FAQ – AFIS2026

Wo liegt der Unterschied zwischen Gesichtserkennung («face recognition») und Gesichtsbildabgleich («facial comparison»)?

- Der Unterschied zwischen Gesichtserkennung und Gesichtsbildabgleich liegt in der Anwendung der Technologie.
- Die Gesichtserkennung bezeichnet die Oberkategorie. Unter anderem gehören dazu die Unterkategorien:
  - Echtzeit-Überwachung, auch «Live Scan» (wird nicht angewandt)
  - Gesichtsbildabgleich (wird mit AFIS2026 angewandt)

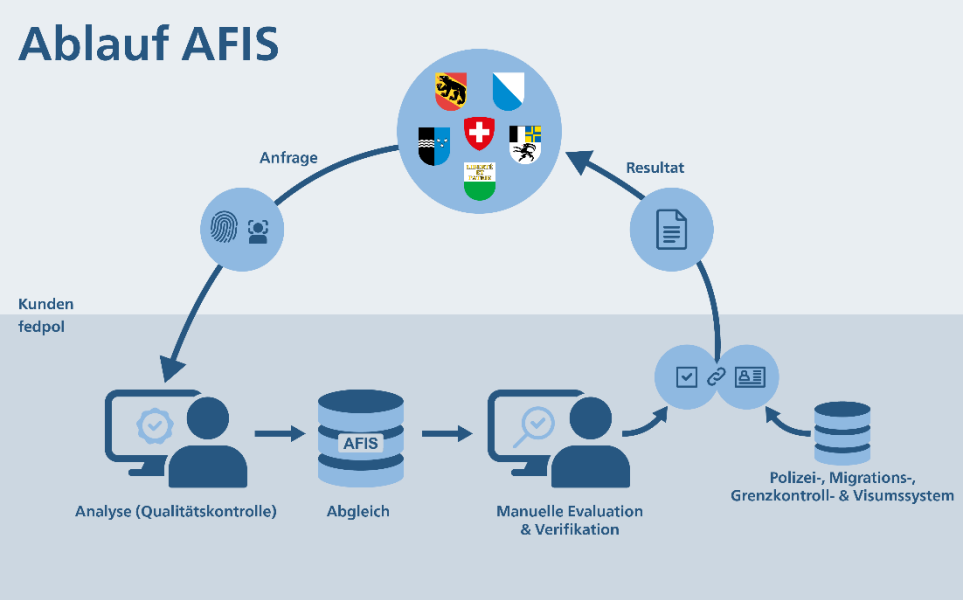
Warum wird der Live Scan nicht verwendet?
Im Rahmen des Projekts AFIS2026 wird die Echtzeit-Gesichtserkennung (Live Scan) auf Basis von Videoüberwachungskameras nicht eingesetzt, da es dafür keine gesetzliche Grundlage gibt. Der Live Scan ist im Projekt AFIS2026 folglich nicht vorgesehen.

Was ist ein Gesichtsbildabgleich?
Das System funktioniert wie beim Fingerabdruckabgleich: Beispielsweise kann in einem Strafverfahren ein Bild einer verdächtigen Person mit im AFIS gespeicherten erkennungsdienstlichen Bildern abgeglichen werden. Die heute verwendeten Erkennungsverfahren stützen sich auf ultramoderne, perfektionierte Algorithmen. Diese filtern – anhand der biometrischen Merkmale (von Gesichtern) und basierend auf dem Grad der Übereinstimmung – unter den gespeicherten Gesichtsbildern die infrage kommenden heraus. Im Falle einer möglichen (vom System ermittelten) Übereinstimmung sorgt eine manuelle Überprüfung durch eine Fachperson für ein noch zuverlässigeres Resultat.

Wer verwendet in Europa diese Technologie?
In der EU wird der Gesichtsbildabgleich zusammen mit Fingerabdrücken und DNA zu einem festen Bestandteil der Bearbeitung biometrischer Daten. Mehrere europäische Länder, darunter Deutschland, Grossbritannien und die Niederlande, haben langjährige Erfahrung mit dem Gesichtsbildabgleich. Wie etwa in Deutschland beobachtet werden konnte, lassen sich mit dem Gesichtsbildabgleich – einem zusätzlichen ermittlungsunterstützenden Instrument – Fälle aufklären, die zuvor aufgrund fehlender Spuren ungelöst blieben. Dank dem, dass zusätzliche Daten abgeglichen werden können, steigt also die Rate der Aufklärung von Straftaten und der Identifikation von Personen.

Wie funktioniert der Gesichtsbildabgleich konkret?

- Das Gesichtsbild trifft im System ein und wird einer Qualitätskontrolle unterzogen.
- Das System analysiert das Bild und extrahiert daraus charakteristische Punkte.
- Aus diesen Punkten erstellt das System ein Modell, eine Struktur (auf Englisch «Template»).
- Dieses Template wird mit den in der Datenbank abgespeicherten Templates verglichen.
- Das System schlägt basierend auf einem Wahrscheinlichkeitswert eine Liste von möglichen Personen vor (Liste potenzieller Matches).
- Diese Vorschläge werden von Sachverständigen verifiziert.



Basierend auf welchen Gesetzesgrundlagen kann in der Schweiz ein Gesichtsbildabgleich durchgeführt werden?
Artikel 354 des Strafgesetzbuches (StGB) bildet die gesetzliche Grundlage für das Informationssystem AFIS und insbesondere die Registratur, die Speicherung und den Abgleich biometrischer erkennungsdienstlicher Daten. Nach Artikel 354 Absatz 1 StGB in Verbindung mit Artikel 2 Buchstabe c der Verordnung über die Bearbeitung biometrischer erkennungsdienstlicher Daten dürfen daktyloskopische Daten und Spuren (z. B. Fingerabdrücke), Signalemente (Personenbeschreibungen) und insbesondere auch Fotografien untereinander abgeglichen werden. Der Abgleich darf allein zum Zweck der Identifizierung einer gesuchten oder unbekannten Person sowie zur Identifikation von Tatortspuren erfolgen. Dass fedpol Fotografien im AFIS bearbeiten kann, ergibt sich zusätzlich aus Artikel 14 Absatz 2 des Bundesgesetzes über die polizeilichen Informationssysteme des Bundes. Von dieser Möglichkeit wurde bislang aus technischen und finanziellen Gründen noch nicht Gebrauch gemacht.

Hat der Eidgenössische Datenschutzbeauftragte das Projekt genehmigt?
Um die hohen Anforderungen unseres Rechtsstaates zu erfüllen, wurden die verschiedenen Anwendungsfälle (Gesichtsbildabgleiche der Kategorien Person–Person, Person–Spur, Spur–Spur und Spur–Person) erneut kritisch auf ihre Gesetzeskonformität geprüft, auch mit Blick auf die Bestimmungen des neuen Datenschutzgesetzes. Der Eidgenössische Datenschutzbeauftragte hat dem Projekt AFIS2026 zugestimmt.

Wieso muss das AFIS erneuert werden?
Das heutige AFIS, das 2016 eingeführt wurde, ist auf eine Betriebsdauer von zehn Jahren ausgelegt. 2026 wird es daher sowohl aus technischer als auch vertraglicher Sicht das Ende seiner Laufzeit erreichen. Mit dem Projekt AFIS2026 soll das bisherige System bis 2026 durch ein neues ersetzt werden. Dabei wird es von den bedeutenden technologischen Fortschritten profitieren, die im Bereich der Methoden zur Identifikation von Finger- und Handflächenabdrücken erzielt wurden.

Was wären die Folgen, wenn AFIS2026 nicht umgesetzt wird?
Die Erneuerung des AFIS ist für verschiedene laufende Projekte und Entwicklungen nötig. Dabei handelt es sich namentlich um das SIS (Schengener Informationssystem), Next Generation Prüm und das EES (Entry/Exit System). Ein Verzicht auf das Projekt AFIS2026 könnte bestimmte grössere Projekte bremsen oder verzögern, die für eine gute Polizeikooperation

nötig sind. Zudem würde es die Bekämpfung der Kriminalität und namentlich die Aufklärung von Kriminalfällen klar behindern, wenn diese Technologie nicht verwendet wird.

Ab wann könnte AFIS2026 in Betrieb genommen werden?
Die Einführung des neuen Systems mit der Komponente für den Gesichtsbildabgleich ist per Ende 2026 geplant. Das Projekt AFIS2026 setzt die fast 40-jährige Erfolgsgeschichte des AFIS fort und ergänzt sie um den Gesichtsbildabgleich. Es geht darum, die biometrische Identifikation von Personen und Spuren zur Kriminalitätsbekämpfung weiterzuentwickeln und auf den neuesten Stand zu bringen – basierend auf bereits bestehenden Gesetzesgrundlagen.

Ist der Gesichtsbildabgleich sicher?
Das System funktioniert wie beim Fingerabdruckabgleich: Beispielsweise kann in einem Strafverfahren ein Bild einer verdächtigen Person mit im AFIS gespeicherten erkennungsdienstlichen Bildern abgeglichen werden. Die heute verwendeten Erkennungsverfahren stützen sich auf ultramoderne, perfektionierte Algorithmen. Diese filtern – anhand der biometrischen Merkmale (von Gesichtern) und basierend auf dem Grad der Übereinstimmung – unter den gespeicherten Gesichtsbildern die infrage kommenden heraus. Im Falle einer möglichen (vom System ermittelten) Übereinstimmung sorgt eine manuelle Überprüfung durch eine Fachperson für ein noch zuverlässigeres Resultat.

Können Personen fälschlicherweise beschuldigt werden?
Der Gesichtsbildabgleich ist ein ermittlungsunterstützendes Instrument – kein Beweis. Wie auch bei den Fingerabdrücken werden die Ergebnisse immer von Fachleuten verifiziert. Es ist nie das System, das entscheidet.

Bei welchen Arten von Delikten wird man den Gesichtsbildabgleich einsetzen dürfen?
Die Verwendung des Gesichtsbildabgleichs ist wie auch die Verwendung von Fingerabdrücken im Schweizer Recht streng geregelt. Für die Spuren gilt Artikel 354 Absatz 1 des Strafgesetzbuchs (StGB; SR 311.0), und nach Artikel 260 der Strafprozessordnung (StPO; SR 312.0) können die Polizei, die Staatsanwaltschaft und die Gerichte die erkennungsdienstliche Erfassung anordnen, beispielsweise bei Vergewaltigung, Mord, Einbruchdiebstahl oder Entführung.

Kann diese Technologie getäuscht werden (zum Beispiel durch «Morphing»)?
Die in der Datenbank erfassten Personenbilder werden von den Behörden erstellt (z. B. Identifikationsfotos oder Frontal- und Profilansichten).
Die Spurenbilder werden in erster Linie vom kriminaltechnischen Dienst analysiert und unterbreitet. Morphing-Versuche sind häufig in den Metadaten der Bilder erkennbar und den kriminaltechnischen Diensten bekannt. Die Tatsache, dass keine öffentlichen Bilddaten, zum Beispiel aus Instagram oder Facebook, im AFIS verwendet werden, minimiert das Risiko von Morphing. Das Bild ist zudem immer nur ein Ermittlungsindiz, keine eindeutige Identifikation.
Beispiel: Insbesondere wenn ein Zeuge eine Tat mit seinem Mobiltelefon filmt oder eine private Überwachungskamera verwendet wurde, muss der kriminaltechnische Dienst die Bilder immer daraufhin überprüfen, ob es Morphing-Versuche gab. Dies ist Teil der manuellen Kontrolle der Qualität der Bilder (Gesichtsspuren) vor deren Speicherung im System.