FAQ – AFIS2026

What is the difference between facial recognition and facial comparison?

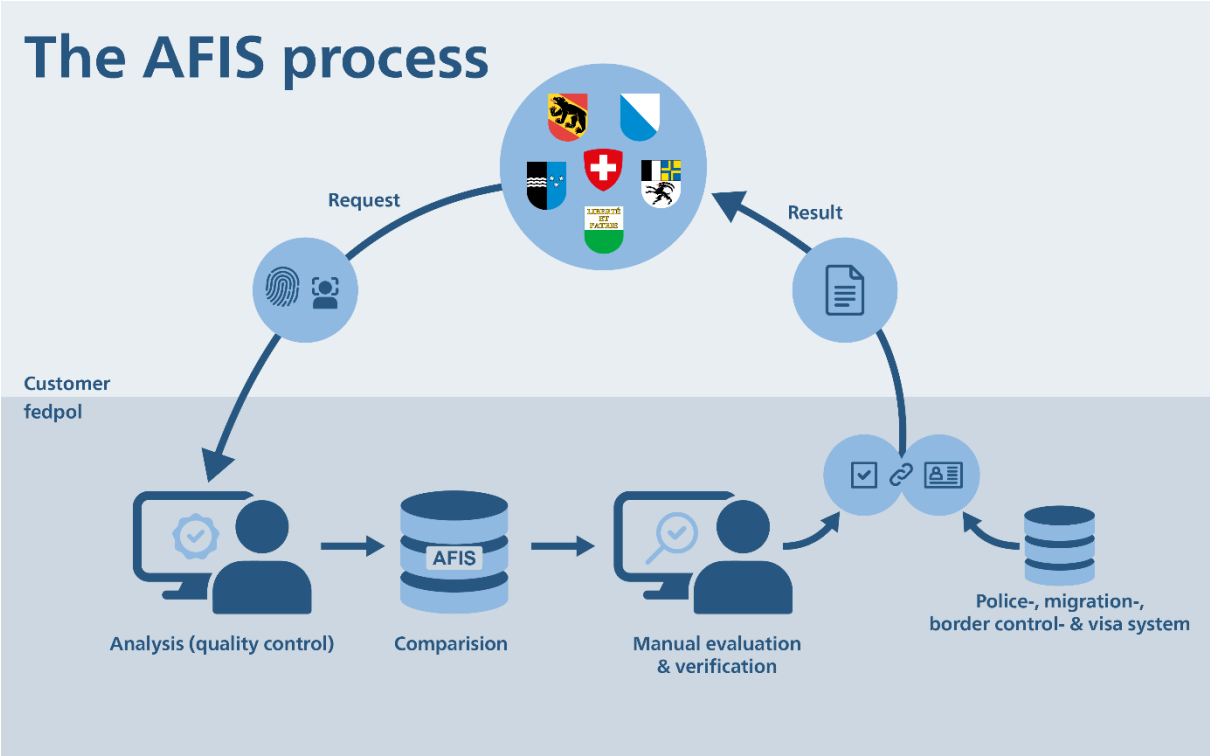
- The difference between facial recognition and facial comparison lies in how the relevant technology is used.
- Facial recognition is the overarching concept, and includes specific practices such as:
    - Real-time monitoring, including live facial recognition (will not be used)
    - Facial comparison (will be used in AFIS2026)

Why won't live facial recognition be used?
Live facial recognition will not be used as part of the AFIS2026 project because there is no legal basis for it, nor are there plans to create such a legal basis for the AFIS.

What is facial comparison?
This system works like fingerprint matching: the facial image of an unknown person is compared with the facial images stored in the AFIS. The recognition process is based on algorithms that have been optimised for this purpose. These algorithms identify possible matching facial images based on biometric characteristics of faces.
In the event of a possible match, an additional manual check by a specialist ensures an even more reliable result. A match is not a positive identification; it is simply a lead to be investigated further.

Where in Europe is this technology being used?
In the EU, facial comparison is becoming an integral part of biometric data processing, along with fingerprints and DNA. Several European countries, including Germany and the Netherlands, have been using facial comparison for many years.
Facial comparison has been used in Germany as an additional tool to support investigations, and has proven useful in solving cases that were unsolved due to a lack of other evidence. This additional source of data for comparison has allowed criminal cases to be solved and unknown people to be identified.

How does the facial comparison process actually work?
- First, the authority submits the facial image to the AFIS system. The image undergoes a quality check.
- The system analyses the image and extracts a set of coordinates from it.
- Based on these coordinates, the system creates a face-specific model, known as a template.
- This template is compared with other templates stored in the AFIS database.
- The system creates a list of potential matches based on a probability value.
- Biometrics specialists verify the suggestions and communicate the results to the authority.



What is the legal basis for using facial comparison in Switzerland?
Article 354 of the Swiss Criminal Code (SCC) forms the legal basis for the AFIS information system and in particular for recording, storing and comparing biometric identification data. According to Article 354 paragraph 1 SCC in conjunction with Article 2 letter c of the Ordinance on the Processing of Biometric Recognition Data, dactyloscopic data and traces (e.g. fingerprints), personal descriptions and, above all, facial images may be compared with each other. The comparison may only be carried out for the purpose of identifying a wanted or unknown person or for identification based on crime scene evidence. fedpol can also process facial images in the AFIS based on Article 14 paragraph 2 of the Federal Act on the Federal Police Information Systems. This option has not yet been used, for technical and financial reasons.

Has the Federal Data Protection Commissioner approved the project?
Switzerland must verify that projects like AFIS2026 meet strict requirements in order to ensure they are in compliance with all the relevant laws. The project's various use cases for facial comparison (person–person, person–evidence, evidence–evidence and evidence–person) were carefully re-examined for their compliance with the law, including the provisions of the new Data Protection Act. The Federal Data Protection Commissioner has approved the AFIS2026 project.

Why does the AFIS system need to be updated?
Introduced in 2016, the current system was designed for a service life of ten years. It will therefore reach the end of its lifespan in 2026, from an operational as well as a contractual perspective.

What would happen without AFIS2026?
The AFIS update is essential for various existing projects which are necessary for good international police cooperation, including the Schengen Information System (SIS), Prüm II, Eurodac III and the Entry/Exit System (EES). Without AFIS2026, these activities would be slowed and possibly pushed back. Furthermore, not being able to use this technology would be a significant setback in the fight against crime and prevent the solving of criminal cases in particular.

When could AFIS2026 be brought into operation?
The new system with the facial comparison component is scheduled to be introduced in the first quarter of 2027. The AFIS2026 project continues the almost 40-year success story of the AFIS and adds facial comparison capabilities. The aim is to develop and update the biometric identification of individuals and evidence in order to combat crime.

Can facial comparison lead to people being wrongly accused?
Facial comparison is an investigative tool – not proof. As with fingerprints, the results are always verified by experts. It is never the system that decides.

What types of offence can facial comparison be used for?
Facial comparison, like the use of fingerprints, is strictly regulated under Swiss law. Under the law, the police, the public prosecutor and the courts can order the taking of identification evidence in cases involving serious crimes such as rape, murder, burglary or kidnapping.

Can this technology be fooled, e.g. by 'face morphing'?
The facial images of known persons stored in the database are created by the authorities. Facial images of unknown persons (facial image evidence) are primarily analysed and shared by forensic services. Morphing attempts are often recognisable in the images' metadata and can be detected by the forensic services. The fact that the AFIS does not contain any public image data, for example from Instagram or Facebook, minimises the risk of morphing being used to deceive the system. Furthermore, the facial image is only ever used as a lead in an investigation, not for positive identification.

Example: When a witness has filmed an offence with their mobile phone or a private surveillance camera has been used, the forensic service must be particularly careful to always check the facial images for any indications of morphing. This is done as part of the manual quality control of facial image evidence before it is submitted to the AFIS.