

SMART GLASS-FLASH

Smart Glasses and Data Eyewear in Switzerland – Current Status and International Developments

A concise overview of what you should know about the debate.

2026 · SMART GLASS-FLASH · APPROX. 10 MIN. READ · DR. IUR. DIRK SPACEK

1. In Brief

- Owning and wearing data glasses with a camera/microphone (“smart glasses”; “Google Glass” used as a generic term) is not, in principle, (yet) prohibited in Switzerland. There is no device-specific regulatory regime.
- Their use, however, quickly runs up against the limits of data protection law (FADP), civil law (protection of personality, Art. 28 CC) and criminal law (Art. 179 et seq. SCC, protecting the secret and private sphere).
- The FDPIC is actively monitoring the topic (see e.g. the 33rd Activity Report 2025/2026) and sees a heightened risk to third parties’ personality rights; political pressure for a ban or usage restrictions is growing at the municipal and cantonal level, as well as through a petition to the Federal Council.
- Internationally, 2026 has brought a noticeable tightening: an EDPB report on the “social acceptability” of smart glasses, warnings from France’s CNIL, a criminal complaint in Germany, a sales ban under discussion in several EU member states, and a statewide courthouse ban together with class actions in the US.

2. What Can Smart Glasses / “Google Glass” Actually Do?

The term “Google Glass” is often used in public debate as a stand-in for the entire category of data glasses, even though Google’s original product (Explorer Edition 2013, most recently Enterprise Edition 2) has not been on the market at all since 2023. In 2026, Google returned to the market with a new generation of data glasses built on the Android XR platform, developed together with partners such as Samsung, Warby Parker, Gentle Monster and Xreal. Data glasses generally contain a built-in camera for taking photos and videos and, in some variants, a visible display (showing notifications, weather data or search results). The Android XR operating system distinguishes three device types: (i) **“AI Glasses” without a Display** – essentially a pair of headphones with a camera, microphone(s) and touch controls on the temple, operated by voice command (“Hey Google”) or a button press, with object recognition, live translation, photo/video capture (limited, depending on the model, to between 30 seconds and 3 minutes) and syncing with a smartphone app; (ii) **“Display AI Glasses”** with an additional micro-display in one or both lenses for notifications, navigation overlays, live captions and text-based AI responses; (iii) wired **“Wired XR Glasses”** with an external battery and a full-area augmented reality display. For all variants, Google mandates two status LEDs (i.e., operating indicators on the device) – one visible to the

wearer and one visible to bystanders, which lights up/blinks when the camera is active. This requirement is often cited in connection with the legal assessment of the “recognisability” of a recording (see item 3). It remains contentious, however, since passers-by can barely see such a blinking light at a normal distance or in bright daylight, and would have few practical means of enforcement against it (they would have to ask people to remove the glasses or hide from them – neither of which is particularly practicable).

Google and Android XR are not alone in this market: Meta currently operates the “Ray-Ban Meta” (Gen 2, no display) and Ray-Ban Meta Display (with colour display and control wristband) models. Samsung is bringing its own Android XR-based glasses to market under the name “Galaxy Glasses”. Numerous other providers exist alongside these, each with a different focus.

To date, biometric facial recognition is (still) neither possible nor permitted on any data glasses model sold on the market (see further below).

3. Switzerland: Data Protection Classification

Photo and video recordings in which people are identifiable generally qualify as personal data within the meaning of the Federal Act on Data Protection (FADP). Anyone who films or photographs using smart glasses thereby becomes a controller within the meaning of the FADP themselves – regardless of whether the recording is made for private or business purposes. Processing is permissible only if it is proportionate, recognisable to the persons concerned (principle of transparency) and legally justified (consent, overriding interest, or a legal basis).

The frequently discussed “personal use” exception (Art. 2 para. 2 lit. a FADP) applies only for as long as the processing genuinely serves purely private or family purposes. If recordings are shared, uploaded to social networks or – as is partly documented among smart glasses manufacturers – transmitted back to cloud services for analysis or AI training purposes, this privilege likely no longer applies and the full FADP compliance package must be observed (see e.g. Rudin Beat, commentary on Art. 2 FADP, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (eds.), *Datenschutzgesetz, Stämpflis Handkommentar (SHK)*, 2nd ed., Bern 2023, Art. 2 N. 14, with the photo album example (“provided the photos are not further distributed”)).

The Federal Data Protection and Information Commissioner (“**FDPIC**”) devotes a dedicated chapter to smart glasses in its 33rd Activity Report 2025/2026 (reporting year April 2025 to March 2026) and has opened a preliminary inquiry into Meta (see www.edoeb.admin.ch/de/taetigkeitsbericht-des-edob). According to the FDPIC, wearers who film people in a recognisable manner must ensure that those affected are informed and give their consent; failure to do so may entail both civil and criminal consequences. In practice this is barely achievable and is presumably not something wearers of smart glasses even consider. For businesses, however, this means specifically that using smart glasses in the workplace or vis-à-vis customers is risky without clear data protection governance.

4. Switzerland: Criminal Law Risks (Art. 179 et seq. SCC) and the Right of Personality (Art. 28 CC)

Title 4 of the SCC (“**Offences Against the Secret or Private Sphere**”, Art. 179–179novies SCC) is of central importance for smart glasses. The key offences:

Provision	Offence	Relevance to Smart Glasses
Art. 179bis	Eavesdropping on/recording another person’s non-public conversation by someone not party to it.	The glasses’ microphone records conversations between third parties that the wearer is not part of.
Art. 179ter	Unauthorised recording of a non-public conversation by a person taking part in it.	Recording one’s own conversations (e.g. a meeting or negotiation) without the consent of all participants.
Art. 179quater	Observing/recording matters from the secret or private sphere using a recording device, without consent.	The key provision for camera glasses: covers recordings in changing rooms, toilets and homes, but also secluded, non-visible areas; no requirement of secrecy.
Art. 179quinquies	List of non-punishable recordings (emergency calls, business orders, etc.)	Narrow exceptions; generally not relevant to everyday use of smart glasses.
Art. 179sexies	Placing on the market/advertising devices specifically designed for unlawful eavesdropping or recording.	According to prevailing legal opinion, scarcely applicable to ordinary smart glasses, since these are not specifically designed for covert surveillance and are (as a regulatory matter) marked with a recording LED.
Art. 179novies	Unauthorised obtaining of sensitive personal data from a data collection that is not publicly accessible.	Potentially relevant in the case of biometric analysis or facial recognition via the glasses (where possible).

In practice, the decisive provision for smart glasses is Art. 179quater SCC: unlike Art. 179bis/179ter, this offence protects not the conversation but the image, and does not require the recording to be covert; what matters alone is that the person concerned is in a situation in which they may legitimately expect not to be observable by the general public (a home, a garden plot, a changing room, but also secluded locations that are nonetheless publicly accessible). Merely filming in public space, by contrast, remains lawful – smart glasses are treated in this respect like any other camera or smartphone. The real additional risk posed by data glasses lies not in the offence itself but in evidentiary terms: because bystanders usually cannot tell whether or when a recording is being made, enforcing the relevant rights in practice becomes more difficult.

In parallel, the **civil-law right of personality** (Art. 28 CC, right to one’s own image) continues to apply and gives rise, independently of criminal law, to claims for injunctive relief, removal and damages, in particular where recordings are published without consent.

4. Regulatory Vacuum and Growing Political Pressure

No device-specific federal statute on smart glasses exists; the general, technology-neutral legal framework applies instead (provisions drawn from the FADP, SCC and CC). Given sharply rising sales figures (Swiss online retailers report a multiple-fold increase for 2026 compared with the previous year), the political debate has, however, gained considerable momentum in recent months:

- **Federal level:** A petition launched in August 2026 (“No Toy for Stalkers”) calls on the Federal Council and the Federal Department of Justice and Police (FDJP) to ban the sale of smart glasses in Switzerland; it gathered several thousand signatures within a few days. A response from the federal government is still pending (watson.ch, “Resistance to Smart Glasses Is Growing – in Switzerland Too”, August 2026. <https://www.watson.ch/wirtschaft/digital/962911430-widerstand-gegen-smart-glasses-waechst-auch-in-der-schweiz>).
- **Municipalities/Cantons:** In Wil SG, a cross-party motion is pending in the municipal parliament that would ban smart glasses at municipal swimming facilities; similar efforts are under way in Lucerne (cantonal parliament) and Basel. The professional association of pool lifeguards has spoken out in favour of a blanket ban with preventive effect (SRF, “Wil SG: Politicians Want to Ban Smart Glasses from Swimming Pools”, 17 August 2026. <https://www.srf.ch/news/schweiz/smart-glasses-in-der-badi-heimliche-aufnahmen-mit-smarten-brillen-kommen-nun-verbote-1>).
- **Supervisory authorities:** The FDPIC is continuously assessing whether the models offered on the market meet FADP requirements and can be used in a data-protection-compliant manner; based on the authorities’ assessment so far, however, an outright ban grounded in current law appears difficult to justify as long as the devices carry a (however discreet) visual recording indicator. The debate remains contentious nonetheless (some consider the recording indicator, and the means of enforcing it, too weak) (SRF, “Smart Glasses with a Camera: Data Protection Risks of AI Glasses Explained”, August 2026. <https://www.srf.ch/news/gesellschaft/digitale-privatsphaere-wie-merke-ich-ob-mich-jemand-mit-smart-glasses-filmt>).

This matters for **businesses** in particular: absent a special federal rule, the **right of domiciliary control (Hausrecht)** remains the most effective tool for prohibiting the wearing or **use of smart glasses on one’s own premises** (reception areas, meeting rooms, workshops, gyms, swimming pools) **altogether** – provided the ban is actively communicated via signage, visitor policies or contractual clauses. The **right of domiciliary control** is **civil-law in nature** and rests on ownership (Art. 641 CC), possession (Art. 919 et seq. CC), or a valid title of use (e.g. a lease or tenancy). It is the power to determine, undisturbed, what happens within a given space and to freely exercise one’s own will there.

5. Overview: Abroad/EU

5.1 EU Level

For users and businesses in the EU, the general GDPR regime applies first and foremost (legal basis under Art. 6 GDPR, heightened requirements under Art. 9 GDPR for biometric analysis, potentially an obligation to carry out a data protection impact assessment). In 2026, the European Data Protection Board (EDPB) commissioned its own study on the “social acceptability” of smart glasses, the results of which were announced for summer 2026. In addition, since 2 August 2026 the ban on certain biometric practices under Art. 5 of the EU AI Act (including real-time remote identification in public spaces and biometric categorisation) has been fully applicable and is potentially relevant to devices with a facial recognition function. In the European Parliament, the

liberal “Renew Europe” group is calling on the Commission to clarify how the GDPR and the AI Act are to be applied to AI-powered data glasses (see e.g. GDPR Local, “Smart Glasses and GDPR: Why Europe Is Cracking Down on Camera-Equipped Eyewear”, 10 June 2026. <https://gdprlocal.com/smart-glasses-and-gdpr/>).

5.2 France

France’s data protection authority, the CNIL, warned as early as May 2026 of a “significant risk” of near-invisible, pervasive surveillance through smart glasses, and called on manufacturers to ensure transparency, purpose limitation and data minimisation, and on users to exercise consideration (informing third parties, switching the device off when not needed). France is among the states reportedly considering a sales ban, according to press reports (PetaPixel, “Meta Smart Glasses Face Calls for Bans Across Europe Over Privacy Concerns”, 4 August 2026. <https://petapixel.com/2026/08/04/meta-smart-glasses-face-calls-for-bans-across-europe-over-privacy-concerns/>).

5.3 Germany

The NGO HateAid filed a criminal complaint against Meta, Ray-Ban, Oakley and various retailers in August 2026 with the German Central Office for Combating Internet Crime, and is demanding a sales ban; the legal grounds cited include the Telecommunications-Digital-Services-Data-Protection Act and § 201a of the German Criminal Code (violation of the intimate personal sphere through image recordings). Germany also has stricter rules than many other EU states on photographing individuals in public spaces, which tends to sharpen the legal starting position there (Euronews, “Meta Smart Glasses Ban Ignores Europe’s Wider Surveillance Threat”, 21 August 2026. <https://www.euronews.com/next/2026/08/21/ban-metas-smart-raise-surveillance-fears-across-europe>).

5.4 United States

In the United States, developments are concentrated along three lines: (i) class actions against Meta over misleading privacy claims, after it emerged that recordings – some from intimate situations – had been reviewed by external service providers for training purposes; (ii) state-level biometric privacy statutes, foremost among them the Illinois Biometric Information Privacy Act (BIPA), which could apply once facial recognition features are activated; (iii) institutional usage bans: the State of New York has, since 20 July 2026, banned smart glasses statewide in all 1,240 courts (the first blanket ban at state level), after individual courts in Pennsylvania, Wisconsin and Hawaii had already issued isolated bans (MEXC News, “Meta AI Smart Glasses Lawsuit Alleges Deceptive Privacy Claims”, 2026. <https://www.mexc.com/it-IT/news/862200>).

6. Biometric Facial Recognition with Smart Glasses

6.1 State of the Art and Manufacturers’ Positions

Current smart glasses have no facial recognition activated as shipped; neither Google (Android XR) nor Meta (Ray-Ban Meta) has enabled such a feature – Meta discontinued its earlier system with such recognition mechanisms in 2021 following settlements (see all-ai.de, “Meta Plans Facial Recognition for Ray-Ban Smartglasses in Everyday Use”, 13 February 2026. <https://www.all-ai.de/news/beitrag2026/zuckerberg-meta-gesichtserkennung>). However, largely finished but disabled code for a feature called “NameTag” has already been found in the Meta app (see heise online, “Ray-Ban Meta: Companion App Contains Code for Facial Recognition”, 5 June 2026. <https://www.heise.de/news/Ray-Ban-Meta-Begleit-App-enthaelt-Code-fuer-Gesichtserkennung-11316322.html>). In 2024, a research project called “I-XRAY” by two Harvard students showed that off-the-shelf Ray-Ban Meta glasses could be paired with the “PimEyes” service to

create a working real-time tool (404 Media, “Someone Put Facial Recognition Tech onto Meta’s Smart Glasses to Instantly Dox Strangers”, 4 October 2024. <https://www.404media.co/someone-put-facial-recognition-tech-onto-metas-smart-glasses-to-instantly-dox-strangers/>).

6.2 EU: Prohibition under Art. 5 of the AI Act

At EU level, real-time remote biometric identification in publicly accessible spaces is, in principle, prohibited under Art. 5 para. 1 lit. h of the AI Act (since 2 February 2025). A narrowly defined, authorisation-dependent exception exists only for law enforcement authorities, for three purposes (searching for victims/missing persons, averting an acute danger, and tracking down suspects of serious crimes). No exception exists for private parties – commercial or private real-time facial recognition is prohibited without exception. Separately, Art. 5 para. 1 lit. e of the AI Act prohibits the untargeted scraping of facial images (the automated collection of photos from the internet for data-analysis or training purposes) to build up recognition databases – the business model of services such as Clearview AI or PimEyes.

6.3 Switzerland: Basis for a Possible Prohibition

Switzerland has no equivalent to the AI Act. At present, the unlawfulness of biometrics in commercially available data glasses arises chiefly from the FADP: since the revision (1 September 2023), identifying biometric data has counted as sensitive personal data (Art. 5 lit. c no. 3 FADP). Storing and processing such data by an unlimited number of data-glasses wearers, without specifically determined purposes of use, would scarcely be proportionate within the meaning of the FADP, and would also lack safeguards against the unlawful disclosure or use of such sensitive personal data. In addition, Art. 179novies SCC applies, which criminalises the unauthorised obtaining of sensitive personal data from a data collection that is not publicly accessible, as does the general right of personality (Art. 28 CC). For use by authorities, including the police, the strict principle of legality also applies (Art. 34 para. 2 FADP), requiring a clear legal basis. This was lacking, for example, in the unlawful 2021 trial use of Clearview by the Zurich city police (see Der Bund / Tages-Anzeiger, “Surveillance Technology in Switzerland: The Police Too Must Abide by the Law”, 6 September 2021. <https://www.derbund.ch/auch-die-polizei-muss-sich-an-das-gesetz-halten-616804935004>). A blanket deployment at public demonstrations would presumably require an explicit legal basis, which is generally lacking.

6.4 Police, Intelligence Services and Demonstrations

Police forces and intelligence services are not categorically exempt from the EU AI Act’s prohibition. Deployment at demonstrations without a concrete danger would presumably remain unlawful. Internationally, however, an expansion is nonetheless apparent: US ICE personnel are reported to already be using privately owned Ray-Ban Meta glasses to film demonstrators, while the Department of Homeland Security is having its own “ICE Glasses” with facial recognition developed (see Telepolis, “ICE Glasses: US Homeland Security Wants to Monitor Citizens with Data Glasses”, 22 April 2026. https://www.telepolis.de/article/ICE-Glasses-US-Heimatschutz-will-Buerger-mit-Daten-brillen-ueberwachen_11267620.html). Since 2026, China has been deploying police smart glasses with facial recognition on a nationwide scale. In the EU/Switzerland this would remain unlawful (Blogspan, “China’s Police Smart Glasses: 95 Percent Facial Recognition – and a System That Thinks Bigger”, 31 May 2026. <https://www.blogspan.net/china-polizei-smartglasses-gesichtserkennung/>). Yet, as the discussion above shows, the technical barrier to an unlawful deployment is low.

6.5 Permissibility Within a Company

Within a company, the same standards apply as for conventional biometric access control systems: the FDPIC requires a justifying ground (consent usually does not suffice in an employment relationship), proportionality, an alternative for employees, and strict compliance with purpose

limitation regarding the data collected in this way (see, in detail, the FDPIC's official guide on biometric recognition systems). Unlike a stationary access reader, however, smart-glasses-based recognition potentially captures everyone it encounters continuously and imperceptibly, which regularly calls proportionality into question and is unlikely to withstand scrutiny under the labour-law prohibition on covert behavioural monitoring (Art. 26 of Ordinance 3 to the Employment Act, ArGV 3) without further ado.

7. Key Takeaways and Recommendations

From a Swiss perspective, there is as yet no approval or sales ban for smart glasses. Rather, risks materialise through the existing framework of data protection, criminal and civil law as soon as people are recognisably filmed or conversations are recorded. Given the political momentum (the petition to the Federal Council, municipal and cantonal motions, the FDPIC's focus), selective regulation is nonetheless likely to be expected in the medium term – whether at the level of an ordinance or at the municipal level (for example, swimming-facility regulations).

- Businesses with public-facing premises should **actively make use of their right of domiciliary control** and communicate usage restrictions clearly.
- For **in-house use** of smart glasses (e.g. for maintenance, logistics, training), a **documented balancing of interests or a data protection impact assessment** within the meaning of the law (Art. 22 FADP) is advisable, along with clear internal instructions on recording, storing and deleting data collected via smart glasses.
- **Employees and customers** must be **informed** of such use. Where legally required, consent must be obtained in advance.
- Developments **at EU level** (the EDPB report, application of the AI Act) should be continuously **monitored**, as they can, in practice, also serve as a point of reference for Swiss practice.
- The use of **biometric facial recognition** for private purposes is **technically** disabled at present on data glasses currently in circulation **as shipped**, and prohibited by law in the EU (except for narrowly defined exceptions in the context of criminal investigation or prosecution). In Switzerland this is not literally prohibited, but is scarcely justifiable under the laws currently in force. It is best left switched off. Abroad (e.g. in the US), this technology is being used more freely by authorities, and in China it has been deployed nationwide by the police since 2026.

This short publication is for general information purposes only and does not replace legal advice in an individual case.

Dirk Spacek, Dr. iur., LL.M. is an attorney and partner in Zurich. He advises companies on all contract and commercial law matters, with a particular focus on issues at the intersection of technology, intellectual property and data/cyber law.