

Dutch regulator fines Clearview AI €30.5m and warns firms not to use it

Source copy kept by wheresthe.ai for the story "Dutch regulator fines Clearview AI €30.5m and warns firms not to use it" (<https://wheresthe.ai/d/nl-dpa-clearview-fine-2024-09/>).

Source: <https://www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-on-clearview-because-of-illegal-data-collection-for-facial-recognition>

Text saved 18 Oct 2026 (the page as published).

SHA-256 of the saved text: d55660096de6155c1b526910db8967b4a62e6e83428a6971eb2a682f8dae932a

Documents the source offers: [https://www.autoriteitpersoonsgegevens.nl/en/system/files?file=2024-09/](https://www.autoriteitpersoonsgegevens.nl/en/system/files?file=2024-09/Decision%20fines%20and%20orders%20subject%20to%20a%20penalty%20Clearview.pdf)

[Decision%20fines%20and%20orders%20subject%20to%20a%20penalty%20Clearview.pdf](https://www.autoriteitpersoonsgegevens.nl/en/system/files?file=2024-09/Decision%20fines%20and%20orders%20subject%20to%20a%20penalty%20Clearview.pdf)

Dutch DPA imposes a fine on Clearview because of illegal data collection for facial recognition

03 September 2024

Themes:

Biometrics

Personal data on the Internet

The Dutch Data Protection Authority (Dutch DPA) imposes a fine of 30.5 million euro and orders subject to a penalty for non-compliance up to more than 5 million euro on Clearview AI. Clearview is an American company that offers facial recognition services. Among other things, Clearview has built an illegal database with billions of photos of faces, including of Dutch people. The Dutch DPA warns that using the services of Clearview is also prohibited.

Clearview is a commercial business that offers facial recognition services to intelligence and investigative services. Customers of Clearview can provide camera images to find out the identity of people shown in the images. For this purpose, Clearview has a database with more than 30 billion photos of people. Clearview scrapes these photos automatically from the Internet. And then converts them into a unique biometric code per face. Without these people knowing this and without them having given consent for this. Never anonymous anymore 'Facial recognition is a highly intrusive technology, that you cannot simply unleash on anyone in the world', Dutch DPA chairman Aleid Wolfsen says. 'If there is a photo of you on the Internet – and doesn't that apply to all of us? – then you can end up in the database of Clearview and be tracked. This is not a doom scenario from a scary film. Nor is it something that could only be done in China.' Clearview says that it provides services to intelligence and investigative services outside the European Union (EU) only. 'That is bad enough as it is', Wolfsen says. 'This really shouldn't go any further. We have to draw a very clear line at incorrect use of this sort of technology.' Wolfsen acknowledges the importance of safety and the detection of criminals by official authorities. He also acknowledges that techniques such as facial recognition can make a contribution to this. 'But certainly not by a commercial business. And by competent authorities in highly exceptional cases only. The police, for example, have to manage the software and database themselves in that case, subject to strict conditions and under the watchful eye of the Dutch DPA and other supervisory authorities.' Services of Clearview illegal Wolfsen warns: do not use Clearview. 'Clearview breaks the law, and this makes using the services of Clearview illegal. Dutch organisations that use Clearview may therefore expect hefty fines from the Dutch DPA.' Violations by Clearview Clearview has seriously violated the privacy law General Data Protection Regulation (GDPR) on several points: the company should never have built the database and is insufficiently transparent. Illegal database Clearview should never have built the database with photos, the unique biometric codes and other information linked to them. This especially applies for the codes. Like fingerprints, these are biometric data. Collecting and using them is prohibited. There are some statutory exceptions to this prohibition, but Clearview cannot rely on them. Insufficient transparency Clearview informs the people who are in the database insufficiently about the fact that the company uses their photo and biometric data. People who are in the database also have the right to access their data. This means that Clearview has to show people which data the company has about them, if they ask for this. But Clearview does not cooperate in requests for access. Incremental penalties Clearview did not stop the violations after the investigation by the Dutch DPA. That is why the Dutch DPA has ordered Clearview to stop those violations. If Clearview fails to do this, the company will have to pay penalties for non-compliance in a total

maximum amount of 5.1 million euro on top of the fine. American company Clearview is an American company without an establishment in Europe. Other data protection authorities have already fined Clearview at various earlier occasions, but the company does not seem to adapt its conduct. That is why the Dutch DPA is looking for ways to make sure that Clearview stops the violations. Among other things, by investigating if the directors of the company can be held personally responsible for the violations. Wolfsen: 'Such company cannot continue to violate the rights of Europeans and get away with it. Certainly not in this serious manner and on this massive scale. We are now going to investigate if we can hold the management of the company personally liable and fine them for directing those violations. That liability already exists if directors know that the GDPR is being violated, have the authority to stop that, but omit to do so, and in this way consciously accept those violations.' Clearview has not objected to this decision and is therefore unable to appeal against the fine.

Publications

Decision fine Clearview AI

PDF, 1 MB

This page was last edited on 03 September 2024

.