a uno», e a Persona non dovrebbe essere consentito di raccogliere dati diversi da quelli strettamente necessari. Spetta infatti al convenuto selezionare un fornitore di servizi adeguato per tale verifica e consentire a tale fornitore di raccogliere solo determinati dati.

62. Noyb è inoltre a conoscenza di un altro interessato che ha acquisito il traffico durante la verifica della propria identità con Persona. Dalla registrazione è emerso che Persona effettua il trattamento di dati relativi al dispositivo utilizzato, all'indirizzo IP e ad altri dati.

63. Richiedendo al reclamante di sottoporsi al trattamento dei propri dati biometrici in violazione del principio di minimizzazione dei dati, il convenuto non solo ha violato tale principio, ma anche il proprio obbligo di attuare misure tecniche e organizzative adeguate, che includono la selezione di un fornitore di servizi o di un responsabile del

⁴²Garante per la protezione dei dati, provvedimento 675 del 13 novembre 2024, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10074601>, Sezione 4.7.

trattamento adeguato. In conclusione, il convenuto ha violato gli articoli 5(1)(c), 25(1) e 28(1) GDPR.

(3) Violazione degli articoli 15 e 12(3) GDPR

64. L'articolo 15 GDPR impone ai titolari del trattamento di dare seguito alle richieste di accesso formulate dagli interessati. L'articolo 12(3) GDPR richiede una risposta il più presto possibile e comunque entro un mese dalla presentazione della richiesta.
65. Nel caso in esame, la reclamante sospettava di essere soggetta a un processo decisionale automatizzato e aveva espressamente chiesto al convenuto di informarla in merito (**Allegato 11**). Tale richiesta è rimasta senza risposta. Non avendo risposto alla richiesta di accesso della reclamante, il convenuto ha violato l'articolo 15 del GDPR e, di conseguenza, l'articolo 12(3) GDPR.

6. RICHIESTE

6.1 Decisione dichiarativa

66. La reclamante chiede al Garante di dichiarare che il convenuto ha commesso le seguenti violazioni:
- la violazione dell'articolo 5(1)(c) GDPR per aver effettuato il trattamento di dati della reclamante che non erano necessari alle finalità perseguite;
 - la violazione dell'articolo 122(1) del Codice in materia di protezione dei dati personali per aver archiviato trackers e pixel senza il consenso della reclamante;
 - la violazione degli articoli 5(1)(c), 25(1) e 28(1) GDPR da parte del convenuto per aver effettuato il trattamento dei dati biometrici e aver incaricato un responsabile del trattamento che non ha tenuto conto (tra gli altri) del principio di minimizzazione dei dati;
 - la violazione degli articoli 12(3) e 15 per mancata risposta alla richiesta di accesso.

6.2 Accesso

67. La reclamante chiede al Garante di ordinare al convenuto di accogliere la sua richiesta di accesso.

6.3 Indagine

68. La reclamante chiede che il Garante indaghi sulle violazioni esposte nel reclamo ed estenda la propria indagine per includere l'utilizzo, da parte del convenuto, di processi decisionali automatizzati.

6.4 Raccomandazione di infliggere una sanzione amministrativa

69. La reclamante suggerisce che il Garante infligga una sanzione amministrativa pecuniaria al titolare del trattamento, ai sensi degli articoli 58(2)(i), e 83(5)(a) e (b) GDPR per le violazioni sopra elencate.

7. CONTATTI

70. Le comunicazioni tra *noyb* e il Garante relative al presente procedimento possono essere inviate via e-mail all'indirizzo [REDACTED], citando il numero di caso C109-04, oppure per telefono al numero [REDACTED].