

SMART GLASS-FLASH

Smart Glasses und Datenbrillen in der Schweiz – aktueller Stand und internationale Entwicklungen

Was man kurz und bündig über die Debatte wissen sollte.

2026 · SMART GLASS-FLASH · CA. 10 MIN. LESEZEIT · DR. IUR. DIRK SPACEK

1. Kurz und bündig

- Der Besitz und das Tragen von Datenbrillen mit Kamera/Mikrofon („Smart Glasses“; „Google Glass“ als Gattungsbegriff) ist in der Schweiz grundsätzlich (noch) nicht verboten. Es gibt kein gerätespezifisches Regulierungsregime.
- Die Nutzung stösst jedoch rasch an Grenzen des Datenschutzrechts (DSG), des Zivilrechts (Persönlichkeitsschutz, Art. 28 ZGB) und des Strafrechts (Art. 179 ff. StGB zum Schutz des Geheim- und Privatbereichs).
- Der EDÖB beobachtet das Thema aktiv (siehe z.B. 33. Tätigkeitsbericht 2025/2026) und sieht ein erhöhtes Risiko für Persönlichkeitsrechte Dritter; auf Gemeinde- und Kantonsebene sowie mit einer Petition an den Bundesrat wächst der politische Druck auf ein Verbot bzw. auf Nutzungseinschränkungen.
- International zeichnet sich 2026 eine spürbare Verschärfung ab: EDPB-Bericht zur „sozialen Akzeptanz“ von Smart Glasses, Warnungen der CNIL (Frankreich), eine Strafanzeige in Deutschland, ein Verkaufsverbot in Diskussion in mehreren EU-Staaten sowie ein landesweites Gerichtsverbot und Sammelklagen in den USA.

2. Was können Smart Glasses / «Google Glass» überhaupt?

Der Begriff «Google Glass» wird in der öffentlichen Debatte oft stellvertretend für die gesamte Gerätekategorie von Datenbrillen verwendet, obschon das ursprüngliche Produkt von Google (Explorer Edition 2013, zuletzt Enterprise Edition 2) seit 2023 gar nicht mehr im Handel ist. Google kehrte 2026 mit einer neuen, auf der Plattform Android XR basierenden Datenbrillengeneration in den Markt zurück, entwickelt zusammen mit Partnern wie Samsung, Warby Parker, Gentle Monster und Xreal. Datenbrillen enthalten i.d.R. eine integrierte Kamera, um Fotos und Videos aufnehmen und in gewissen Varianten ein visibles Display (mit Benachrichtigungen, Wetterdaten oder Suchergebnissen). Das Betriebssystem Android XR unterscheidet drei Gerätetypen: (i) «**AI Glasses**» **ohne Display** – im Kern ein Kopfhörer mit Kamera, Mikrofon(en) und Touch-Bedienung am Brillenbügel, gesteuert per Sprachbefehl («Hey Google») oder Tastendruck, mit Objekterkennung, Live-Übersetzung, Bild-/Videoaufnahme (je nach Modell auf 30 Sekunden bis 3 Minuten begrenzt) und Synchronisation mit einer Smartphone-App; (ii) «**Display AI Glasses**» mit einem zusätzlichen Mikro-Display in einem oder beiden Brillengläsern für Benachrichtigungen, Navigations-Overlays, Live-Untertitel und textuelle KI-Antworten; (iii) kabelgebundene «**Wired XR Glasses**» mit externem Akku und einem vollflächigem Augmented Reality-Display. Für alle Varianten schreibt Google verbindlich zwei Status-LEDs (d.h. Betriebsanzeigen des Geräts) vor – eine für die tragende Person und eine für Aussenstehende sichtbare, die bei aktiver Kameranutzung aufleuchtet/blinkt. Diese Vorgabe wird

für die rechtliche Einordnung der «Erkennbarkeit» einer Aufnahme (vgl. Ziff. 3) oft thematisiert. Sie bleibt aber umstritten, weil Passanten solches Blinken auf normale Distanz und auch beim Blenden von Tageslicht kaum sehen und wenig praktische Durchsetzungsmöglichkeiten dagegen hätten (sie müssten Leute auffordern, die Brille auszuziehen oder sich von ihnen verstecken – beides wäre nicht gut praktikabel).

Google bzw. Android XR sind auf diesem Markt nicht allein: Aktuell betreibt Meta mit den Modellen «Ray-Ban Meta» (Gen 2, ohne Display) und Ray-Ban Meta Display (mit Farbdisplay und Steuerarmband). Samsung bringt mit den «Galaxy Glasses» eine eigene, ebenfalls auf Android XR basierende Brille. Daneben existieren zahlreiche weitere Anbieter mit unterschiedlichen Schwerpunkten.

Biometrische Gesichtserkennung ist per dato auf allen im Markt vertriebenen Datenbrillen-Modellen (noch) nicht möglich bzw. nicht gestattet (siehe dazu weiter hinten).

3. Schweiz: Datenschutzrechtliche Einordnung

Bild- und Videoaufnahmen, auf denen Personen erkennbar sind, gelten grundsätzlich als Personendaten im Sinne des Datenschutzgesetzes (DSG). Wer mit Smart Glasses filmt oder fotografiert, wird damit selbst zur verantwortlichen Person im Sinne des DSG – unabhängig davon, ob die Aufnahme nun zu privaten oder geschäftlichen Zwecken erfolgt. Eine Bearbeitung ist nur zulässig, wenn sie verhältnismässig ist, für die betroffenen Personen erkennbar (Transparenzgrundsatz) und rechtlich gerechtfertigt ist (Einwilligung, überwiegendes Interesse oder gesetzliche Grundlage).

Die vielfach diskutierte «private Tätigkeit»-Ausnahme (Art. 2 Abs. 2 lit. a DSG) greift nur, solange die Bearbeitung tatsächlich rein privaten/familiären Zwecken dient. Werden Aufnahmen jedoch geteilt, in soziale Netzwerke hochgeladen oder – wie bei Smart-Glasses-Herstellern teils dokumentiert – an Cloud-Dienste zur Auswertung oder zum KI-Training zurückübermittelt, dürfte diese Privilegierung entfallen und das volle DSG-Compliance-Paket ist einzuhalten (siehe z.B. dazu Rudin Beat, Kommentierung zu Art. 2 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar (SHK), 2. Auflage, Bern 2023 Art. 2 N. 14 mit dem Fotoalbum-Beispiel («sofern die Fotos nicht weiterverbreitet werden»)).

Der Eidgenössische Datenschutzbeauftragte («EDÖB») widmet Smart Glasses im 33. Tätigkeitsbericht 2025/2026 (Berichtsjahr April 2025 bis März 2026) ein eigenes Kapitel und ordnet eine Vorabklärung gegenüber Meta ein (siehe dazu www.edoeb.admin.ch/de/taetigkeitsbericht-des-edob). Gemäss EDÖB müssen Trägerinnen und Träger, die Personen erkennbar filmen, sicherstellen, dass die betroffenen Personen informiert sind und einwilligen; eine Missachtung könne zivil- wie strafrechtliche Folgen nach sich ziehen. Praktisch ist das kaum umsetzbar und wohl von den Trägern der Smart Glasses auch nicht angedacht. Für Unternehmen bedeutet dies aber konkret: Der Einsatz von Smart Glasses am Arbeitsplatz oder gegenüber der Kundschaft ist ohne klare Datenschutz-Governance riskant.

4. Schweiz: Strafrechtliche Risiken (Art. 179 ff. StGB) und Persönlichkeitsrecht (Art. 28 ZGB)

Der 4. Titel des StGB («**Strafbare Handlungen gegen den Geheim- oder Privatbereich**», Art. 179–179novies StGB) ist für Smart Glasses von zentraler Bedeutung. Die wichtigsten Tatbestände:

Norm	Tatbestand	Relevanz für Smart Glasses
Art. 179bis	Abhören/Aufnehmen eines fremden, nichtöffentlichen Gesprächs durch Nicht-Teilnehmende.	Mikrofon der Brille zeichnet Gespräche Dritter auf, an denen die tragende Person nicht beteiligt ist.
Art. 179ter	Unbefugtes Aufnehmen eines nichtöffentlichen Gesprächs durch eine daran beteiligte Person.	Mitschnitt eigener Gespräche (z.B. Meeting, Verhandlung) ohne Einwilligung aller Beteiligten.
Art. 179quater	Beobachten/Aufnehmen von Tatsachen aus dem Geheim- oder Privatbereich mit einem Aufnahmegerät, ohne Einwilligung.	Kernnorm für Kamerabrillen: erfasst Aufnahmen in Garde-roben, Toiletten, Wohnungen, aber auch verdeckten, nicht einsehbaren Bereichen; kein Erfordernis der Heimlichkeit.
Art. 179quinquies	Katalog nicht strafbarer Aufnahmen (Notrufe, Geschäftsbestellungen etc.)	Enge Ausnahmen; im Alltagsgebrauch für Smart Glasses idR nicht einschlägig.
Art. 179sexies	Inverkehrbringen/Anpreisen speziell zum widerrechtlichen Abhören/Aufnehmen konstruierter Geräte.	Nach h.L. auf gewöhnliche Smart Glasses kaum anwendbar, da diese nicht spezifisch zur verdeckten Überwachung konstruiert und (regulatorisch) durch eine Aufnahme-LED gekennzeichnet sind.
Art. 179novies	Unbefugtes Beschaffen besonders schützenswerter Personendaten aus einer nicht öffentlich zugänglichen Datensammlung.	Potenziell relevant bei biometrischer Auswertung oder Gesichts-erkennung über die Brille (sofern möglich).

Praktisch entscheidend für Smart Glasses ist Art. 179quater StGB: Dieser Tatbestand schützt – anders als Art. 179bis/179ter – nicht das Gespräch, sondern das Bild, und verlangt keine Heimlichkeit der Aufnahme; massgebend ist allein, dass die betroffene Person sich in einer Situation befindet, in der sie berechtigterweise nicht mit einer Einsehbarkeit durch die Allgemeinheit rechnen muss (Wohnung, Gartenparzelle, Umkleidekabine, aber auch abgeschiedene, obschon öffentlich zugängliche Orte). Das blosses Filmen im öffentlichen Raum bleibt demgegenüber straflos – Smart Glasses werden insoweit wie jede andere Kamera oder ein Smartphone behandelt. Die eigentliche Zusatzgefahr der Datenbrille liegt nicht im Tatbestand selbst, sondern in der Beweisbarkeit: Weil für Umstehende meistens nicht erkennbar ist, ob und wann aufgenommen wird, wird sowohl die Durchsetzung des Rechts in der Praxis erschwert.

Parallel dazu bleibt das **zivilrechtliche Persönlichkeitsrecht** (Art. 28 ZGB, Recht am eigenen Bild) anwendbar und begründet unabhängig vom Strafrecht Unterlassungs-, Beseitigungs- und Schadenersatzansprüche, insbesondere bei der Veröffentlichung von Aufnahmen ohne Einwilligung.

4. Regulatorisches Vakuum und wachsender politischer Druck

Ein gerätespezifisches Bundesgesetz zu Smart Glasses existiert nicht; es gilt der allgemeine, technologieneutrale Rechtsrahmen (Tatbestände aus dem DSG, StGB, ZGB). Angesichts stark steigender Verkaufszahlen (Schweizer Online-Händler berichten für 2026 von einer Vervielfachung gegenüber dem Vorjahr) hat die politische Diskussion in den letzten Monaten jedoch deutlich an Fahrt gewonnen:

- **Bund:** Eine im August 2026 lancierte Petition („Kein Spielzeug für Stalker“) fordert vom Bundesrat bzw. dem EJPD ein Verkaufsverbot für Smart Glasses in der Schweiz; sie

verzeichnete innert weniger Tage mehrere Tausend Unterschriften. Eine Stellungnahme des Bundes steht noch aus (watson.ch, „Widerstand gegen Smart Glasses wächst – auch in der Schweiz“, August 2026. <https://www.watson.ch/wirtschaft/digital/962911430-widerstand-gegen-smart-glasses-waechst-auch-in-der-schweiz>).

- **Gemeinden/Kantone:** In Wil SG ist im Stadtparlament ein parteiübergreifender Vorstoss hängig, der Smart Glasses in städtischen Badeanstalten verbieten will; ähnliche Bestrebungen laufen in Luzern (Kantonsrat) und Basel. Der Berufsverband der Bademeister spricht sich für ein flächendeckendes Verbot mit präventiver Wirkung aus (SRF, „Wil SG: Politik will Smart Glasses aus Badis verbannen“, 17. August 2026. <https://www.srf.ch/news/schweiz/smart-glasses-in-der-badi-heimliche-aufnahmen-mit-smarten-brillen-kommen-nun-verbote-1>).
- **Aufsichtsbehörden:** Der EDÖB prüft laufend, ob auf dem Markt angebotene Modelle den Anforderungen des DSG genügen und datenschutzkonform eingesetzt werden können; ein eigentliches Verbot gestützt auf das geltende Recht erscheint nach bisheriger Einschätzung der Behörden aber schwer begründbar, solange die Geräte eine (wenn auch dezente) optische Aufnahme-Signalisierung aufweisen. Die Debatte hierzu bleibt aber kontrovers (manche erachten die Aufnahme-Signalisierung und Durchsetzungsmöglichkeiten dagegen als zu schwach) (SRF, „Smart Glasses mit Kamera: Datenschutzrisiken der KI-Brillen erklärt“, August 2026. <https://www.srf.ch/news/gesellschaft/digitale-privatsphaere-wie-merke-ich-ob-mich-jemand-mit-smart-glasses-filmt>).

Für **Unternehmen** bedeutsam: Ohne bundesrechtliche Sonderregel bleibt das **Hausrecht** das griffigste Instrument, um das Tragen bzw. den **Einsatz von Smart Glasses auf dem eigenen Areal** (Empfang, Sitzungszimmer, Werkstatt, Fitnessstudio, Badeanstalt) **zu untersagen** – vorausgesetzt, das Verbot wird aktiv kommuniziert über Aushänge, Besucherreglement oder Vertragsklauseln. Das **Hausrecht** ist **zivilrechtlicher Natur** und stützt sich auf Eigentum (Art. 641 ZGB), Besitz (Art. 919 ff. ZGB) oder einem gültigen Nutzungstitel (z.B. Miete, Pacht). Es ist die Befugnis, über einen bestimmten Raum ungestört zu bestimmen und den eigenen Willen frei zu betätigen.

5. Überblick Ausland/EU

5.1 EU-Ebene

Auf Nutzerinnen und Nutzer sowie Unternehmen in der EU findet zunächst das allgemeine DSGVO-Regime Anwendung (Rechtsgrundlage nach Art. 6 DSGVO, verschärfte Anforderungen nach Art. 9 DSGVO bei biometrischer Auswertung, ggf. Pflicht zu einer Datenschutz-Folgenabschätzung). Der Europäische Datenschutzausschuss (EDPB) hat 2026 eine eigene Untersuchung zur «sozialen Akzeptanz» von Smart Glasses in Auftrag gegeben, deren Ergebnisse für Sommer 2026 angekündigt wurden. Zusätzlich ist seit dem 2. August 2026 das Verbot gewisser biometrischer Praktiken nach Art. 5 KI-Verordnung (u.a. Echtzeit-Fernidentifikation im öffentlichen Raum, biometrische Kategorisierung) vollständig anwendbar und für Geräte mit Gesichtserkennungsfunktion potenziell einschlägig. Im EU-Parlament fordert die liberale Fraktion «Renew Europe» die Kommission zur Klärung auf, wie DSGVO und KI-Verordnung auf KI-

gestützte Datenbrillen anzuwenden sind (siehe z.B. GDPR Local, „Smart Glasses and GDPR: Why Europe Is Cracking Down on Camera-Equipped Eyewear“, 10. Juni 2026. <https://gdprlocal.com/smart-glasses-and-gdpr/>).

5.2 Frankreich

Die französische Datenschutzaufsichtsbehörde CNIL warnte bereits im Mai 2026 vor einem «erheblichen Risiko» einer nahezu unsichtbaren und allgegenwärtigen Überwachung durch Smart Glasses und rief Herstellende zu Transparenz, Zweckbindung und Datenminimierung sowie Nutzende zur Rücksichtnahme (Information Dritter, Deaktivierung bei fehlendem Bedarf) auf. Frankreich gehört zu den Staaten, die laut Presseberichten ein Verkaufsverbot prüfen (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 Deutschland

Die NGO HateAid reichte im August 2026 gegen Meta, Ray-Ban, Oakley sowie diverse Händler Strafanzeige bei der deutschen Zentralstelle zur Bekämpfung der Internetkriminalität ein und verlangt ein Verkaufsverbot; als Rechtsgrundlage werden u.a. das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz sowie § 201a deutsches StGB (Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen) angeführt. Deutschland kennt zudem strengere Regeln zum Fotografieren einzelner Personen im öffentlichen Raum als viele andere EU-Staaten, was die rechtliche Ausgangslage dort tendenziell verschärft (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 USA

In den USA konzentriert sich die Entwicklung auf drei Stossrichtungen: (i) Sammelklagen gegen Meta wegen irreführender Datenschutzversprechen, nachdem bekannt wurde, dass Aufnahmen – teils aus intimen Situationen – zu Trainingszwecken durch externe Dienstleistende gesichtet wurden; (ii) biometrische Datenschutzgesetze auf Bundesstaatenebene, allen voran der Illinois Biometric Information Privacy Act (BIPA), die bei Aktivierung von Gesichtserkennungsfunktionen greifen könnten; (iii) institutionelle Nutzungsverbote: Der Bundesstaat New York untersagt Smart Glasses seit dem 20. Juli 2026 landesweit in sämtlichen 1'240 Gerichten (erstes flächendeckendes Verbot auf Bundesstaatenebene), nachdem einzelne Gerichte in Pennsylvania, Wisconsin und Hawaii bereits zuvor punktuelle Verbote erlassen hatten (MEXC News, «Meta AI Smart Glasses Lawsuit Alleges Deceptive Privacy Claims», 2026. <https://www.mexc.com/it-IT/news/862200>).

6. Biometrische Gesichtserkennung mit Smart Glasses

6.1 Stand der Technik und Haltung der Hersteller

Aktuelle Smart Glasses haben werkseitig keine aktivierte Gesichtserkennung; weder Google (Android XR) noch Meta (Ray-Ban Meta) haben eine solche Funktion freigeschaltet – Metas früheres System mit solchen Erkennungsmechanismen wurde 2021 nach Vergleichen eingestellt (siehe all-ai.de, «Meta plant Gesichtserkennung für Ray-Ban Smartglasses im Alltag», 13. Februar 2026. <https://www.all-ai.de/news/beitrage2026/zuckerberg-meta-gesichtserkennung>). In der Meta-App wurde jedoch bereits fertiger, aber deaktivierter Code für eine Funktion „NameTag“ gefunden (siehe heise online, «Ray-Ban Meta: Begleit-App enthält Code für Gesichtserkennung», 5. Juni 2026. <https://www.heise.de/news/Ray-Ban-Meta-Begleit-App-enthaelt-Code-fuer-Gesichts-erkennung-11316322.html>). 2024 zeigte ein Forschungsprojekt «I-XRAY» zweier Harvard-Studierender, dass sich handelsübliche Ray-Ban-Meta-Brillen mit dem Dienst «PimEyes»

zu einem funktionierenden Echtzeit-Tool koppeln lassen könnten (404 Media, «Someone Put Facial Recognition Tech onto Meta's Smart Glasses to Instantly Dox Strangers», 4. Oktober 2024. <https://www.404media.co/someone-put-facial-recognition-tech-onto-metas-smart-glasses-to-instantly-dox-strangers/>).

6.2 EU: Verbot nach Art. 5 KI-VO

Auf EU-Ebene ist biometrische Echtzeit-Fernidentifikation im öffentlichen Raum nach Art. 5 Abs. 1 lit. h KI-VO grundsätzlich verboten (seit 2. Februar 2025). Eine eng gefasste, genehmigungspflichtige Ausnahme besteht nur für Strafverfolgungsbehörden zu drei Zwecken (Opfer-/Vermisstensuche, Abwehr akuter Gefahr, Fahndung nach schweren Straftaten). Für Private besteht keine Ausnahme – kommerzielle oder private Echtzeit-Gesichtserkennung ist ausnahmslos verboten. Separat untersagt Art. 5 Abs. 1 lit. e KI-VO das ungezielte Scraping von Gesichtsbildern (automatisiertes Sammeln von Fotos aus dem Internet für Datenanalysezwecke/Trainingszwecke) zum Aufbau von Erkennungsdatenbanken (das Geschäftsmodell von Diensten wie z.B. Clearview AI oder PimEyes).

6.3 Schweiz: Grundlage eines möglichen Verbots

Die Schweiz kennt kein KI-VO-Pendant. Eine Unzulässigkeit von Biometrie in öffentlich verfügbaren Datenbrillen ergibt sich derzeit vor allem aus dem DSG: Seit der Revision (1. September 2023) gelten identifizierende biometrische Daten als besonders schützenswerte Personendaten (Art. 5 lit. c Ziff. 3 DSG). Die Speicherung und Bearbeitung solcher Daten durch eine unbeschränkte Vielzahl von Datenbrillenträgern ohne spezifisch determinierte Verwendungszwecke wäre kaum verhältnismässig i.S. des DSG und würde auch Schutzmechanismen ermangeln gegen die unzulässige Weitergabe/-verwendung solcher besonders schützenswerten Personendaten. Ergänzend greift Art. 179novies StGB, welches unbefugtes Beschaffen besonders schützenswerter Personendaten aus einer nicht öffentlich zugänglichen Datensammlung als strafbar erklärt sowie das allgemeine Persönlichkeitsrecht (Art. 28 ZGB). Für den Einsatz von Behörden inkl. Polizei gilt zudem das strenge Legalitätsprinzip (Art. 34 Abs. 2 DSG) mit dem Erfordernis einer klaren gesetzlichen Grundlage. Daran fehlte es z.B. 2021 beim ungesetzlichen Clearview-Testeinsatz der Stadtpolizei Zürich (siehe Der Bund / Tages-Anzeiger, «Überwachungstechnologie in der Schweiz: Auch die Polizei muss sich an das Gesetz halten», 6. September 2021. <https://www.derbund.ch/auch-die-polizei-muss-sich-an-das-gesetz-halten-616804935004>). Ein flächendeckender Einsatz an Kundgebungen dürfte eine explizite Gesetzesgrundlage voraussetzen, die meist fehlt.

6.4 Polizei, Nachrichtendienste und Demonstrationen

Polizei und Nachrichtendienste sind vom KI-VO-Verbot in der EU nicht kategorisch ausgenommen. Ein Einsatz an Kundgebungen ohne konkrete Gefahrenlage bliebe wohl unzulässig. International zeigt sich dennoch eine Ausweitung: US-ICE-Mitarbeitende sollen bereits private Ray-Ban-Meta-Brillen zum Filmen von Demonstrierenden nutzen, während das Heimatschutzministerium eigene «ICE Glasses» mit Gesichtserkennung entwickeln lässt (siehe Telepolis, „ICE Glasses: US-Heimatschutz will Bürger mit Datenbrillen überwachen“, 22. April 2026. https://www.telepolis.de/article/ICE-Glasses-US-Heimatschutz-will-Buerger-mit-Daten-brillen-ueberwachen_11267620.html). China setzt seit 2026 flächendeckend Polizei-Smart-Glasses mit Gesichtserkennung ein. In der EU/Schweiz bliebe dies unzulässig (Blogspan, «Chinas Polizei-Smartglasses: 95 Prozent Gesichtserkennung – und ein System, das grösser denkt», 31. Mai 2026. <https://www.blogspan.net/china-polizei-smartglasses-gesichtserkennung/>). Doch die technische Hürde für einen rechtswidrigen Einsatz ist wie die bisherigen Ausführungen zeigen gering.

6.5 Zulässigkeit innerhalb eines Unternehmens

Innerhalb eines Unternehmens gelten dieselben Massstäbe wie bei klassischen biometrischen Zutrittskontrollsystemen: Der EDÖB verlangt einen Rechtfertigungsgrund (eine Einwilligung genügt im Arbeitsverhältnis meist nicht), Verhältnismässigkeit, eine Alternative für Mitarbeitende sowie strikte Einhaltung Zweckbindung bezüglich der damit gesammelten Daten (siehe im Detail dazu den offiziellen Leitfaden des EDÖB zu biometrischen Erkennungssystemen). Anders als ein stationärer Zutrittsleser erfasst eine Smart-Glasses-Erkennung jedoch potenziell fortlaufend und unerkennbar alle Menschen, die ihr begegnen, was die Verhältnismässigkeit regelmässig in Frage stellt und unter dem arbeitsrechtlichen Verbot heimlicher Verhaltenskontrolle (Art. 26 ArGV 3) nicht ohne Weiteres standhalten dürfte.

7. Key Take Away und Empfehlungen

Aus Schweizer Sicht besteht für Smart Glasses noch kein Zulassungs- oder Verkaufsverbot. Risiken realisieren sich vielmehr über den bestehenden Rahmen aus Datenschutz, Strafrecht und Zivilrecht, sobald Personen erkennbar aufgenommen oder Gespräche aufgenommen werden. Angesichts der politischen Dynamik (Petition an den Bundesrat, kommunale und kantonale Vorstösse, EDÖB-Fokus) ist mittelfristig aber wohl mit punktueller Regulierung zu rechnen – sei es auf Verordnungs-, sei es auf kommunaler Ebene (als Beispiel z.B. Badeanlage-Reglemente).

- Unternehmen mit Publikumsverkehr sollten das **Hausrecht aktiv nutzen** und Nutzungsbeschränkungen klar kommunizieren.
- Beim **betrieblichen Einsatz** von Smart Glasses (z.B. für Wartung, Logistik, Ausbildung) empfiehlt sich eine **dokumentierte Interessenabwägung bzw. eine Datenschutzfolgeabschätzung** im gesetzlichen Sinne (Art. 22 DSG) und klare interne Weisungen zu Aufnahme, Speicherung und Löschung von mit Smart Glasses gesammelten Daten.
- **Mitarbeitende und Kundschaft** sind über den Einsatz zu **informieren**. Wo gesetzlich nötig, sind Einwilligungen vorgängig einzuholen.
- Die **Entwicklung auf EU-Ebene** (EDPB-Bericht, Anwendung der KI-Verordnung) sind laufend zu **beobachten**, weil sie faktisch als Referenzrahmen auch für die Schweizer Praxis wirken können.
- Der Einsatz von **biometrischer Gesichtserkennung** für private Zwecke ist **technisch** derzeit bei den im Verkehr befindlichen Datenbrillen **deaktiviert** und in der EU gesetzlich verboten (nur für eng umschriebene Ausnahmetatbestände im strafrechtlichen Untersuchungs-/Verfolgungskontext). In der Schweiz ist dies zwar nicht sprichwörtlich verboten, aber mit den gegenwärtigen Gesetzen kaum rechtfertigbar. Man lässt es bei der Deaktivierung lieber bleiben. Im Ausland (z.B. USA) wird diese Technologie von Behörden freizügiger eingesetzt, in China von der Polizei seit 2026 flächendeckend.

Diese Kurzpublikation dient der allgemeinen Information und ersetzt keine Rechtsberatung im Einzelfall.

Dirk Spacek, Dr. iur., LL.M. ist Rechtsanwalt und Partner in Zürich. Er berät Unternehmen in allen vertrags- und wirtschaftsrechtlichen Belangen mit besonderem Fokus auf Fragen an der Schnittstelle von Technologie, Immaterialgüter- und Daten/Cyberrecht.