Verbraucherzentrale
Bundesverband

Smart Glasses: Datenschutzrisiken und Herstellerverantwortung

Positionspapier des Verbraucherzentrale Bundesverbands (vzbv)

14. Oktober 2026

Inhalt

I. Verbraucherrelevanz 3

II. Zusammenfassung 4

III. Geltende Rechtslage 5

1. Verbot getarnter Überwachungsgeräte nach § 8 TDDDG 5
2. Datenschutzrechtliche Verantwortung der Nutzer:innen 6

IV. Das strukturelle Problem der Verantwortungsverteilung 7

V. Warum ein pauschales Verbot nicht die überzeugendste Lösung ist 8

VI. Stärkere Herstellerverantwortung als Lösungsbaustein 8

Impressum 10

I. Verbraucherrelevanz

Smart Glasses können sowohl für Personen im Umfeld als auch für ihre Nutzer:innen erhebliche Risiken mit sich bringen. Anlass der aktuellen Debatte sind insbesondere die Ray-Ban Meta AI Glasses. Die Geräte ähneln herkömmlichen Brillen, enthalten aber unter anderem eine Kamera, mehrere Mikrofone, Lautsprecher und eine Verbindung zur Meta-AI-App. Nutzer:innen können damit Fotos und Videos aufnehmen, Informationen über ihre Umgebung abrufen und Inhalte über soziale Netzwerke teilen. Für Menschen mit Sehbehinderungen können sich daraus zugleich neue Assistenzmöglichkeiten ergeben.

Da die Brille am Körper getragen wird und der Blickrichtung folgt, können Außenstehende kaum beurteilen, ob sie aufgenommen oder ihre Daten durch ein KI-System ausgewertet werden. Eine kleine weiße Leuchte weist zwar auf Foto- und Videoaufnahmen hin. Ihre Wahrnehmbarkeit hängt jedoch von Entfernung, Blickwinkel und Lichtverhältnissen ab. Auch bei sichtbarer Leuchte bleibt offen, welche Funktion aktiv ist und wie die erfassten Daten verarbeitet werden.

Auch für die Nutzer:innen entstehen erhebliche Unsicherheiten. Ein datenschutzkonformer Einsatz der Aufnahme- und KI-Funktionen ist im öffentlichen Raum in vielen Situationen kaum möglich. Dennoch bewerben die Hersteller diese Funktionen, überlassen es aber weitgehend den Nutzer:innen, ihren rechtmäßigen Einsatz sicherzustellen.

II. Zusammenfassung

Die Debatte um die Ray-Ban Meta AI Glasses zeigt eine strukturelle Lücke im geltenden Recht: Hersteller bringen Produkte mit weitreichenden Aufnahme- und Analysefunktionen auf den Markt, während die Verantwortung für deren datenschutzkonformen Einsatz häufig bei den Nutzer:innen liegt. Diese müssen damit rechtliche Risiken auffangen, die wesentlich durch die Gestaltung des Produkts entstehen.

Die Bundesnetzagentur und der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit bewerten unterschiedlich, ob die Aufnahmeanzeige der Brillen ausreicht, um ein Verbot nach § 8 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) auszuschließen. Diese unterschiedlichen Bewertungen zeigen, dass die geltende Rechtslage keine ausreichende Sicherheit bietet. Die Debatte um die Hinweisleuchte greift aber ohnehin zu kurz: Selbst wenn unbeteiligte Personen ein Aufnahmesignal wahrnehmen, ersetzt dies weder eine erforderliche Einwilligung noch die notwendige Information über die Datenverarbeitung.

Ein pauschales Verbot von Smart Glasses ist aus Sicht des Verbraucherzentrale Bundesverbands (vzbv) jedoch nicht die überzeugendste Lösung. Aufnahme- und Analysefunktionen dürften künftig auch in weitere körpernah getragene Geräte integriert werden – Berichten zufolge entwickelt etwa Apple Kopfhörer mit integrierten Kameras beziehungsweise optischen Sensoren.[1] Ein auf Smart Glasses beschränktes Verbot würde daher zu kurz greifen, könnte zugleich legitime Assistenzfunktionen erfassen und würde das strukturelle Problem nicht lösen.

> Der vzbv fordert deshalb eine stärkere Verantwortung von Soft- und Hardwareherstellern. Hersteller sollten verpflichtet werden, ihre Produkte so zu gestalten, dass Verbraucher:innen sie datenschutzkonform verwenden können und die Rechte unbeteiligter Personen geschützt werden. Die Verpflichtung sollte produktübergreifend auf europäischer Ebene gelten und damit auch smarte Kraftfahrzeuge, vernetzte Türklingelkameras und andere Produkte mit Aufnahme- und Analysefunktionen erfassen. Die Bundesregierung sollte sich im Rahmen der aktuellen Reform der Datenschutz-Grundverordnung (DSGVO) für entsprechende Vorgaben einsetzen.

[1] Siehe etwa Apfeltalk: Kamera-AirPods von Apple: Alle neuen Gerüchte im Überblick, 2026, https://www.apfeltalk.de/magazin/news/kamera-airpods-von-apple-alle-neuen-geruechte-im-ueberblick/, 14.10.2026.

III. Geltende Rechtslage

1. Verbot getarnter Überwachungsgeräte nach § 8 TDDDG

§ 8 des TDDDG richtet sich gegen getarnte Überwachungsgeräte. Verboten sind unter anderem Telekommunikationsanlagen, die ihrer Form nach einen anderen Gegenstand vortäuschen oder mit einem Gegenstand des täglichen Gebrauchs verkleidet sind. Zusätzlich müssen sie dazu geeignet und bestimmt sein, das Bild einer Person unbemerkt aufzunehmen oder das nicht öffentlich gesprochene Wort unbemerkt abzuhören.

Als zum unbemerkten Aufnehmen oder Abhören bestimmt gilt ein Gerät insbesondere dann, wenn seine Aufnahmefunktion beim bestimmungsgemäßen Gebrauch für die betroffene Person nicht eindeutig erkennbar ist. Das Verbot kann bereits die Herstellung, das Bereitstellen auf dem Markt und den Besitz des Geräts erfassen. Es setzt keinen nachgewiesenen Datenschutzverstoß durch eine konkrete Aufnahme voraus.

Der Hamburgische Datenschutzbeauftragte hält es aufgrund einer technischen Untersuchung für möglich, dass die Ray-Ban Meta AI Glasses unter diese Vorschrift fallen. Nach seiner Einschätzung ist die integrierte Leuchte nicht unter allen üblichen Bedingungen ausreichend wahrnehmbar.[2] Für die Durchsetzung des Verbots sei jedoch die Bundesnetzagentur zuständig.[3]

Die Bundesnetzagentur bewertet die bislang geprüften Modelle anders. Nach ihrer Auffassung macht die integrierte Leuchte die Aufnahmefunktion für Personen in der Umgebung hinreichend erkennbar. Sie sieht daher derzeit keinen Anlass für ein förmliches Verbotsverfahren.[4]

Die unterschiedlichen Bewertungen betreffen vor allem die Frage, wann eine Aufnahmefunktion „eindeutig erkennbar“ ist. Bloße technische Sichtbarkeit unter bestimmten Prüfbedingungen ist nicht zwingend mit praktischer Erkennbarkeit im Alltag gleichzusetzen. Darüber hinaus bleibt unklar, welchen Aussagegehalt ein kleines weißes Licht für Außenstehende hat.[5]

Der Anwendungsbereich von § 8 TDDDG bleibt zugleich auf getarnte Überwachungsgeräte begrenzt. Nicht jedes vernetzte Produkt mit einer unauffällig integrierten Kamera fällt deshalb automatisch unter die Vorschrift. Das erschwert ihre Anwendung auf komplexe Produkte, bei denen die Umgebungserfassung nur eine von mehreren Funktionen darstellt. Vergleichbare Abgrenzungsfragen entstehen etwa bei smarten Kraftfahrzeugen und vernetzten Türklingelkameras.

---

[2] Siehe Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit: Abschlussbericht zur technischen und datenschutzrechtlichen Untersuchung der Ray-Ban Meta AI Glasses, 2026, S. 1–2 und 32, https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/260910_HmbBfDI_Abschlussbericht_Ray_Ban_Meta_AI_Glasses_DE.pdf, 14.10.2026.

[3] Siehe Fuchs, Thomas: Endet die Privatsphäre im öffentlichen Raum? Gastbeitrag im Tagesspiegel Background, 2026, https://datenschutz-hamburg.de/news/endet-die-privatsphaere-im-oeffentlichen-raum-warum-die-debatte-um-smartglasses-so-wichtig-ist, 14.10.2026.

[4] Siehe Krempl, Stefan: Kein Verbot für Meta-Brillen: Behörde sieht LED-Signal als ausreichend, 2026, https://www.heise.de/news/Smart-Glasses-Bundesnetzagentur-verfolgt-kein-Verbot-von-Metas-Kamera-Brille-11415153.html, 14.10.2026.

[5] Siehe Bruna, Yann: The connected gaze. Video recording, surveillance and administering evidence in the age of smart glasses. Forschungsbericht im Rahmen des Support Pool of Experts des Europäischen Datenschutzausschusses, 2026, S. 27–29, https://www.edpb.europa.eu/system/files/2026-10/20261001_spe_report_smart_glass_en.pdf, 14.10.2026.

2. Datenschutzrechtliche Verantwortung der Nutzer:innen

Unabhängig von § 8 TDDDG richtet sich die Rechtmäßigkeit konkreter Aufnahmen nach der DSGVO, soweit personenbezogene Daten verarbeitet werden und die Haushaltsausnahme nicht greift.

Die Haushaltsausnahme gilt für ausschließlich persönliche oder familiäre Tätigkeiten. Sie kann etwa Aufnahmen von Familienmitgliedern oder engen Freund:innen im privaten Umfeld erfassen. Sie gilt aber nicht generell für jede Aufnahme durch eine Privatperson. Insbesondere bei der systematischen Erfassung des öffentlichen Raums oder bei einer Veröffentlichung in sozialen Netzwerken kann der persönliche und familiäre Bereich überschritten sein.

Greift die Haushaltsausnahme nicht, benötigen Nutzer:innen eine Rechtsgrundlage für die Verarbeitung. In Betracht kommen etwa eine Einwilligung der betroffenen Person oder berechtigte Interessen. Beide Möglichkeiten stoßen bei Smart Glasses auf erhebliche praktische Grenzen.

Eine Einwilligung setzt voraus, dass Betroffene ausreichend informiert werden und freiwillig zustimmen. Eine leuchtende Anzeige erfüllt diese Voraussetzungen nicht. Selbst wenn Betroffene das Signal wahrnehmen, liegt darin weder eine Einwilligung in die Aufnahme noch in eine Übermittlung, Veröffentlichung oder Verwendung ihrer Daten für das Training eines KI-Systems.

Bei einer Verarbeitung aufgrund berechtigter Interessen müssen die Interessen der Nutzer:innen gegen die Rechte und Freiheiten der betroffenen Personen abgewogen werden. In einzelnen Fällen können berechtigte Interessen vorliegen, etwa bei konkreten Sicherheitsinteressen, der Orientierung oder bestimmten Assistenzfunktionen. Bei der gezielten Aufnahme unbeteiligter Personen, die damit nicht rechnen müssen und der Erfassung kaum ausweichen können, werden deren Rechte jedoch häufig überwiegen.

Besonders problematisch sind weitergehende Verarbeitungen. Wird Meta AI eingesetzt, können personenbezogene Daten Dritter an Meta übermittelt und analysiert werden. Bei einer Veröffentlichung in sozialen Netzwerken oder einer Verwendung für das KI-Training kommen weitere Zwecke und Verarbeitungsschritte hinzu. Dabei können auch Hersteller oder Diensteanbieter datenschutzrechtlich verantwortlich sein. Die datenschutzrechtliche Bewertung hängt von der konkreten Funktion, den Datenflüssen und den Einstellungen des jeweiligen Dienstes ab.[6]

[6] Siehe Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (2026) (wie Anm. 1), Abschnitt IV.3 und IV.4.

IV. Das strukturelle Problem der Verantwortungsverteilung

Für die einzelne Aufnahme liegt die datenschutzrechtliche Verantwortung häufig bei der Person, die die Brille trägt und ihre Funktionen aktiviert. Nutzer:innen entscheiden, ob sie die Kamera einschalten, wohin sie blicken und ob sie eine Aufnahme speichern oder veröffentlichen.

Die Hersteller bestimmen jedoch die wesentlichen technischen Rahmenbedingungen. Dazu gehören insbesondere:

- die Integration und Sichtbarkeit von Kamera und Mikrofonen,
- die Funktionsweise von Aufnahmeanzeigen,
- die Voreinstellungen,
- die Art und Dauer der Speicherung,
- die Verbindung mit KI-Anwendungen und sozialen Netzwerken,
- die Möglichkeiten einer Übermittlung und Weiterverwendung der Daten,
- die Schutzvorkehrungen gegen Missbrauch.

Verbraucher:innen erwerben also ein Produkt, dessen zentrale Funktionen sie in vielen Alltagssituationen nur unter schwer überschaubaren rechtlichen Voraussetzungen verwenden können. Gleichzeitig haben sie kaum Einfluss auf die technische Gestaltung, aus der diese Risiken entstehen.

Der Hersteller kann sich darauf berufen, dass er die einzelne Aufnahme nicht auslöst und nicht bestimmt, welche Personen erfasst werden. Soweit Aufnahmen auf dem Gerät verbleiben und das Unternehmen sie weder erhält noch anderweitig verarbeitet, kann dies seine datenschutzrechtliche Rolle nach geltendem Recht begrenzen.

Anders kann die Bewertung ausfallen, wenn Hersteller oder Anbieter Daten für eigene Zwecke verarbeiten, etwa bei der Veröffentlichung über soziale Netzwerke, im Rahmen eines KI-Dienstes oder für das KI-Training. Je nach konkreter Verarbeitung können eigene oder gemeinsame Verantwortlichkeiten bestehen.

Unabhängig von dieser Einordnung bleibt ein verbraucherpolitisches Problem: Unternehmen bestimmen durch die Produktgestaltung maßgeblich, welche Risiken entstehen und welche Schutzvorkehrungen bestehen. Sie sollten die daraus folgenden rechtlichen Risiken nicht weitgehend auf die Käufer:innen und Nutzer:innen ihrer Produkte abwälzen dürfen.

Dieses Problem reicht über Meta und Smart Glasses hinaus. Vergleichbare Konstellationen entstehen bei smarten Kraftfahrzeugen, deren Kameras die Umgebung erfassen, bei vernetzten Türklingelkameras und bei anderen Geräten, die Daten über Personen in ihrer Umgebung sammeln. Smart Glasses sind damit ein besonders anschauliches Beispiel für eine allgemeine Regelungslücke bei vernetzten Soft- und Hardwareprodukten.

V. Warum ein pauschales Verbot nicht die überzeugendste Lösung ist

Die Risiken von Smart Glasses haben zu Forderungen nach einem Verbot der Geräte geführt. Ein pauschales Produktverbot ist aus Sicht des vzbv jedoch nicht die überzeugendste Lösung.

Bereits der Gegenstand eines solchen Verbots lässt sich nur schwer trennscharf bestimmen. Ein auf die aktuellen Meta-Brillen beschränktes Verbot ließe vergleichbare Geräte anderer Hersteller unberührt. Ein Verbot sämtlicher Brillen mit Kameras könnte dagegen auch legitime Assistenzfunktionen und Produkte mit wirksamen Schutzvorkehrungen erfassen.

Eine weiter gefasste Regelung für Kameras in Alltagsgegenständen würde neue Abgrenzungsfragen schaffen. Neben Brillen könnten etwa andere körpernah getragene Geräte, smarte Kraftfahrzeuge, Türklingeln und Haushaltsgeräte betroffen sein. Die zunehmende Integration von Sensoren in unterschiedliche Produkte macht eine Regulierung anhand der äußeren Produktform immer weniger sachgerecht.

Ein Verbot von Smart Glasses würde heimliche und rechtswidrige Aufnahmen auch nicht verhindern. Personen, die andere Menschen unbemerkt aufnehmen wollen, können dafür bereits Smartphones, kleine Kameras und zahlreiche andere leicht verfügbare Geräte verwenden. Smart Glasses können solche Aufnahmen erleichtern, sind aber weder deren Voraussetzung noch die einzige technische Möglichkeit.

Gezielte Beschränkungen können in besonders sensiblen Bereichen dennoch sinnvoll sein. Das betrifft beispielsweise Umkleiden, Saunen, Sanitärbereiche oder andere Orte, an denen Menschen in besonderem Maß auf den Schutz ihrer Privatsphäre vertrauen. In privaten Einrichtungen können Betreiber:innen entsprechende Regeln vielfach bereits über ihr Hausrecht durchsetzen. Solche Maßnahmen können einen ergänzenden Schutz bieten, lösen aber nicht das strukturelle Problem der Produktgestaltung und Verantwortungsverteilung.

VI. Stärkere Herstellerverantwortung als Lösungsbaustein

Eine stärkere Verantwortung von Soft- und Hardwareherstellern ist ein zentraler Baustein, um die beschriebenen Probleme zu lösen. Der vzbv fordert solche Regelungen bereits seit Längerem.

Unternehmen sollten sich ihrer Verantwortung nicht allein dadurch entziehen können, dass sie auf ihre Rolle als Auftragsverarbeiter verweisen oder geltend machen, dass Nutzer:innen die konkrete Verarbeitung auslösen. Entscheidend sollte stärker berücksichtigt werden, welchen tatsächlichen Einfluss ein Unternehmen auf die Produktgestaltung, die Voreinstellungen, die Datenflüsse und die Schutzvorkehrungen hat.

Hersteller sollten daher verpflichtet werden, ihre Produkte so zu gestalten, dass Verbraucher:innen sie datenschutzkonform verwenden können. Dabei müssen sie auch die Rechte von Personen schützen, die von dem Produkt erfasst werden, ohne selbst Käufer:innen oder Nutzer:innen zu sein.

Die Hersteller sollten hierfür vorhersehbare Nutzungsweisen und Missbrauchsrisiken bereits bei der Produktentwicklung berücksichtigen und geeignete Schutzvorkehrungen treffen. Je nach Produkt können dazu beispielsweise datenschutzfreundliche Voreinstellungen, Datenminimierung oder technische Begrenzungen besonders riskanter Funktionen gehören.[7]

Eine stärkere Herstellerverantwortung schützt zwei Gruppen: Sie schützt unbeteiligte Personen davor, ohne hinreichende Rechtsgrundlage erfasst und analysiert zu werden. Zugleich schützt sie die Käufer:innen vernetzter Produkte vor schwer überschaubaren rechtlichen Risiken bei der Nutzung beworbener Funktionen.

Eine europäische Regelung ist nationalen Einzellösungen vorzuziehen. Einheitliche Vorgaben verhindern eine Zersplitterung des Binnenmarkts und vereinfachen die Rechtsanwendung. Diese sollten nach dem Marktortprinzip auch für Hersteller aus Drittstaaten gelten, die ihre Produkte in der Europäischen Union anbieten. Die Größe des europäischen Markts schafft zugleich einen starken Anreiz für Hersteller, ihre Produkte an die europäischen Vorgaben anzupassen.

Entsprechende Vorschläge hat der vzbv etwa in seinem Beitrag zum Digital Fitness Check der Europäischen Kommission vorgelegt.[8] Die Forderung nach stärkerer Herstellerverantwortung findet auch bei der Datenschutzkonferenz und dem Berufsverband der Datenschutzbeauftragten Deutschlands Unterstützung.[9] Bund und Länder vereinbaren in ihrer föderalen Modernisierungsagenda ebenfalls, sich für Datenschutzpflichten der Hersteller und Anbieter von Standardlösungen einzusetzen.[10] Änderungsanträge der Fraktion Die Grünen/EFA im Europäischen Parlament zum Digital Omnibus greifen zentrale Elemente dieser Vorschläge auf.[11] Die aktuelle Reform der DSGVO bietet damit eine Gelegenheit, die Verantwortungsverteilung bei vernetzten Produkten neu zu justieren.

---

[7] Siehe Europäischer Datenschutzausschuss: Statement on Smart glasses, 2026, Rn. 33, https://www.edpb.europa.eu/system/files/2026-10/20261310_edpb_statement_smart-glasses_en.pdf, 14.10.2026.

[8] Siehe Verbraucherzentrale Bundesverband: Digital Fitness Check. Stellungnahme des Verbraucherzentrale Bundesverbands (vzbv) zu der Sondierung (call for evidence) der Europäischen Kommission, 2026, S. 7f, https://www.vzbv.de/sites/default/files/2026-03/26-03-11_vzbv_Stellungnahme_EU%20KOM_Digital%20Fitness%20Check.pdf, 14.10.2026.

[9] Siehe Datenschutzkonferenz: DSGVO-Reform: IT-Hersteller in die Verantwortung nehmen! Entschließung vom 12. Dezember 2025, 2025, https://www.datenschutzkonferenz-online.de/media/en/DSK_Entschliessung_DSGVO_Herstellerverantwortung.pdf, 13.10.2026; Berufsverband der Datenschutzbeauftragten Deutschlands: Datenschutz gestalten. Positionspapier zur Reform der EU-Datenschutz-Grundverordnung (DSGVO), 2025, https://www.bvdnet.de/wp-content/uploads/2025/06/20250624_BvD-Positionspapier-zur-Reform-der-DSGVO.pdf, 14.10.2026.

[10] Siehe Bundeskanzler und Regierungschefinnen und Regierungschefs der Länder: Die Föderale Modernisierungsagenda. Beschluss vom 4. Dezember 2025, 2025, Nr. 166, Ziffer 4, https://www.bundesregierung.de/resource/blob/975228/2397654/c57248be7fa2d61ab6d8b12c0f29f05b/2025-12-04-mpk-staatsmodernisierung-data.pdf, 14.10.2026.

[11] Siehe Europäisches Parlament, Ausschüsse für Industrie, Forschung und Energie sowie für bürgerliche Freiheiten, Justiz und Inneres: Änderungsanträge zum Berichtsentwurf zum Digital Omnibus (2025/0360(COD)), 2026, Änderungsanträge 980 und 983, PE791.072v01-00, https://data.europarl.europa.eu/distribution/reds_iCmDoc_Amd/CJ72-AM-791072/CJ72-AM-791072_en.pdf; Änderungsantrag 1171, PE791.073v01-00, https://data.europarl.europa.eu/distribution/reds_iCmDoc_Amd/CJ72-AM-791073/CJ72-AM-791073_en.pdf, jeweils 14.10.2026.

Impressum

Herausgegeben von:
Verbraucherzentrale Bundesverband e.V.
Rudi-Dutschke-Straße 17, 10969 Berlin

T +49 30 25800-0
digitales@vzbv.de
vzbv.de

Der Verbraucherzentrale Bundesverband e.V. ist im Deutschen Lobbyregister und im europäischen Transparenzregister registriert. Sie erreichen die entsprechenden Einträge hier und hier.