



noyb – European Center for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Wien
Österreich

Datenschutzbehörde (DSB)

Barichgasse 40–42

1030 Wien

Per E-Mail [REDACTED]

Wien, 27.10.2026

noyb-Fall-Nr.: C109-02

Beschwerdeführer:

[REDACTED]
geboren am [REDACTED]
[REDACTED]

vertreten gemäß
Artikel 80(1) der DSGVO
durch:

noyb – European Center for Digital Rights
Goldschlagstraße 172/4/3/2, 1140 Wien, Österreich

Antragsgegner:

**Scale AI, Inc.,
650 Townsend Street, San Francisco
Vereinigte Staaten**

wegen:

**Verstoß gegen Artikel 5(1)(c) Artikel 12(3), Artikel
15, Artikel 25(1) und Artikel 28(1) DSGVO sowie
gegen Artikel 165(3) des
Telekommunikationsgesetzes 2021**

BESCHWERDE

1. VERTRETUNG

1. *noyb* – European Center for Digital Rights ist eine gemeinnützige Organisation, die im Bereich des Schutzes der Rechte und Freiheiten betroffener Personen tätig ist, mit Sitz in der Goldschlagstraße 172/4/3/2, 1140 Wien, Österreich, ZVR-Nummer: 1354838270 (im Folgenden: „noyb“) (**Beilage 1**).
2. *noyb* ist der Vertreter des Beschwerdeführers gemäß Artikel 80(1) DSGVO (**Beilage 2**).

2. HINTERGRUND

3. Plattformarbeit ist eine Beschäftigungsform, von der Hunderte Millionen Menschen betroffen sind, darunter mindestens 43 Millionen in Europa. Ihre Anzahl hat sich seit 2022 mehr als verdoppelt und wird voraussichtlich exponentiell wachsen (im Folgenden „Plattformarbeit“).¹
4. Zur Plattformarbeit zählen unter anderem Kuriere, sogenannte „Uberisierte“ Fahrer sowie – eine Kategorie, deren Zahl in letzter Zeit besonders schnell gewachsen ist – Datenannotatoren, die an der Moderation und dem Training von Systemen der künstlichen Intelligenz arbeiten. Diese letzte Kategorie ist Gegenstand dieser Beschwerde.
5. Plattformarbeit ist im Vergleich zu anderen Beschäftigungsformen im Allgemeinen mit einer besonderen Gefährdung verbunden. Erstens werden die Arbeiter oft – zu Unrecht – als selbstständig eingestuft, wodurch ihnen die mit dem Arbeitnehmerstatus verbundenen sozialen Leistungen vorenthalten werden. Zudem „verdient“ mehr als die Hälfte dieser Personen *„weniger als den Netto-Mindeststundenlohn in dem Land, in dem sie arbeiten“*.²
6. Zudem führt der Einsatz von Algorithmen im Plattformbetrieb zu Diskriminierung oder verschärft diese. Schließlich unterziehen Plattformen die Arbeiter einer verstärkten digitalen Überwachung.³
7. Der europäische Gesetzgeber ist sich dieser Probleme bewusst und arbeitet derzeit an einem Rechtsrahmen zum Schutz dieser Arbeiter.⁴ Aufsichtsbehörden spielen eine zentrale Rolle bei der Untersuchung der Arbeitsweise der Plattformen und bei der Durchsetzung der Betroffenenrechte. Beispielsweise haben die italienische und die

¹<https://www.consilium.europa.eu/fr/infographics/digital-platform-workers/>, abgerufen am 20.10.2026.

²<https://www.consilium.europa.eu/fr/infographics/digital-platform-workers/>, abgerufen am 20.10.2026.

³Datenschutzbehörde, Entscheidung 10074601 vom 13. November 2024, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10074601>.

⁴<https://www.consilium.europa.eu/fr/infographics/digital-platform-workers/>, abgerufen am 20.10.2026.

niederländische Aufsichtsbehörde kürzlich Bußgelder gegen Glovo und Uber wegen rechtswidriger automatisierte Entscheidungsfindung verhängt.⁵

3. SACHVERHALT

3.1. Die Beschwerdegegnerin

8. Scale AI ist ein Unternehmen mit Sitz in San Francisco, USA, das unter anderem als Verantwortlicher für Outlier fungiert, einer Plattform zur Datenannotation (im Folgenden: „Plattform“).⁶
9. Über die Plattform organisiert die Beklagte die Arbeit von Hunderttausenden von Personen, die Daten annotieren und KI-Systeme für Kunden wie Meta, OpenAI oder X.ai trainieren.⁷
10. Die Arbeit wird in der Regel nach folgendem Ablauf durchgeführt: Ein Kunde sendet Daten an den Beschwerdegegnerin, die (mithilfe von Algorithmen) einer Person eine Aufgabe im Zusammenhang mit diesen Daten zuweist – beispielsweise das Sortieren oder Kennzeichnen der Daten nach bestimmten Kriterien oder das Beantworten von Aufforderungen zur Verbesserung großer Sprachmodelle (LLMs). Die Plattform überprüft anschließend etwaige Fehler und weist einer anderen Person die Aufgabe zu, diese zu korrigieren und die Qualität der Arbeit zu bestätigen.

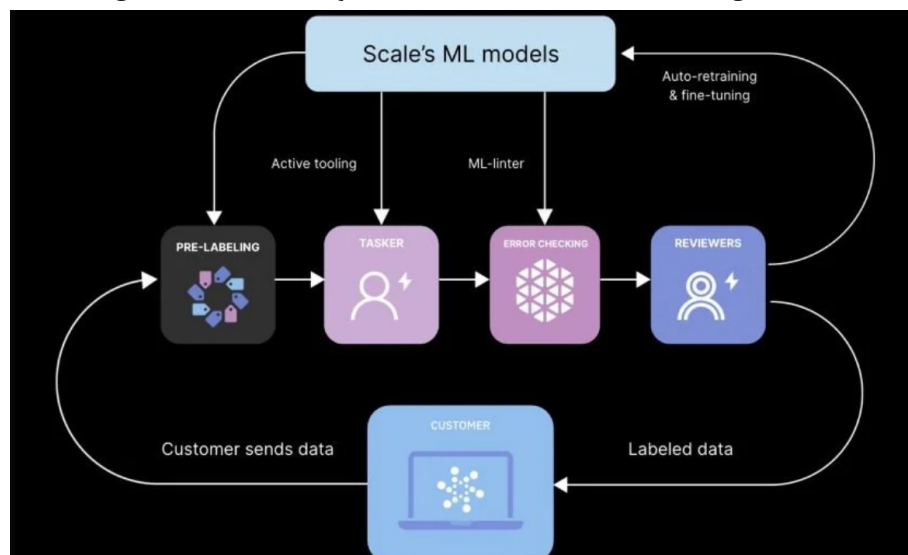


Abbildung 1: Quelle: <https://www.leadrpro.com/blog/what-is-scale-ai-a-comprehensive-overview>

⁵Italienische Datenschutzbehörde, Entscheidung 10074601 vom 13. November 2024, [Dutch Data Protection Authority, https://autoriteitpersoonsgegevens.nl/actueel/uber-krijgt-boete-van-bijna-825-miljoen-euro-voor-geautomatiseerd-blokkeren-van-chauffeurs](https://autoriteitpersoonsgegevens.nl/actueel/uber-krijgt-boete-van-bijna-825-miljoen-euro-voor-geautomatiseerd-blokkeren-van-chauffeurs), abgerufen am 20.10.2026..

⁶<https://outlier.ai/legal/privacy-policy>, abgerufen am 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>, abgerufen am 20.10.2026..

11. Die Arbeiter werden als unabhängige Auftragnehmer und nicht als Angestellte beschäftigt. Sie erhalten eine Benachrichtigung, sobald ihnen eine Aufgabe zugewiesen wird, und haben dann eine begrenzte Zeit, diese zu erledigen; danach sinkt der Stundensatz (für Informationen zu den Arbeitsbedingungen auf der Plattform siehe **Beilage 3**).
12. Eine Aufgabe kann beispielsweise darin bestehen, mehrere Antworten zu vergleichen, die ein LLM als Reaktion auf die Anfrage eines Nutzers generieren könnte. Sie kann auch die Korrektur von Antworten umfassen, die ein LLM in einem bestimmten Fachgebiet wie Programmierung, Physik oder Mathematik liefert.
13. Eine Überprüfung der Datenschutzerklärung der Beschwerdegegnerin⁸ zeigt, dass diese eine erhebliche Menge an Daten über ihre Arbeiter verarbeitet, darunter Datenkategorien, die automatisch erfasst werden („Automatisch erhobene Daten“). Zu diesen Datenkategorien gehören die eindeutige Kennung des verwendeten Geräts, die IP-Adresse, Informationen, die über Cookies oder Pixel erfasst werden (die im Dokument nicht näher bezeichnet werden) sowie die Website, die vor dem Zugriff auf die Plattform besucht wurde. Die Beschwerdegegnerin verarbeitet diese Daten zu verschiedenen Zwecken, darunter zum Zweck ihres „berechtigten Interesses am Betrieb der Plattform“ (**Beilage 4**).
14. Die Beschwerdeführerin gibt außerdem an, dass sie automatisch erhobene Daten aufgrund ihres berechtigten Interesses an der Weiterentwicklung ihrer Dienste und Produkte sowie an der Erforschung und Erprobung von Verbesserungen der Dienste ihrer Kunden verarbeitet – das heißt, zum Training ihrer KI-Systeme.

3.2. Der Beschwerdeführer

15. Im April 2025 richtete der Beschwerdeführer ein Konto auf der Plattform ein. Dazu durchlief er einen Identitätsprüfungsprozess (siehe Abschnitt 3.3). Bis September 2025 erledigte er etwa 10 Aufgaben.
16. Zu den Aufgaben gehört beispielsweise der Vergleich von dialogorientierten KI-Modellen durch die Bewertung verschiedener Antworten, die das LLM auf eine bestimmte „Eingabe“ liefert.

3.3. Verarbeitung biometrischer Daten

17. Wie oben erwähnt, musste der Beschwerdeführer zur Einrichtung seines Kontos seine Identität über einen von einem Subunternehmer bereitgestellten Drittanbieter-Dienst verifizieren: Persona.⁹¹⁰ Er wurde aufgefordert, ein Ausweisdokument hochzuladen und anschließend die Kamera seines Smartphones oder Computers zu aktivieren, um

⁸<https://outlier.ai/legal/privacy-policy>, abgerufen am 20.10.2026..

ein Video von sich selbst aufzunehmen. Die Überprüfung erfolgte anschließend in unregelmäßigen Abständen (**Beilage 5**).

18. Die Datenschutzerklärung der Plattform bestätigt die Erfahrungen des Beschwerdeführers: Die Identitätsüberprüfung erfolgt in Form eines Foto- oder Video-„Selfies“ oder einer Sprachaufzeichnung sowie einer Analyse des Ausweisdokuments des Nutzers. Die Plattform gibt zudem an, diese Daten zu verarbeiten, „um die *Integrität der Dienste zu wahren und Betrug zu bekämpfen*“, indem „Qualifikationen“ überprüft und Gesichtserkennungsdaten generiert werden.¹¹

„(...) wenn Sie sich für die Nutzung dieser Dienste anmelden und im Anschluss daran in regelmäßigen Abständen, können wir Bilder sowie Video- oder Audioaufnahmen, die Sie zeigen – einschließlich Selfies und Bilder Ihres amtlichen Ausweises –, erfassen, speichern und analysieren und diese Bilder und Aufnahmen verwenden, um Ihre Berechtigungen zu überprüfen oder Informationen und Messwerte bezüglich Ihres Gesichts zu generieren („Verifizierungsdaten“), die nach den Gesetzen bestimmter Rechtsordnungen als „biometrische“ oder „sensible“ Daten angesehen werden können“¹² (freie Übersetzung, Hervorhebung hinzugefügt)

19. Persona verarbeitet die an sie übermittelten Daten gemäß ihrer Datenschutzerklärung, auf die die Beschwerdegegnerin verweist. Dieses Dokument beschreibt die Verarbeitung der Daten durch Persona im Rahmen der Erbringung ihrer Dienstleistung. Insbesondere räumt sich Persona das Recht ein, Daten von einer unbegrenzten Anzahl von nicht näher definierten „Dritten“ zu erheben, und gibt lediglich allgemeine Datenkategorien der erhobenen Informationen über eine offene Liste an, die lediglich verschiedene Beispiele „enthält“, wie IP-Adressen, Geräteinformationen, Geolokalisierungsdaten, eindeutige Identifikatoren, Adressdaten, Verbraucherkreditdaten und andere Daten:

„Wir können außerdem die folgenden Informationen von Ihnen, unserem Kunden, oder von Dritten erheben, um die für Ihre Rechtsordnung geeignete Methode zur Identitätsprüfung zu ermitteln und umzusetzen sowie die Einhaltung geltender Gesetze und Verordnungen sicherzustellen:

- **Geräteinformationen**, einschließlich IP-Adresse, Gerätetyp, Betriebssystem Ihres Geräts, Browser, Cookies und Gerätekennungen sowie weitere Software, einschließlich Typ, Version, Sprache, Einstellungen und Konfiguration;
- (...) **öffentlich zugängliche Daten**, einschließlich Daten aus öffentlichen Registern und sozialen Medien;

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

¹⁰<https://outlier.ai/legal/privacy-policy>, abgerufen am 20.10.2026..

¹¹ „Verwenden Sie diese Bilder und Aufzeichnungen, um Ihre Fähigkeiten zu überprüfen oder Informationen und Messwerte zu Ihrem Gesicht zu generieren („Verifizierungsdaten“), die nach den Gesetzen einiger Rechtsordnungen als „biometrische“ Daten oder „sensible“ Daten gelten können.“, <https://outlier.ai/legal/privacy-policy>, abgerufen am 20.10.2026..

¹²<https://outlier.ai/legal/privacy-policy>, abgerufen am 20.10.2026..

- (...) **Zusätzliche Daten zur Altersüberprüfung:** Wir können Ihre personenbezogenen Daten zum Zweck der Altersüberprüfung über unser Netzwerk vertrauenswürdiger Datenquellen von Dritten überprüfen, darunter: öffentlich zugängliche Quellen (wie offene staatliche Datenbanken), nationale und staatliche Identitätsregister, Verbraucherauskünfte, Versorgungsunternehmen, Mobilfunknetzbetreiber und Postadressdatenbanken. Die Arten der „ergänzenden Daten zur Altersüberprüfung“, die wir aus diesen Quellen beziehen, variieren je nach den im jeweiligen Land verfügbaren Überprüfungsmöglichkeiten.“¹³ (freie Übersetzung, Hervorhebung hinzugefügt)

20. Persona setzt derzeit etwa fünfzehn Subunternehmer ein, darunter OpenAI, Groqcloud und Anthropic, für verschiedene Aufgaben der Datenextraktion und -analyse.¹⁴ Die Verarbeitung der Daten erfolgt über eine in den USA ansässige Infrastruktur, darunter Amazon Web Services und Google Cloud.¹⁵

21. Es gab zudem Berichte über fragwürdige Sicherheitspraktiken seitens Persona. So wurden beispielsweise im Oktober 2025 etwa 70.000 bei Persona gespeicherte Fotos von amtlichen Ausweisdokumenten von Hackern gestohlen. Im Februar 2026 stellte sich heraus, dass der Quellcode von Persona öffentlich zugänglich war.¹⁶ Dieser Code enthüllte unter anderem, dass (i) Persona bei jeder „Identitätsüberprüfung“ möglicherweise 269 verschiedene Prüfungen durchführt, darunter Abgleiche zwischen den bereitgestellten Daten und Datenbanken; und (ii) Persona „unerwünschte Medien“ nach 14 Kategorien (einschließlich Terrorismus und Spionage) filtert und Risiko- sowie „Ähnlichkeits“-Werte zuweist.¹⁷

22. Persona hat diese Sicherheitslücken bestätigt.¹⁸ Diese Praktiken haben tatsächlich dazu geführt, dass einer ihrer wichtigsten Kunden, die Plattform Discord, seinen Vertrag mit Persona über die Altersüberprüfung seiner Nutzer gekündigt hat.¹⁹

23. Die Privatsphäre-Erklärung von Persona wurde am 9 April 2026 aktualisiert. Die vorherige Version, die seit der Registrierung des Beschwerdeführers in Kraft war,²⁰ sah die Möglichkeit der Verarbeitung von Ausweisdokumenten zum Zweck der

¹³ <https://withpersona.com/legal/privacy-policy>, abgerufen am 20.10.2026..

¹⁴ <https://withpersona.com/legal/subprocessors>, abgerufen am 20.10.2026..

¹⁵ <https://withpersona.com/legal/subprocessors>, abgerufen am 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, abgerufen am 20.10.2026..

¹⁷ <https://www.malwarebytes.com/blog/news/2026/02/age-verification-vendor-persona-left-frontend-exposed> und <https://vmfunc.re/blog/persona>, abgerufen am 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.

²⁰ Siehe beispielsweise die Fassung vom 12. Januar 2025:

<https://web.archive.org/web/20250112151512/https://withpersona.com/legal/idv-privacy-policy>, abgerufen 20.10.2026..

„Service-Schulung“ über die KI-Systeme des Unternehmens vor (siehe Screenshot unten).²¹

The screenshot shows a privacy policy document with three columns. The first column contains text about service improvement and research, with a red box around it. The second column is titled 'Uploaded Content' and lists 'Geolocation Data', 'Identifiers and Device Information', and 'Usage Data', with a red box around the title. The third column contains text about legitimate interests.

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.
---	--	--

Abbildung 2: Datenschutzerklärung vor dem 9 April 2026

3.4. Traffic-Analyse

24. Am 8. Juli 2026 zeichnete der Beschwerdeführer den Datenverkehr auf der Plattform in Form einer HAR-Datei²² auf, während er sich auf der Plattform befand (**Beilage 6**). Er führte diese Aufzeichnung unter Verwendung der im Anhang beschriebenen Methodik durch (**Beilage 7**).

²¹ Die Datenschutzerklärung von Persona ist unter <https://withpersona.com/legal/idv-privacy-policy> verfügbar. Abgerufen am 20.10.2026..

Die am 9 April 2026 aktualisierte Fassung ist hier verfügbar:

<https://web.archive.org/web/20260422094923/https://withpersona.com/legal/idv-privacy-policy>

Die am 8. Mai 2025 aktualisierte Version, die eine Erklärung zur Nutzung von durch Nutzer hochgeladenen Dokumenten für den Zweck der Schulung durch den Dienst enthält, ist hier verfügbar:

<https://web.archive.org/web/20260326065823/https://withpersona.com/legal/idv-privacy-policy>

²² Eine HAR-Datei (Abkürzung für „*HTTP Archive*“) ist ein vollständiges Protokoll der Interaktionen zwischen einem Browser und Webservern während einer Browsersitzung.

25. Aus den HAR-Dateien geht hervor, dass die Plattform Tracker²³ enthält, die von den folgenden Dritten platziert wurden: Fullstory, Sprig, TikTok, Facebook, Datadog, Segment, Quora, Forethought, Sentry, Twitter Analytics, Google Amplitude.
26. Abbildung 3 zeigt die Anzahl der identifizierten Anfragen für einige dieser Drittanbieter in Beilage 6 .²⁴ Es folgen detailliertere Erläuterungen zu bestimmten Beispielen für Tracker.

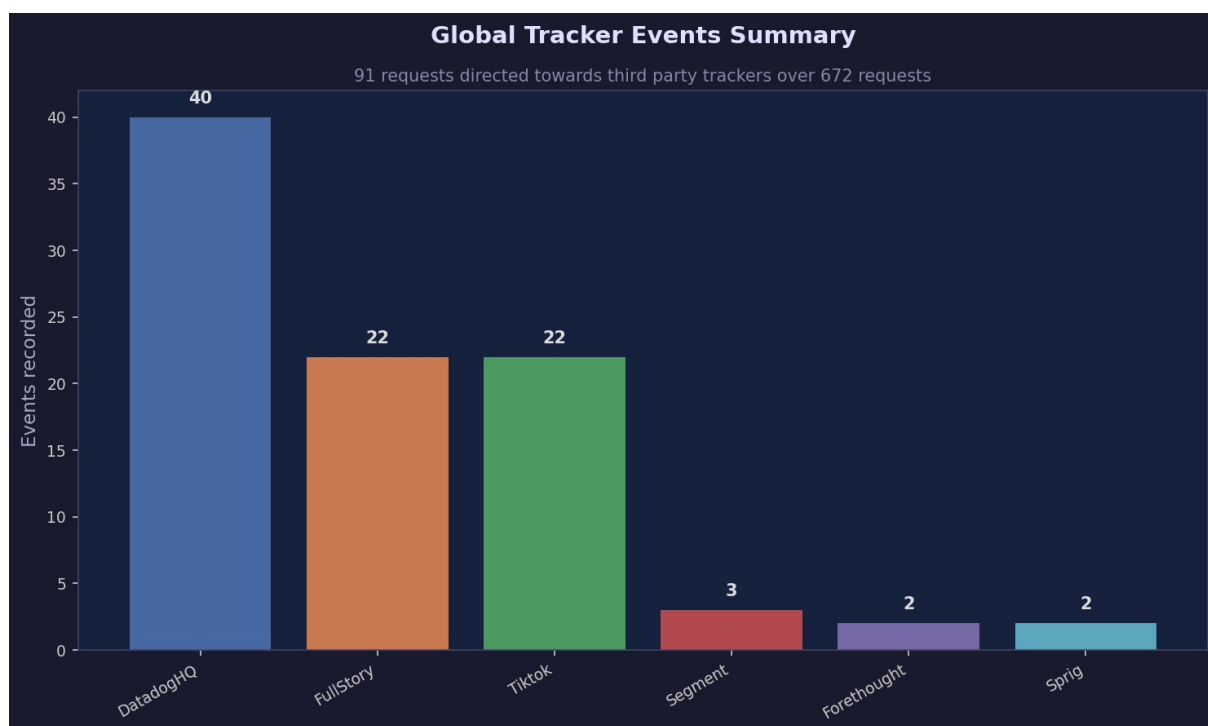


Abbildung 3: Zusammenfassung von Trackern in Beilage 6

Beispiel 1: „Social-Media“-Tracker

27. Die HAR-Dateien zeigen das Vorhandensein von Trackern von Facebook und TikTok. Bei anderen betroffenen Personen waren auch Snapchat und LinkedIn enthalten. Der Twitter-Tracker sendet beispielsweise eine beträchtliche Anzahl von Anfragen. Diese Anfragen werden unter anderem typischerweise für gezielte Werbung genutzt.²⁵

²³ Ein Tracker ist ein – oft unsichtbares – Tool, das Informationen über das Online-Verhalten einer Person sammelt. Es kann die besuchten Websites, die aufgerufenen Seiten, die Verweildauer auf Inhalten, den ungefähren Standort des Nutzers, die Art des verwendeten Geräts und so weiter aufzeichnen. „Ein Tracking-Pixel ist eine alternative Tracking-Methode zu Cookies, die traditionell als 1-Pixel-mal-1-Pixel-Bild implementiert wird, das in die Website eingebettet, für den Nutzer jedoch unsichtbar ist. Das Laden dieses Bildes, dessen Name eine Nutzer-ID enthält, teilt dem Server, auf dem es gehostet wird, mit, dass der verfolgte Nutzer eine Seite besucht oder eine E-Mail gelesen hat.“ Siehe <https://www.cnil.fr/fr/definition/tracking-pixelweb-beacon-ou-pixel-espion>, abgerufen am 20.10.2026..

²⁴ Eine Anfrage ist eine von einem Programm oder Gerät an ein anderes gesendete Abfrage, auf deren Antwort gewartet wird.

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

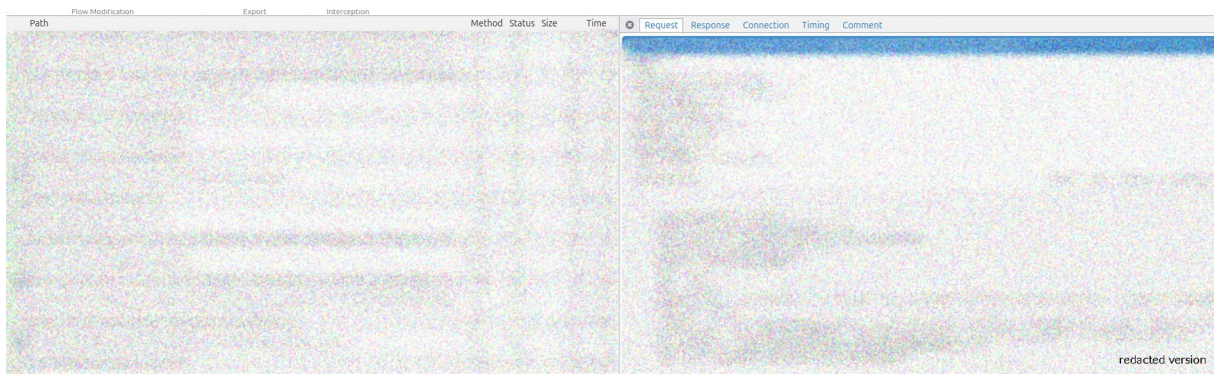


Abbildung 4: Twitter-Tracker

Beispiel 2: Der Forethought-Tracker

28. Forethought Technologies Inc. ist ein US-amerikanisches Unternehmen, das eine KI-Plattform für den Kundensupport anbietet.²⁶ Der in den HAR-Dateien erkannte Forethought-Tracker enthält unter anderem folgende Elemente: eindeutige Kennung („data-ft-corp-user-id“), aufgerufene Seite (hier „earnings“), Nachname, Vorname und E-Mail-Adresse des Beschwerdeführers (**Beilage 6**).

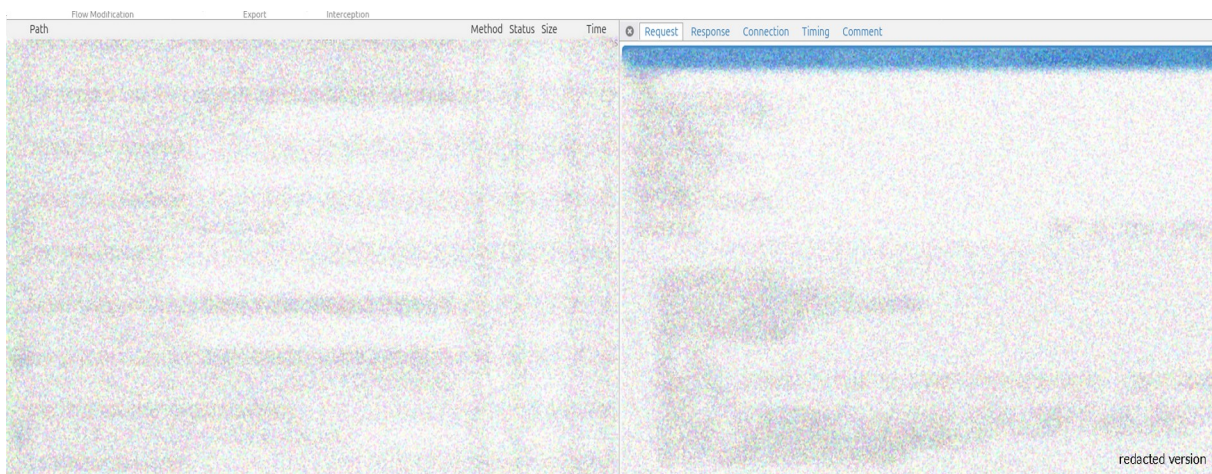


Abbildung 5: Forethought Tracker – Ausschnitt von Beilage 6

²⁶ <https://forethought.ai/>, abgerufen am 20.10.2026..

Weitere Beispiele

29. Fullstory bietet ein Tool zur Sitzungswiedergabe an, das Mausbewegungen, Klicks, Tastenanschläge usw. aufzeichnet.²⁷ In diesem Fall sendet der Fullstory-Tracker alle paar Sekunden eine Anfrage. Er zeichnet bestimmte Ereignisse auf, wie beispielsweise die Seite, die der Beschwerdeführer aufruft (siehe **Beilage 6**).
30. Ein weiterer Tracker wird von Sprig eingesetzt²⁸, das interne Umfrage-Tools bereitstellt, die ein Arbeitgeber bei seinen Mitarbeitern durchführen kann. In diesem Fall nahm der Beschwerdeführer während der Analyse nicht an einer Umfrage teil, doch der Tracker erfasst unter anderem den Nachnamen, den Vornamen, die E-Mail-Adresse und die Telefonnummer des Beschwerdeführers.

3.6. Das Auskunftersuchen

31. Am 22. Dezember 2025 richtete der Beschwerdeführer einen Antrag auf Auskunft an die E-Mail-Adressen privacy@outlier.ai und outlier@lionheartsquared.eu, wie in der Datenschutzerklärung der Plattform angegeben (**Beilage 8**). Einer der Zwecke des Antrags bestand darin, festzustellen, ob im Hinblick auf den Beschwerdeführer eine automatisierte Entscheidung angewendet worden war.
32. Trotz einer Nachfassanfrage am 3. Februar 2026 hat die Beschwerdegegnerin auf diesen Antrag bislang nicht geantwortet.
33. Am 25. Mai 2026 wandte sich der Beschwerdeführer zudem an Persona, um Zugang zu seinen personenbezogenen Daten zu beantragen. Abgesehen von einer Empfangsbestätigung blieb auch dieses Auskunftersuchen unbeantwortet (**Beilage 9**).

4. ZUSTÄNDIGE BEHÖRDE

34. Der Beschwerdeführer lebt und arbeitet in Österreich, während die Beschwerdegegnerin in den Vereinigten Staaten ansässig ist und keinen Hauptgeschäftssitz in der Europäischen Union hat. Der DSB ist daher gemäß Artikel 77 der DSGVO für die Bearbeitung dieser Beschwerde zuständig.

5. RECHTSGRUNDLAGE

5.1. Verstöße

²⁷ Sehen Sie sich die Videopräsentation von „Full Story“ zu ihrer Arbeit an: <https://www.youtube.com/watch?v=Q18TO1ZVz8>, abgerufen am 20.10.2026..

²⁸ <https://sprig.com/>, abgerufen am 20.10.2026..

35. Die zu prüfenden Praktiken lassen sich unterteilen in (1) das Setzen von Trackern; (2) die Verarbeitung von biometrischen Daten; und (3) das Auskunftersuchen. Es liegen jeweils Verstöße vor gegen

(1.a) Artikel 5(1)(c) DSGVO, indem die Daten des Beschwerdeführers verarbeitet und Tracker unter Verstoß gegen den Grundsatz der Datenminimierung platziert wurden;

(1.b) Artikel 5(3) der Richtlinie 2002/58/EG über die Privatsphäre in der elektronischen Kommunikation (ePrivacy), in Österreich umgesetzt durch § 165(3) des Telekommunikationsgesetzes 2021, durch das Setzen von Trackern auf dem Gerät des Beschwerdeführers ohne seine Einwilligung;

(2) Artikel 5(1)(c) in Verbindung mit Artikel 25(1) und Artikel 28(1) DSGVO, indem die biometrischen Daten des Beschwerdeführers unter Verstoß gegen den Grundsatz der Datenminimierung, die Auswahl eines geeigneten Auftragsverarbeiters und den Grundsatz des eingebauten Datenschutzes verarbeitet wurden;

(3) Artikel 15 und Artikel 12(3) DSGVO durch die Nichtbeantwortung des Auskunftersuchens des Beschwerdeführers.

(1.a) Verstoß gegen Artikel 5(1)(c) DSGVO

36. Der Grundsatz der Datenminimierung ist eine Ausprägung des Grundsatzes der Verhältnismäßigkeit, der verlangt, dass jeder Eingriff in ein Grundrecht verhältnismäßig sein muss.²⁹ Insbesondere verlangt Artikel 5(1)(c) DSGVO, dass die verarbeiteten Daten angemessen und relevant sind und auf das für die verfolgten Zwecke unbedingt erforderliche Maß beschränkt bleiben.

37. Im vorliegenden Fall verarbeitet die Beschwerdegegnerin, wie oben beschrieben (§ 13), automatisch erhobene Daten wie die IP-Adresse, die vom Beschwerdeführer vor dem Zugriff auf die Plattform besuchte Website, Informationen zur eindeutigen Identifizierung des Geräts sowie die *oben* (Abschnitt 3.4) erörterten Tracker.

38. Zu den angegebenen Zwecken der Verarbeitung dieser Daten gehören:

- die Bereitstellung, der Betrieb und die Verwaltung der Plattform;
- die Personalisierung des Dienstes;
- die Verbesserung der Produkte und Dienstleistungen der Beschwerdegegnerin; und

²⁹EuGH, *NTH Haustechnik GmbH*, C-484/24, 18. Juni 2026, Abs. 95.

- die Verbesserung der Produkte und Dienstleistungen der Kunden der Beschwerdegegnerin.³⁰

39. Ein weiteres Dokument, die „Cookie-Richtlinie“ der Plattform, verweist ebenfalls auf die Zwecke des Profiling und der gezielten Werbung.³¹
40. Es ist schwer nachvollziehbar, inwiefern die Verarbeitung aller automatisch erhobenen Daten – einschließlich derjenigen, die über die in Abschnitt 3.4 beschriebenen Tracker erfasst werden – für die genannten Zwecke unbedingt erforderlich sein könnte. So ist es beispielsweise für keinen dieser Zwecke offensichtlich notwendig zu wissen, welche Website vor dem Besuch der Plattform aufgerufen wurde, oder die Telefonnummer weiterzugeben.
41. Was die Verbesserung der Produkte und Dienstleistungen der Kunden der Beschwerdegegnerin betrifft – wozu auch das Training ihrer KI-Systeme gehören dürfte –, erscheint es, ganz abgesehen von den ernsthaften Zweifeln an der Rechtmäßigkeit dieses Zwecks, unverhältnismäßig, dass die Daten des Beschwerdeführers, insbesondere diejenigen, die über Tracker, die IP-Adresse oder die vor dem Besuch der Plattform besuchte Website verarbeitet werden, zu diesem Zweck verarbeitet werden sollten.
42. Die Traffic-Analyse hat zudem gezeigt, dass zahlreiche Tracker von Social-Media-Plattformen, Analyseunternehmen und verschiedenen Dienstleistern platziert werden. Wie *oben* beschrieben, werden somit Daten wie die Kontaktdaten des Beschwerdeführers, seine Aktivitäten auf der Plattform, seine Mausbewegungen und eindeutige Identifikatoren verarbeitet. Auch hier ist schwer nachvollziehbar, wie eine derart systematische und ständige Verarbeitung zugunsten so vieler Empfänger für die Verfolgung der angegebenen Zwecke unbedingt erforderlich sein könnte.
43. Im Vergleich mit Social-Media-Plattformen unterscheiden sich die von der Plattform verfolgten Zwecke vollständig von denen der Social-Media-Plattformen. Es ist daher umso schwieriger, den Nutzen des Trackings nachzuweisen, geschweige denn dessen Notwendigkeit.
44. Es ist zudem zu beachten, dass alle diese Zwecke angeblich im berechtigten Interesse der Plattform verfolgt werden. Gemäß Artikel 6(1)(f) DSGVO, wie er vom EuGH und dem EDSA ausgelegt wird, erfordert diese Rechtsgrundlage insbesondere, dass die Daten im Einklang mit dem Grundsatz der Datenminimierung verarbeitet werden,

³⁰<https://outlier.ai/legal/privacy-policy>, abgerufen am 20.10.2026..

³¹<https://outlier.ai/legal/cookies-policy>, abgerufen am 20.10.2026..

um anwendbar zu sein.³² Ein Verstoß gegen den Grundsatz der Datenminimierung macht daher die Rechtsgrundlage des berechtigten Interesses unanwendbar.

45. Um dem Grundsatz der Datenminimierung nachzukommen, hätte die Beschwerdegegnerin beispielsweise zum Zweck der Verbesserung ihrer Produkte und Dienstleistungen nur bestimmte gerätebezogene Daten – wie den verwendeten Browser, die Sprache und die Art des verwendeten Geräts (Mobilgerät oder Computer) – verarbeiten dürfen oder bestimmte Daten nur dann verarbeiten dürfen, wenn bestimmte auslösende Ereignisse eintraten, wie z. B. „Fehler“. Was Tracker betrifft, hätte der Beklagte zudem eine Reihe von Trackern entfernen und/oder die Daten, die über diese verarbeitet werden können, einschränken müssen. Insbesondere im Hinblick auf Session-Replay-Tools hätte der Beklagte, wie von der CNIL in ihrem Entwurf der Empfehlungen zu Session-Replay-Tools³³ empfohlen, das Tool nur gelegentlich und nach dem Zufallsprinzip einsetzen, eine Maskierungs- oder Hash-Technik implementieren oder die Erfassung eindeutiger Identifikatoren vermeiden können. Im vorliegenden Fall wurden jedoch eindeutige Identifikatoren erfasst.
46. Die italienische Behörde hat die Platzierung bestimmter Tracker zu Analysezwecken auf Geräten von Arbeitern geprüft. Diese Tracker ermöglichten, genau wie im vorliegenden Fall, die Verarbeitung von Identifikatoren der Arbeiter, ihrer IP-Adressen, gerätebezogener Daten sowie E-Mail-Adressen und Telefonnummern. Die Behörde stufte diese umfangreiche Verarbeitung und die Weitergabe von Daten an Dritte als Überwachung ein, die gegen den Grundsatz der Datenminimierung verstößt.³⁴
47. Aus dem Vorstehenden folgt daher, dass die Daten des Beschwerdeführers unter Verstoß gegen den Grundsatz der Datenminimierung gemäß Artikel 5(1)(c) DSGVO verarbeitet wurden.

³²EuGH, C-252/21, *Meta gegen Bundeskartellamt*, Abs. 109; C-708/18, *Asociația de Proprietari bloc M5A-ScaraA*, Abs. 48; C-621/22, *Koninklijke Nederlandse Lawn Tennisbond*, Abs. 51–52; EDSA, Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6(1)(f) DSGVO, 8. Oktober 2024, Abs. 29.

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

³⁴Italienische Datenschutzbehörde, Entscheidung 10074601 vom 13. November 2024, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10074601>, Abschnitt 4.11.

(1.b) Verstoß gegen Artikel 5(3) der ePrivacy-Richtlinie und § 165(3) des Telekommunikationsgesetzes 2021

48. Das Platzieren von Pixeln und Trackern stellt eine Speicherung auf dem Gerät des Nutzers dar und fällt daher ebenfalls unter Artikel 5(3) ePrivacy-Richtlinie.³⁵

49. § 165(3) des Telekommunikationsgesetzes 2021 setzt Artikel 5(3) der vorgenannten Richtlinie um und sieht vor, dass

„Betreiber öffentlicher Kommunikationsdienste und Anbieter eines Dienstes der Informationsgesellschaft im Sinne von § 3 Z 1 E-Commerce-Gesetz, BGBl. I Nr. 152/2001, sind verpflichtet, den Nutzer oder Benutzer darüber zu informieren, welche personenbezogenen Daten er verarbeiten wird, auf welcher Rechtsgrundlage und für welche Zwecke dies erfolgt und für wie lange die Daten gespeichert werden. Eine Erhebung dieser Daten ist nur zulässig, wenn der Nutzer oder Benutzer seine Einwilligung dazu aktiv und auf der Grundlage klarer und umfassender Informationen erteilt hat. Dies steht einer technischen Speicherung oder dem Zugriff nicht entgegen, wenn der alleinige Zweck darin besteht, die Übertragung einer Nachricht über ein Kommunikationsnetz durchzuführen, oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Nutzer oder Benutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann. Der Nutzer ist auch über die Nutzungsmöglichkeiten aufgrund der in elektronischen Fassungen der Verzeichnisse eingebetteten Suchfunktionen zu informieren. Diese Information hat in geeigneter Form, insbesondere im Rahmen der Allgemeinen Geschäftsbedingungen und spätestens bei Beginn der Rechtsbeziehungen, zu erfolgen.“

50. Im vorliegenden Fall haben die Verkehrsanalyse und eine Überprüfung der Erklärung zur Privatsphäre (siehe *oben*, Abschnitt 3.1) gezeigt, dass die Beschwerdegegnerin Tracker und Pixel auf dem Endgerät des Beschwerdeführers platziert hat.

51. Die Beschwerdegegnerin beruft sich auf ihr berechtigtes Interesse an der Platzierung dieser Tracker und verstößt damit gegen den oben genannten § 165(3), der die Einwilligung der betroffenen Person vorschreibt.

(2) Verstoß gegen Artikel 5(1)(c) in Verbindung mit Artikel 25(1) und Artikel 28(1) DSGVO

52. Artikel 25(1) DSGVO verpflichtet Verantwortliche, geeignete technische und organisatorische Maßnahmen zu ergreifen, um sicherzustellen, dass Grundsätze wie die Datenminimierung und die Rechtmäßigkeit zum Wohle der betroffenen Personen eingehalten werden.

53. Der EDSA stellt klar, dass Verantwortliche keinen Auftragsverarbeiter auswählen dürfen, dazu beitragen, ihren Verpflichtungen nicht nachzukommen, da sie für die Einhaltung von Artikel 25 DSGVO verantwortlich sind.³⁶ Mit anderen Worten: Zu den

³⁵EDSA, Leitlinien 2023/02 zum technischen Anwendungsbereich von Art. 5 Abs. 3 ePrivacy-Richtlinie, § 50.

³⁶https://www.edsa.europa.eu/sites/default/files/files/file1/edsa_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf, abgerufen am 20.10.2026., §

geeigneten Maßnahmen gehört auch die Auswahl eines geeigneten Auftragsverarbeiters.³⁷

54. Auch verpflichtet Artikel 28(1) der DSGVO die Verantwortlichen dazu, Auftragsverarbeiter auszuwählen, die in der Lage sind, die Einhaltung der DSGVO zu gewährleisten.
55. Diese Maßnahmen sind besonders wichtig, wenn es um die Verarbeitung sensibler Daten gemäß Artikel 9 der DSGVO geht, wie beispielsweise biometrische Daten. In diesem Zusammenhang stellte der EDSA fest, dass die Verarbeitung solcher Daten „an sich“ einen schwerwiegenden Eingriff in die Privatsphäre darstellt.³⁸ Die Maßnahmen können in der Pseudonymisierung bestehen oder darin, dass von Auftragsverarbeitern die Umsetzung bestimmter Verfahren zur Datenminimierung verlangt wird.³⁹
56. Die italienische Aufsichtsbehörde entschied in einem Fall, in dem ein Unternehmen von seinen Plattformarbeitern verlangte, sich durch biometrische Verifizierung zu identifizieren, dass die Verarbeitung solcher Daten für die Erbringung der betreffenden Dienstleistung nicht erforderlich sei.⁴⁰
57. Es ist unstrittig, dass die Beschwerdeführerin die biometrischen Daten des Beschwerdeführers zum Zweck der Identitäts- und Altersüberprüfung verarbeitet. In diesem Abschnitt wird dargelegt, (i) dass die Verarbeitung biometrischer Daten an sich nicht unbedingt erforderlich ist und somit gegen Artikel 5(1)(c) der DSGVO verstößt, und (ii) dass selbst wenn dies der Fall wäre, die an Persona übertragene Verarbeitung dennoch unter Verstoß gegen Artikel 5(1)(c) in Verbindung mit Artikel 25(1) und Artikel 28(1) DSGVO erfolgte.

(i) Die Verarbeitung biometrischer Daten ist nicht erforderlich

58. Die Verarbeitung biometrischer Daten erfolgt hier „zur Wahrung der Integrität der Dienste und zur Betrugsbekämpfung“. ⁴¹ Die vage Formulierung lässt vermuten, dass der Zweck hier darin besteht, sicherzustellen, dass tatsächlich der entsprechende

96.

³⁷ Ebenso: Garante per la protezione dei dati personali, Entscheidung 10074601 vom 13. November 2024, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10074601>, Abschnitt 4.11.

³⁸ Leitlinien 05/2022 zur Nutzung von Gesichtserkennungstechnologie in der Strafverfolgung, 26. April 2023, § 36.

³⁹ https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf, abgerufen am 20.10.2026., § 9.

⁴⁰ Datenschutzbehörde, Entscheidung 10074601 vom 13. November 2024, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10074601>, Abschnitt 4.7.

⁴¹ <https://outlier.ai/legal/privacy-policy>, abgerufen am 20.10.2026.

Arbeiter die Aufgaben ausführt. In dem oben genannten italienischen Fall verfolgte der Verantwortliche einen ähnlichen Zweck und räumte im Verfahren ein, dass die biometrische Überprüfung *an sich* keine ausreichende Maßnahme zur Betrugsbekämpfung darstellt, sondern vielmehr als Abschreckung dient. Die italienische Behörde kam daher zu dem Schluss, dass eine biometrische Überprüfung nicht unbedingt erforderlich war.⁴² Diese Überlegung gilt sinngemäß auch im vorliegenden Fall.

59. Tatsächlich gibt es andere, weniger in die Privatsphäre eingreifende Mittel zur Identitätsprüfung von Arbeitern, um den genannten Zweck zu erreichen. Beispiele hierfür sind die Zwei-Faktor-Authentifizierung (2FA) oder ein physischer Schlüssel, der zum Einloggen eingesteckt werden muss.

(ii) Selbst wenn die Behörde die Verarbeitung für notwendig erachtet hätte, verstößt sie dennoch gegen Artikel 5(1)(c), Artikel 25(1) und Artikel 28(1)

60. Da auf sein Auskunftersuchen keine Antwort erfolgte, kann sich der Beschwerdeführer nur auf die Datenschutzerklärung von Persona stützen, in der, wie oben beschrieben, angegeben ist, dass das Unternehmen Daten zum verwendeten Gerät, zur IP-Adresse und andere Daten verarbeitet und die empfangenen Daten zudem mit Daten aus anderen Datenbanken abgleicht. Dies entspricht einer als „One-to-Many“ bezeichneten Identifizierungstechnik, bei der ein Gesicht mit anderen in einer Datenbank gespeicherten Gesichtern verglichen wird. Die „One-to-Many“-Technik steht im Gegensatz zur „One-to-One“-Verifizierungstechnik, bei der in diesem Zusammenhang ein Gesicht mit einem Ausweisdokument verglichen würde.

61. Die Richtlinie (EU) 2024/2831 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 zur Verbesserung der Arbeitsbedingungen bei plattformgestützter Arbeit – auch wenn sie noch nicht umgesetzt ist – könnte bei der Beurteilung der Rechtmäßigkeit dieser Art der Überprüfung herangezogen werden. In Erwägungsgrund 41 heißt es ausdrücklich, dass, falls biometrische Daten verarbeitet werden müssen, die „One-to-One“-Überprüfungsmethode anzuwenden ist.

62. Im vorliegenden Fall ist die Verarbeitung der genannten Daten im Verhältnis zum beabsichtigten Zweck, nämlich der Identitätsüberprüfung, eindeutig unverhältnismäßig.

63. Um dem Grundsatz der Datenminimierung zu entsprechen, sollte die Überprüfung nach der „One-to-One“-Methode durchgeführt werden, und Persona sollte nicht gestattet werden, andere Daten als die unbedingt erforderlichen zu erheben. Es liegt

⁴²Italienische Datenschutzbehörde, Entscheidung Nr. 10074601 vom 13. November 2024, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10074601>, Abschnitt 4.7.

nämlich in der Verantwortung der Beschwerdegegnerin, einen geeigneten Dienstleister für diese Überprüfung auszuwählen und diesem Dienstleister zu gestatten, nur bestimmte Daten zu erheben.

64. *noyb* ist ein anderer Betroffener bekannt, der den Datenverkehr aufgezeichnet hat, während er seine Identität über Persona verifizieren ließ. Die Analyse hat gezeigt, dass Persona Daten über das benutzte Gerät, die IP-Adresse und weitere Daten verarbeitet hat.
65. Indem die Beschwerdegegnerin vom Beschwerdeführer verlangte, sich einer Verarbeitung seiner biometrischen Daten unterziehen, die gegen den Grundsatz der Datenminimierung verstößt, hat sie nicht nur gegen diesen Grundsatz verstoßen, sondern auch gegen ihre Verpflichtung, geeignete technische und organisatorische Maßnahmen zu ergreifen, wozu auch die Auswahl eines geeigneten Dienstleisters oder Auftragsverarbeiters gehört. Zusammenfassend hat die Beschwerdegegnerin gegen Artikel 5(1)(c), Artikel 25(1) und Artikel 28(1) DSGVO verstoßen.

(3) Verstoß gegen Artikel 15 und Artikel 12(3) DSGVO

66. Artikel 15 DSGVO verpflichtet die Verantwortlichen, den Anträgen der betroffenen Personen auf Auskunft nachzukommen. Artikel 12(3) der DSGVO verlangt eine Antwort so schnell wie möglich, spätestens jedoch einen Monat nach Stellung des Auskunftersuchens.
67. Im vorliegenden Fall hatte der Beschwerdeführer den Verdacht, dass er einer automatisierten Entscheidung unterlag, und hatte die Beschwerdegegnerin ausdrücklich gebeten, ihn darüber zu informieren (**Beilage 8**). Diese Anfrage blieb unbeantwortet. Durch die Nichtbeantwortung des Auskunftersuchens des Beschwerdeführers hat die Beschwerdegegnerin gegen Artikel 15 DSGVO und folglich auch gegen Artikel 12(3) DSGVO verstoßen.

6. ANTRÄGE

6.1. Feststellungsentscheidung

68. Der Beschwerdeführer beantragt, dass die Behörde folgende von der Beschwerdegegnerin begangene Verstöße feststellt:
- einen Verstoß gegen Artikel 5(1)(c) DSGVO durch die Verarbeitung von Daten des Beschwerdeführers, die für die verfolgten Zwecke nicht erforderlich waren;
 - einen Verstoß gegen § 165(3) des Telekommunikationsgesetzes 2021 durch das Setzen von Trackern und Pixeln ohne die Einwilligung des Beschwerdeführers;

- einen Verstoß gegen Artikel 5(1)(c), Artikel 25(1) und Artikel 28(1) DSGVO durch die Beschwerdegegnerin bei der Verarbeitung von biometrischen Daten und durch die Beauftragung eines Auftragsverarbeiters, der (unter anderem) den Grundsatz der Datenminimierung nicht beachtet hat;
- einen Verstoß gegen Artikel 12(3) und Artikel 15 DSGVO durch die Nichtbeantwortung des Auskunftersuchens;

6.2. Auskunft

69. Der Beschwerdeführer beantragt, dass die Behörde die Beschwerdegegnerin anweist, seinem Antrag auf Auskunftserteilung stattzugeben.

6.3. Untersuchung

70. Der Beschwerdeführer beantragt, dass die Behörde die in der Beschwerde dargelegten Verstöße untersucht und ihre Untersuchung auf die Praxis der automatisierten Entscheidung des Beklagten ausweitet.

6.4. Empfehlung zur Verhängung einer Geldbuße

71. Der Beschwerdeführer schlägt vor, dass die Aufsichtsbehörde gemäß Artikel 58(2)(i) sowie Artikel 83(5)(a) und (b) DSGVO wegen der festgestellten Verstöße eine Geldbuße gegen den Verantwortlichen verhängt.

7. KONTAKT

72. Die Kommunikation zwischen *noyb* und der Aufsichtsbehörde im Zusammenhang mit diesem Verfahren kann per E-Mail an [REDACTED] unter Angabe der Fallnummer C109-02 oder telefonisch unter [REDACTED] erfolgen.