



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

Autoriteit Persoonsgegevens
Hoge Nieuwstraat 8
2514 EL Den Haag

Vienna, 27.10.2026

noyb Case No.: C109-05

Complainant:

[REDACTED]
born [REDACTED]
[REDACTED]

Represented under

Article 80(1) of the GDPR by:

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

Respondent:

Scale AI, Inc.,
650 Townsend Street, San Francisco
United States

Re:

**The violation of Articles 5(1)(c), 12(3), 15, 25(1), and
28(1) of the GDPR and Article 11.7a
Telecommunicatiewet**

COMPLAINT

1. REPRESENTATION

1. *noyb* – the European Center for Digital Rights is a nonprofit organization active in the field of protecting the rights and freedoms of data subjects, with its registered office at Goldschlagstraße 172/4/3/2, 1140 Vienna, Austria, ZVR registration number: 1354838270 (hereinafter: “noyb”) (**Appendix 1**).
2. *noyb* represents the complainant pursuant to Article 80(1) GDPR (**Appendix 2**).

2. BACKGROUND

3. Platform work is a form of employment that affects hundreds of millions of people, including at least 43 million in Europe. Their numbers have more than doubled since 2022 and are expected to grow exponentially (hereinafter “Platform Work”).¹
4. Platform Work includes, among others, couriers, so-called “Uberized” drivers, and—a category whose numbers have been growing particularly rapidly recently—data annotators, who work on moderating and training artificial intelligence systems. This last category is the subject of this complaint.
5. Platform Work generally entails a particular vulnerability compared to other jobs. First, workers are often—wrongly—considered self-employed, which excludes them from the social benefits associated with employee status. In addition, more than half of these individuals “*earn less than the net hourly minimum wage in the country where they work.*”²
6. Furthermore, the use of algorithms in platform operations creates and/or exacerbates discrimination. Finally, platforms subject workers to increased digital surveillance.³
7. European lawmakers, well aware of these issues, are currently developing a legal framework to protect these workers.⁴ Supervisory authorities play a key role in investigating the Platforms’ practices and enforcing data subjects rights. The Italian and Dutch authorities have for example recently imposed fines to Glovo and Uber in relation to unlawful automated decision making.⁵

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

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

³See, e.g., https://www.edpb.europa.eu/news/national-news/2021/riders-italian-sa-says-no-algorithms-causing-discrimination-platform-glovo_en, accessed on 20.10.2026; Data Protection Authority, Decision 10074601, dated November 13, 2024, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10074601>.

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

3. FACTS OF THE CASE

3.1. The defendant

8. Scale AI is a company based in San Francisco, United States, which, among other things, acts as the data controller for Outlier, a data annotation platform (hereinafter the “Platform”).⁶
9. Through the Platform, the defendant organizes the work of hundreds of thousands of individuals who annotate data and train AI systems for clients such as Meta, OpenAI, or X.ai.⁷
10. The work is generally carried out according to the following process. A client sends data to the defendant, which (using algorithms) assigns a task related to that data to an individual—for example, sorting or labelling the data according to certain criteria, or responding to prompts to improve large language models (LLMs). The Platform then reviews any errors and assigns the task of correcting them and confirming the quality of the work to another individual.

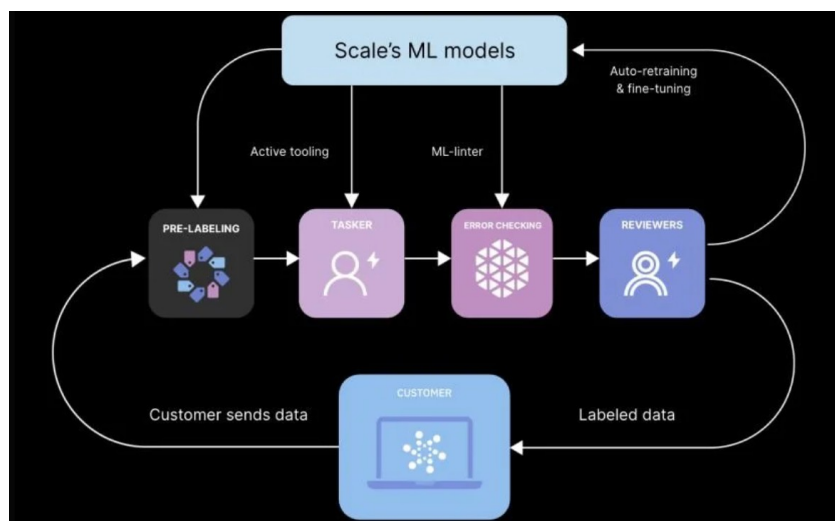


Figure 1: (source: <https://www.leadrpro.com/blog/what-is-scale-ai-a-comprehensive-overview>)

⁵Italian Data Protection Authority, Decision 10074601, dated November 13, 2024, Dutch Data Protection Authority, <https://autoriteitpersoonsgegevens.nl/actueel/uber-krijgt-boete-van-bijna-825-miljoen-euro-voor-geautomatiseerd-blokkeren-van-chauffeurs>, consulted on 20.10.2026.

⁶<https://outlier.ai/legal/privacy-policy>, accessed on 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>, accessed on 20.10.2026.

11. Workers are hired as independent contractors, not as employees. They receive a notification as soon as a task is assigned to them and then have a limited amount of time to complete it; after that, the hourly rate decreases (for information on working conditions within the Platform, see **Appendix 3**).
12. A task may, for example, involve comparing several responses that an LLM might generate in response to a user's query. It may also involve correcting responses provided by an LLM in specific fields of expertise, such as coding, physics, or mathematics.
13. A review of the defendant's privacy notice⁸ shows that it processes a significant amount of data regarding its workers, including a category of data that it collects automatically (the "Automatically Collected Data"). This category includes the unique identifier of the device used, the IP address, information collected via cookies or pixels (not identified in the document), and the website visited prior to accessing the Platform. The defendant processes this data for various purposes, including its "*legitimate interest in operating the platform*" (**Appendix 4**).
14. The defendant also states that it processes Automatically Collected Data for its legitimate interest in developing its services and products, as well as in researching and testing improvements to its clients' services—that is, for training their AI systems.

3.2. The complainant

15. In May 2024, the complainant created an account on the Platform. To do so, he underwent an identity verification process (see Section 3.3). He completed approximately [REDACTED] tasks until May 2026 (**Appendix 5**).
16. Tasks involve for example comparing conversational AI models by rating different responses provided by the LLM to a given "prompt."

3.3. Processing of Biometric Data

17. As noted above, to create his account, the complainant had to verify his identity via a third-party service provided by a subcontractor: Persona.⁹¹⁰ He was asked to upload an ID document, then to activate the camera on his phone or computer to record a video of himself. Verification subsequently took place at irregular intervals (**Appendix 6**).

⁸<https://outlier.ai/legal/privacy-policy>, accessed on 20.10.2026.

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

¹⁰<https://outlier.ai/legal/privacy-policy>, accessed on 20.10.2026.

18. The Platform’s privacy policy confirms the complainant’s experience: identity verification takes the form of a photo or video “selfie” or a voice recording, along with an analysis of the user’s identification document. The Platform also states that it processes this data *“to help preserve the integrity of the Services and combat fraud”* by verifying “qualifications” and generating facial recognition data.

“(…) when you sign up to use the Services, and at regular intervals thereafter, we may collect, store, and analyze images as well as video or audio recordings depicting you—including selfies and images of your official ID—and 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”¹¹ (emphasis added)

19. Persona processes the data transmitted to it in accordance with its privacy policy, to which the defendant refers. This document describes Persona’s processing—when providing its service. Notably, Personal grants itself the right to collect data from an unlimited number of undefined “third parties” and only provides broad categories of collected information via an open list, that only “includes” various examples, such as IP addresses, device information, geolocation data, unique identifiers, address data, consumer credit data, and other data:

“We may also collect the following information from you, our customer, or third parties to determine and provide the appropriate age assurance method for your jurisdiction and to support compliance with applicable laws and regulations:

*- **Device information**, including IP address, device type, your device’s operating system, browser, cookie, and device identifiers, as well as other software, including type, version, language, settings, and configuration;*

*- (...) **Publicly available data**, including data from public records, the public internet and social media;*

*- (...) **Additional Age Assurance data**: We may verify personal data about you for age assurance purposes with our network of trusted third-party data sources, including the following: publicly available sources (such as open government databases), government and national ID registries, consumer credit bureaus, utility companies, mobile network providers and postal address databases. The types of this “Additional Age Assurance Data” we obtain from these sources will vary depending on the verification checks available in the particular country..¹² (emphasis added)*

20. Persona currently uses about fifteen subcontractors, including OpenAI, Groqcloud, and Anthropic, for various data extraction and analysis tasks.¹³ Data processing takes place via U.S.-based infrastructure, including Amazon Web Services and Google Cloud.¹⁴

¹¹<https://outlier.ai/legal/privacy-policy>, accessed on 20.10.2026.

¹²<https://withpersona.com/legal/privacy-policy>, accessed on 20.10.2026.

¹³<https://withpersona.com/legal/subprocessors>, accessed on 20.10.2026.

¹⁴<https://withpersona.com/legal/subprocessors>, accessed on 20.10.2026.

21. There have also been reports of questionable security practices on the part of Persona.¹⁵ For example, in October 2025, approximately 70,000 photos of government-issued IDs stored with Persona were stolen by hackers. In February 2026, Persona's source code was found to be publicly available.¹⁶ This code revealed, among other things, that (i) for each "identity verification," Persona may perform 269 distinct checks, including comparisons between the data provided and databases; and (ii) Persona filters "unfavorable media" according to 14 categories (including terrorism and espionage), and assigns risk and "similarity" scores.¹⁷
22. Persona has confirmed these security vulnerabilities.¹⁸ These practices have, in fact, led one of their major clients, the Discord platform, to terminate its contract with Persona for verifying the ages of its users.¹⁹
23. Persona's privacy policy was updated on April 9, 2026. Its previous version, in effect since the complainant's registration,²⁰ included the possibility of processing identification documents for the purpose of "service training" via its AI systems (see screenshot below).²¹

¹⁵ 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, accessed on 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, accessed on 20.10.2026.

¹⁷ <https://www.malwarebytes.com/blog/news/2026/02/age-verification-vendor-persona-left-frontend-exposed> and <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, accessed on 20.10.2026.

¹⁸ <https://withpersona.com/blog/post-incident-review-source-map-exposure-non-production-subdomain>, accessed on 20.10.2026.

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, accessed on 20.10.2026.

²⁰ See, for example, the version dated January 12, 2025: <https://web.archive.org/web/20250112151512/https://withpersona.com/legal/idv-privacy-policy>, accessed on 20.10.2026.

²¹ Persona's privacy policy is available at <https://withpersona.com/legal/idv-privacy-policy>, accessed on 20.10.2026.

The version updated on April 9, 2026, is available here:

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

The version updated on May 8, 2025, which includes a statement regarding the service's use of documents uploaded by users for training purposes, is available here: <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.
--	--	--

Figure 2: Privacy notice prior to 9 April 2026

3.4. Traffic Analysis

24. On May 22, 2026, the complainant captured traffic on the Platform in the form of a HAR file²² while browsing the Platform (**Appendix 7**). He performed this capture using the methodology described in **appendix 8**.
25. Appendix 7 shows that the Platform includes trackers²³ placed by the following third parties: Fullstory, Sprig, LinkedIn, Posthog, Segment, Run.app, and Google.
26. Another data subject analysed the traffic while verifying their identity with Persona and found that it included trackers from Fullstory, Amplitude, Posthog and Datahog HQ.
27. Figure 3 shows the number of requests identified for some of these third parties in Appendix 7.²⁴ More detailed explanations for certain examples of trackers follow.

²² An HAR file (short for *HTTP Archive*) is a complete log of interactions between a browser and web servers during a browsing session.

²³ A tracker is a tool—often invisible—that collects information about a person’s online behavior. It can record the websites visited, the pages viewed, the time spent on content, the user’s approximate location, the type of device used, and so on. “A tracking pixel is an alternative tracking method to cookies, traditionally implemented as a 1-pixel-by-1-pixel image embedded in the website but invisible to the user. Loading this image, whose name contains a user identifier, informs the server hosting it that the tracked user has visited a page or read an email.” See <https://www.cnil.fr/fr/definition/tracking-pixelweb-beacon-ou-pixel-espion>, accessed on 20.10.2026.

²⁴ A request is a query sent by one program or device to another, awaiting a response in return.

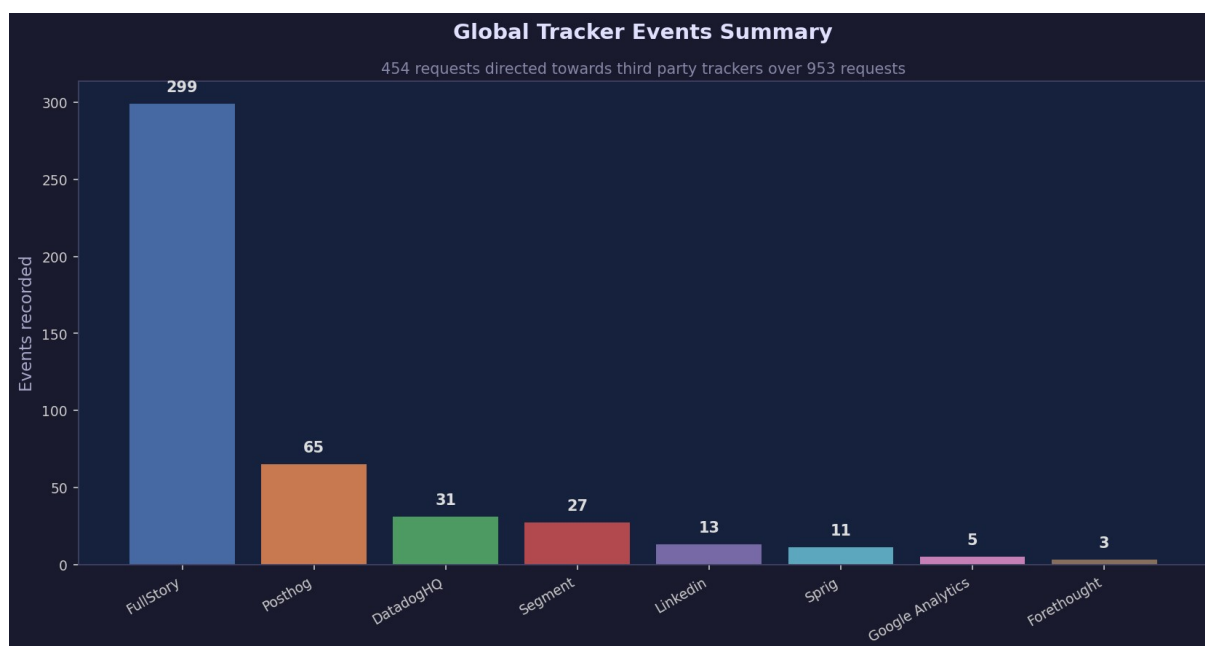


Figure 3: Number of requests in Appendix 7

Example 1: “Social Media” Tracker

28. The HAR file attached as **appendix 7** shows the presence of trackers from LinkedIn in relation to its ads service.

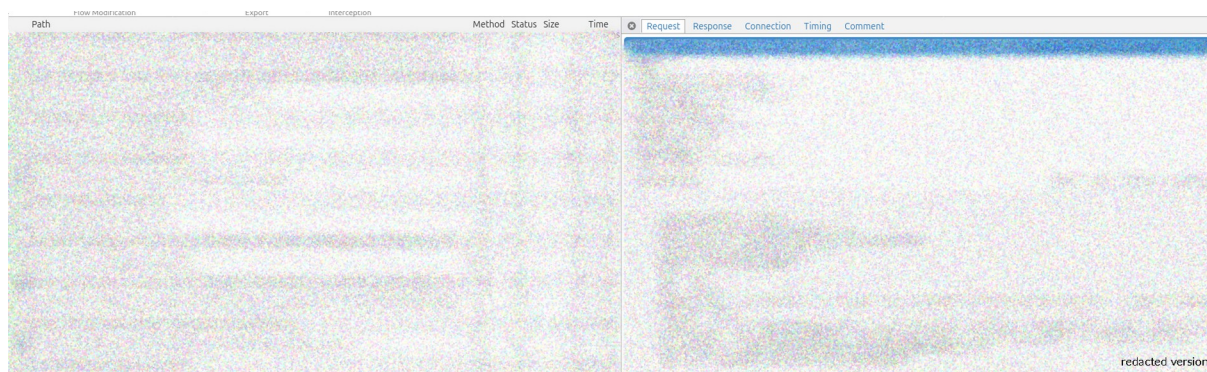


Figure 4 : LinkedIn tracker

Example 2

29. Fullstory offers a session replay tool that records mouse movements, clicks, keystrokes, etc.²⁵ In this case, the Fullstory tracker sends a request every few seconds. It records specific events like the page the complainant is consulting (see **Appendix 7**).

²⁵ Watch Full Story’s video presentation of its work: <https://www.youtube.com/watch?v=Q18TO1lZVz8>, accessed 20.10.2026.

Other examples

30. Another tracker is deployed by Sprig²⁶, which provides internal survey tools that an employer can administer to its workers. In this case, the complainant was not responding to a survey during the analysis but the tracker collects data such as his full name, phone number, email address, unique identifiers, device information, pay information and page visited.

3.5. The Access Request

31. On [REDACTED], the complainant sent a request for access to the email address privacy@outlier.ai, as specified in the Platform's privacy policy (**Appendix 9**). One of the purposes of the request was to determine whether automated decision-making had been applied to her.
32. Despite a follow-up on 28 January 2026, that was also addressed to outlier@lionheartssquared.eu, the defendant has not yet responded to this request.
33. On [REDACTED], the complainant also requested access to his data from Persona, which after confirming receipt of his request, redirected him to Outlier (**Appendix 10**).

4. COMPETENT AUTHORITY

34. The complainant lives and works in the Netherlands, and the Respondent is established in the United States, with no principal place of business in the European Union. The AP therefore has jurisdiction to handle this complaint in accordance with Article 77 of the GDPR.

5. LEGAL BASIS

5.1. Violations

35. The practices under review can be divided into (1) the placement of trackers; (2) the processing of biometric data; and (3) the request for access. They respectively violate
- (1.a) Article 5(1)(c) of the GDPR by processing the complainant's data and placing trackers in violation of the principle of data minimization;
 - (1.b) Article 5(3) of Directive 2002/58/EC on privacy and electronic communications (ePrivacy), transposed in the Netherlands by Article 11.7a

²⁶<https://sprig.com/>, accessed on 20.10.2026.

Telecommunicatiewet, by placing trackers on the complainant's device without consent;

(2) Articles 5(1)(c) *juncto* 25(1) and 28(1) of the GDPR, by processing the complainant's biometric data in violation of the principle of data minimization, the selection of an appropriate processor, and data protection by default;

(3) Articles 15 and 12(3) of the GDPR by failing to respond to the complainant's request for access.

(1.a) Violation of Article 5(1)(c) of the GDPR

36. The principle of data minimization is an application of the principle of proportionality, which requires that any interference with a fundamental right be proportionate.²⁷ In particular, Article 5(1)(c) of the GDPR requires that the data processed be adequate, relevant, and limited to what is strictly necessary for the purposes pursued.

37. In this case, as described above (§13), the defendant processes Automatically Collected Data such as the IP address, the website visited by the Plaintiff prior to accessing the Platform, information that uniquely identifies the device, and the trackers discussed *above* (section 3.4).

38. The stated purposes for processing this data include:

- providing, operating, and administering the Platform;
- personalizing the service;
- improving the defendant's products and services; and
- improving the products and services of the defendant's customers.²⁸

39. Another document, the Platform's "cookies" policy, also refers to the purposes of profiling and targeted advertising.²⁹

40. It is difficult to see how the processing of all Data Collected Automatically—including via the trackers described in Section 3.4—could be strictly necessary for the purposes cited. For example, knowing which website was visited before the Platform or sharing the name of data subjects is clearly not necessary for any of those purposes.

²⁷CJEU, *NTH Haustechnik GmbH*, C-484/24, June 18, 2026, para. 95.

²⁸<https://outlier.ai/legal/privacy-policy>, accessed on 20.10.2026.

²⁹<https://outlier.ai/legal/cookies-policy>, accessed on 20.10.2026.

41. With regard to improving the defendant's clients' products and services — which certainly includes training their AI systems — not to mention the serious doubts regarding the legality of this purpose it appears disproportionate that the complainant's data, particularly that processed through trackers, the IP address, or the website visited prior to the Platform, should be processed for this purpose.
42. Traffic analysis has also shown that numerous trackers are placed by social media platforms, analytics companies, and various service providers. As described *above*, data such as the complainant's contact information, his activity on the Platform, mouse movements, and unique identifiers are thus processed. Once again, it is difficult to see how such systematic and constant processing, for the benefit of so many recipients, could be strictly necessary for the pursuit of the stated purposes.
43. With regard to social media platforms, in particular, the purposes pursued by the Platform are completely distinct from those of social media platforms. It is therefore all the more difficult to establish the usefulness of tracking, let alone its necessity.
44. It should also be noted that all these purposes are stated to be pursued in the Platform's legitimate interest. In accordance with Article 6(1)(f) of the GDPR, as interpreted by the CJEU and the EDPB, this legal basis requires, in particular, that the data be processed in accordance with the principle of data minimization in order to be valid.³⁰ A violation of the principle of data minimization therefore renders the legal basis of legitimate interest invalid.
45. To comply with the principle of data minimization, the defendant could have, for example, for the purpose of improving its products and services, processed only certain device-related data—such as the browser used, the language, and the type of device used (mobile or computer)—or processed certain data only when specific triggering events occurred, such as “bugs”. Regarding trackers, the defendant should also have removed a number of trackers and/or limited the data that can be processed through them. In particular, regarding session replay tools, the defendant could have, as recommended by the CNIL in its draft recommendations on session replay tools³¹, used the tool only occasionally and randomly, implemented a masking or hashing technique, or avoided collecting unique identifiers.

³⁰CJEU, C-252/21, *Meta v. Bundeskartellamt*, para. 109; C-708/18, *Asociația de Proprietari bloc M5A-ScaraA*, para. 48; C-621/22, *Koninklijke Nederlandse Lawn Tennisbond*, paras. 51–52; EDPB, Guidelines 1/2024 on the processing of personal data based on Article 6(1)(f) of the GDPR, October 8, 2024, para. 29.

³¹https://www.cnil.fr/sites/default/files/2026-02/projet_de_recommandation_rejeu_session.pdf, accessed on 20.10.2026.

46. The Italian authority had the opportunity to examine the placement of certain trackers for analytical purposes on workers' devices. These trackers, just as in the present case, enabled the processing of workers' identifiers, their IP addresses, device-related data, and email addresses and phone numbers. The authority characterized this extensive processing and the sharing of data with third parties as surveillance, in violation of the principle of data minimization.³²

47. It therefore follows from the foregoing that the complainant's data was processed in violation of the principle of data minimization under Article 5(1)(c) of the GDPR.

(1.b) Violation of Article 5(3) of the ePrivacy Directive and Article 11.7a Telecommunicatiewet

48. The placement of pixels and trackers constitutes storage on the user's device and is therefore also governed by Article 5(3) of the ePrivacy Directive.³³

49. Article 11.7a Telecommunicatiewet transposes Article 5(3) of the aforementioned directive and provides that

“1 Onverminderd de Algemene verordening gegevensbescherming is het via een elektronisch communicatienetwerk opslaan van of toegang verkrijgen tot informatie in de randapparatuur van een gebruiker, alleen toegestaan op voorwaarde dat de betrokken gebruiker:

a. is voorzien van duidelijke en volledige informatie overeenkomstig de Algemene verordening gegevensbescherming, in ieder geval over de doeleinden waarvoor deze informatie wordt gebruikt, en

b. daarvoor toestemming heeft verleend. (...)”

50. In this case, the traffic analysis and a review of the privacy policy (see *above*, section 3.1) have demonstrated that the defendant placed trackers and pixels on the complainant's terminal.

51. The defendant relies on its legitimate interest to place these trackers, in violation of the aforementioned Article 11.7a, which requires consent from the data subject.

(2) Violation of Articles 5(1)(c) *juncto* Articles 25(1) and 28(1) GDPR

52. Article 25(1) of the GDPR requires data controllers to implement appropriate technical and organizational measures to ensure that principles such as data minimization and lawfulness are respected for the benefit of data subjects.

53. The EDPB specifies that data controllers must not select a processor that does not enable them to comply with their obligations, since they are responsible for

³²Italian Data Protection Authority, Decision 10074601, dated November 13, 2024, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10074601>, section 4.11.

³³EDPB, Guidelines 2023/02 on the Technical Scope of Art. 5(3) of the ePrivacy Directive, §50.

compliance with Article 25 GDPR.³⁴ In other words, appropriate measures include the selection of an appropriate processor.³⁵

54. Similarly, Article 28(1) of the GDPR also requires data controllers to select processors capable of ensuring compliance with the GDPR.

55. These measures are particularly relevant when it comes to the processing of sensitive data under Article 9 of the GDPR, such as biometric data. The EDPB specifies in this regard that the processing of such data constitutes “*in itself*” a serious infringement of privacy.³⁶ The measures may consist of pseudonymization or requiring processors to implement certain data minimization practices.³⁷

56. The Italian supervisory authority ruled, in a case where a company required its platform workers to identify themselves through biometric verification, that the processing of such data was not essential to the provision of the service in question.³⁸

57. It is undisputed that the defendant processes the Plaintiff’s biometric data for the purposes of verifying identity and age. This section demonstrates (i) that the processing of biometric data in and of itself is not strictly necessary, in violation of Article 5(1)(c) of the GDPR, and (ii) that even if it were, the processing as delegated to Persona was nevertheless carried out in violation of Articles 5(1)(c) *juncto* 25(1) and 28(1) of the GDPR.

(i) The processing of biometric data is not necessary

58. The processing of biometric data is carried out here “*to help preserve the integrity of the Services and combat fraud.*”³⁹ The vague wording suggests that the purpose here is to ensure that it is indeed the hired employee who is performing the tasks. In the aforementioned Italian case, the data controller pursued a similar purpose and acknowledged during the proceedings that biometric verification does not *in*

³⁴https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf, accessed on 20.10.2026, §96.

³⁵Similarly, Garante per la protezione dei dati personali, Decision 10074601, dated November 13, 2024, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10074601>, section 4.11.

³⁶Guidelines 05/2022 on the Use of Facial Recognition Technology in Law Enforcement, April 26, 2023, §36.

³⁷https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf, accessed on 20.10.2026, §9.

³⁸Data Protection Authority, Decision 10074601, dated November 13, 2024, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10074601>, section 4.7.

³⁹<https://outlier.ai/legal/privacy-policy>, accessed on 20.10.2026.

itself constitute a sufficient measure to prevent the phenomenon but rather serves as a deterrent. The Italian authority therefore concluded that biometric verification was not strictly necessary.⁴⁰ This consideration applies *mutatis mutandis* in the present case.

59. In fact, to achieve the stated purpose, there are other, less intrusive means of authenticating workers. Examples include two-factor authentication (2FA) or a physical key that must be inserted to log in.

***(ii) Even if the authority considered the processing to be necessary,
it violates Articles 5(1)(c), 25(1), and 28(1)***

60. With no response to her request for access, the complainant can only rely on Persona’s privacy notice which states that Persona compares the data it receives with data from other databases. This corresponds to an identification technique known as “*one-to-many*,” which involves comparing a face with other faces stored in a database. The “*one-to-many*” technique is contrasted with the “*one-to-one*” verification technique, which in this context would involve comparing a face with an identity document.

61. Noyb is also aware of another data subject who recorded the traffic while verifying their identity with Persona. It showed that Persona processes data relating to the device used, the IP address, and other data.

62. Directive (EU) 2024/2831 of the European Parliament and of the Council of October 23, 2024, on improving working conditions in platform-based work—although not yet transposed—may be useful in assessing the legality of this type of verification. Recital 41 expressly states that if biometric data must be processed, the “*one-to-one*” verification method should be used.

63. In this case, the processing of the aforementioned data is clearly excessive in relation to the intended purpose, namely identity verification.

64. To comply with the principle of data minimization, the verification should be conducted using the *one-to-one* method, and Persona should not be permitted to collect any data other than that which is strictly necessary. It is indeed the defendant’s responsibility to select an appropriate service provider for this verification and to allow that provider to collect only certain data.

65. By requiring the complainant to undergo processing of his biometric data in violation of the principle of data minimization, the defendant not only violated this

⁴⁰Italian Data Protection Authority, Decision No. 10074601, dated November 13, 2024, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10074601>, Section 4.7.

principle but also its obligation to implement appropriate technical and organizational measures, which include selecting an appropriate service provider or processor. In conclusion, the defendant has violated Articles 5(1)(c), 25(1), and 28(1) of the GDPR.

(3) Violation of Articles 15 and 12(3) of the GDPR

66. Article 15 of the GDPR requires data controllers to comply with data subjects' requests for access. Article 12(3) of the GDPR requires a response as soon as possible and no later than one month after the request is made.

67. In this case, the complainant suspected that she was subject to automated decision-making and had expressly requested that the Respondent inform her of this (**Appendix 10**). This request went unanswered. By failing to respond to the complainant's request for access, the Respondent violated Article 15 of the GDPR and, consequently, Article 12(3) of the GDPR.

6. CLAIMS

6.1. Declaratory Decision

68. The complainant requests that the authority declare the following violations committed by the Respondent:

- a violation of Article 5(1)(c) of the GDPR by processing the complainant's data that was not necessary for the purposes pursued;
- a violation of Article 11.7a Telecommunicatiewet by placing trackers and pixels without the complainant's consent;
- a violation of Articles 5(1)(c), 25(1), and 28(1) of the GDPR by the defendant in processing biometric data and engaging a processor that did not take into account (among other things) the principle of data minimization;
- a violation of Articles 12(3) and 15 by failing to respond to the request for access.

6.2. Access

69. The complainant requests that the authority order the Respondent to grant him request for access.

6.2. Investigation

70. The complainant requests that the authority investigate the violations set forth in the complaint and expand its investigation to include the Respondent's practice of automated decision-making.

6.3. Recommendation to impose a Fine

71. The complainant suggests that the supervisory authority impose an administrative fine on the data controller, in accordance with Articles 58(2)(i) and 83(5)(a) and (b) of the GDPR, for the violations identified.

7. CONTACT

72. Communications between *noyb* and the supervisory authority in connection with this proceeding may be sent by email to [REDACTED], citing case number C109-05, or by phone at [REDACTED]