Leitfaden zu smarten Technologien wie Smart Glasses

Datenschutz, Regulierung und Handlungsempfehlungen



bitkom

Inhalt

1 Einleitung: Warum jetzt handeln? 3

2 Technologische Übersicht: Was sind smarte Technologien? 4

Die Entwicklung smarter Geräte 5

Kamera ist nicht gleich Aufnahme: Speichern oder verarbeiten? 8

Anwendungsfälle 9

Rechtliche Einordnung der Unterscheidung 10

Haushaltsausnahme bei privater Nutzung 11

Bewertung nach §8 TDDDG 11

Sensorik ist nicht automatisch Aufnahme 12

3 Zentrale Herausforderungen für die Privatsphäre und datenschutzrechtliche Anforderungen 13

Umfassende Datenerfassung 13

Barrierefreiheit als verbindlicher Prüfungsmaßstab 15

Aufklärung und Produktgestaltung statt Produktverbot 15

Standort- und Wertschöpfungsperspektive berücksichtigen. 15

Transparenz und Information 16

Sicherheitsaspekte 17

Beruflicher und institutioneller Einsatz 17

4 Handlungsempfehlungen 19

Für Anbieter 20

Für Nutzerinnen und Nutzer 25

Für Aufsichtsbehörden 26

Für die Politik 28

1 Einleitung: Warum jetzt handeln?

Smart Glasses rücken zunehmend in den Alltag und zugleich in den Fokus von Politik und Aufsichtsbehörden. In mehreren europäischen Ländern wird derzeit diskutiert, wie mit Geräten umzugehen ist, die Kameras, Mikrofone und KI-Funktionen in alltagstaugliche, körpernah getragene Geräte integrieren.

Auch in Deutschland wird zunehmend diskutiert, welche datenschutzrechtlichen und regulatorischen Herausforderungen mit Smart Glasses verbunden sind. Im Mittelpunkt stehen dabei insbesondere Fragen zur Aufnahme unbeteiligter Personen, zur Erkennbarkeit laufender Aufnahmen und zur möglichen verdeckten Nutzung von Aufnahmefunktionen. Diskutiert wird zudem, wie bestimmte Geräte oder Funktionen aufgrund ihrer Bauform und Funktionsweise einzustufen sind. Entscheidend ist dabei nicht nur, ob Daten erfasst werden, sondern auch wie transparent dies geschieht und für welchen Zweck die Daten verarbeitet werden.

Die gesellschaftliche Haltung ist zugleich ambivalent: 43 Prozent der Deutschen ab 16 Jahren haben laut einer repräsentativen Studie im Auftrag des Bitkom Smart Glasses bereits genutzt oder würden sie gerne nutzen. Gleichzeitig möchten 76 Prozent nicht von anderen mit solchen Brillen aufgenommen werden, und 82 Prozent halten eine deutlich sichtbare Kennzeichnung laufender Aufnahmen für wichtig. An Smart Glasses scheiden sich damit tatsächlich die Geister: Offenheit für die Technologie trifft auf ein ausgeprägtes Bedürfnis nach Transparenz und Kontrolle.

Die Debatte reicht jedoch über Smart Glasses hinaus. Kameras, Mikrofone und andere Sensoren finden sich bereits heute in Smartphones, Kopfhörern, Fahrzeugen, Drohnen oder Haushaltsrobotern und werden künftig in immer mehr KI-gestützte Systeme integriert. Die entscheidenden Fragen sind deshalb nicht an eine einzelne Geräteklasse gebunden: Was darf ein smartes Gerät erfassen? Wann entsteht eine Aufnahme, wann werden Daten lediglich für eine Funktion verarbeitet? Was darf gespeichert, weitergegeben oder für KI-Anwendungen genutzt werden?

Dieses Papier ordnet smarte Technologien und ihre unterschiedlichen Funktionen ein und untersucht am Beispiel von Smart Glasses, welche Herausforderungen sich für Privatsphäre, Datenschutz, Sicherheitsinteressen und Regulierung ergeben. Im Mittelpunkt stehen dabei insbesondere die Unterscheidung zwischen Aufnahme, Verarbeitung und Speicherung, die Transparenz gegenüber betroffenen Personen sowie die Frage, wie bestehende rechtliche Anforderungen auf neue Geräte und Funktionen angewendet werden können. Darauf aufbauend werden Ansätze aufgezeigt, wie sich Innovation, gesellschaftliche Teilhabe und ein hohes Schutzniveau für die Privatsphäre miteinander verbinden lassen.

43%

sind der Nutzung von Smart Glasses gegenüber offen eingestellt.

↗Dataverse (2026)

82%

wollen, dass Aufnahmen deutlich sichtbar angezeigt werden.

↗Dataverse (2026)

2 Technologische Übersicht: Was sind smarte Technologien?

Smarte Technologien sind längst Teil unseres Alltags. Smartphones, Smartwatches, Kopfhörer, Haushaltsroboter oder vernetzte Fahrzeuge verfügen heute über Sensoren, Rechenleistung und Software, mit denen sie Informationen über ihre Nutzerinnen und Nutzer oder ihre Umgebung erfassen und verarbeiten können. Mit der zunehmenden Verbreitung von Künstlicher Intelligenz werden diese Geräte zugleich immer besser darin, Situationen zu interpretieren, Zusammenhänge zu erkennen und selbstständig auf ihre Umgebung zu reagieren.

Charakteristisch für viele smarte Technologien ist damit, dass sie nicht mehr ausschließlich auf eine bewusste Eingabe reagieren. Stattdessen können sie ihre Umgebung kontinuierlich oder situationsabhängig wahrnehmen. Dafür kommen unterschiedliche Sensoren zum Einsatz: etwa Kameras, Mikrofone, Bewegungs- und Abstandssensoren, GPS, Beschleunigungssensoren, Radar, Lidar oder Sensoren zur Messung von Temperatur, Licht oder anderen Umgebungsbedingungen. Je nach Gerät werden diese Informationen lokal verarbeitet oder an andere Geräte beziehungsweise Cloud-Dienste übertragen.

Besonders deutlich wird diese Entwicklung bei Smart Glasses und anderen körpernah getragenen Geräten. Moderne smarte Brillen können beispielsweise Kameras, Mikrofone und Bewegungssensoren kombinieren und damit erfassen, was sich im Sichtfeld der Nutzerinnen und Nutzer befindet. In Verbindung mit KI können Objekte, Texte oder Situationen erkannt und Informationen unmittelbar zur Verfügung gestellt werden. Perspektivisch können solche Systeme stärker zu persönlichen, kontextbezogenen digitalen Assistenten werden.

Ähnliche Prinzipien finden sich bereits heute in zahlreichen anderen smarten Geräten:

- **Smarte Kopfhörer und Hearables** verfügen bereits heute über Mikrofone, Bewegungs- und teilweise weitere Sensoren. Sie können beispielsweise Umgebungsgeräusche analysieren, Sprache erkennen oder ihre Audiowiedergabe an die jeweilige Situation anpassen. Mit leistungsfähigeren KI-Systemen könnten Kopfhörer künftig noch stärker auf den Kontext ihrer Nutzerinnen und Nutzer reagieren und beispielsweise Gespräche, Orte oder Aktivitäten berücksichtigen.
- **Haushalts- und Serviceroboter** erfassen ihre Umgebung ebenfalls mit einer Vielzahl von Sensoren. Staubsaugerroboter nutzen beispielsweise Kameras, Laser- oder Abstandssensoren, um Räume zu kartieren, Hindernisse zu erkennen und sich autonom zu bewegen. Je leistungsfähiger solche Systeme werden, desto genauer können sie Räume, Gegenstände oder Personen unterscheiden und ihre Tätigkeit daran anpassen.
- **Drohnen** kombinieren häufig Kameras mit GPS, Beschleunigungs-, Höhen- und Abstandssensoren. Damit können sie ihre Umgebung aus der Luft erfassen und zum Beispiel für Inspektionen, Vermessungen, Landwirtschaft, Logistik oder

Medienproduktionen eingesetzt werden. Auch hier ermöglichen Fortschritte bei KI und Computer Vision eine zunehmend automatisierte Auswertung der erfassten Daten.

- **Smarte Fahrzeuge und Mobilitätssysteme** gehören ebenfalls zu den besonders sensorintensiven Technologien. Kameras, Radar, Ultraschall und teilweise Lidar erfassen Verkehrsteilnehmende, Fahrbahnen und Hindernisse. Diese Informationen bilden die Grundlage für Assistenzsysteme und perspektivisch für immer stärker automatisiertes Fahren.
- **Smart-Home- und Sicherheitssysteme** erfassen ebenfalls Informationen über ihre unmittelbare Umgebung. Dazu gehören etwa intelligente Türklingeln, Überwachungskameras, Bewegungsmelder, smarte Lautsprecher oder andere vernetzte Sensoren. Sie können erkennen, ob sich Personen in einem Raum befinden, Geräusche wahrnehmen oder Ereignisse automatisiert klassifizieren und entsprechende Aktionen auslösen.
- Darüber hinaus entstehen zunehmend **mobile Roboter, Lieferroboter und autonome Systeme**, die sich im öffentlichen oder halböffentlichen Raum bewegen. Auch sie sind darauf angewiesen, ihre Umgebung kontinuierlich zu erfassen und zu interpretieren. Ähnliche Technologien kommen in Industrie und Logistik beispielsweise bei autonomen Transportfahrzeugen oder kollaborativen Robotern zum Einsatz. Perspektivisch gilt dies in besonderem Maße für humanoide und andere autonome Roboter: Damit sie sinnvoll mit Menschen interagieren können, müssen sie ihre Umgebung und ihre jeweiligen Interaktionspartner erkennen und Situationen entsprechend einordnen können.

Die Entwicklung smarter Geräte

Gemeinsam ist diesen Technologien ein grundlegender Wandel: Digitale Geräte werden zunehmend von Werkzeugen, die auf konkrete Eingaben reagieren, zu Systemen, die ihre Umgebung wahrnehmen und Situationen selbstständig einordnen können. Fortschritte bei Sensorik, Miniaturisierung, Konnektivität und Künstlicher Intelligenz beschleunigen diese Entwicklung.

Diese Entwicklung beschränkt sich nicht auf einzelne Endgeräte. Mit 5G Advanced und perspektivisch 6G gewinnt auch die integrierte Sensorik und Kommunikation (Integrated Sensing and Communication, ISAC) an Bedeutung. Dabei werden Kommunikationsnetze nicht nur zur Datenübertragung genutzt, sondern können zugleich Informationen über ihre Umgebung erfassen, etwa Positionen, Bewegungen oder Objekte. Dadurch entstehen neue Anwendungsmöglichkeiten unter anderem für Verkehr, Gesundheitswesen, öffentliche Sicherheit, Katastrophenschutz und den Schutz kritischer Infrastrukturen.

Damit verändern sich zugleich die Anforderungen an den verantwortungsvollen Einsatz solcher Technologien. Je näher Geräte am Menschen eingesetzt werden und je umfassender sie ihre Umgebung erfassen können, desto wichtiger werden Fragen danach, welche Daten erhoben werden, wann und für wen eine Erfassung erkennbar ist, wo Daten verarbeitet und gespeichert werden und welche Kontrollmöglichkeiten Nutzerinnen und Nutzer sowie möglicherweise erfasste Dritte haben. Dabei sollte die

Bewertung nicht allein an einzelnen Geräteklassen ansetzen. Vergleichbare Funktionen und damit auch vergleichbare Fragestellungen können bei sehr unterschiedlichen Geräten auftreten. Entscheidend ist vielmehr, welche Informationen sie erfassen und wie diese anschließend verarbeitet werden.

Die aktuelle Diskussion um Smart Glasses ist deshalb Teil einer größeren technologischen Entwicklung. Die dabei aufgeworfenen Fragen betreffen nicht allein Brillen, sondern grundsätzlich smarte, sensorbasierte und KI-gestützte Geräte. Viele dieser Fragen sind zudem nicht grundsätzlich neu: Smartphones, Dashcams, smarte Türklingeln, Staubsaugerroboter oder Fahrzeuge erfassen bereits heute ihre Umgebung und können dabei auch Informationen über andere Personen verarbeiten. Smart Glasses rücken diese bereits bestehende Entwicklung besonders stark in den Fokus, schaffen die zugrunde liegenden Herausforderungen aber nicht erst.

Der Begriff Smart Glasses wird in der öffentlichen und regulatorischen Debatte häufig als Sammelbegriff verwendet. Tatsächlich verbergen sich dahinter jedoch sehr unterschiedliche Geräte – von Brillen mit Lautsprechern und Mikrofonen über kamerabasierte KI-Brillen bis hin zu Augmented- und Mixed-Reality-Systemen. Sie unterscheiden sich nicht nur in ihrer Bauform und ihren Funktionen, sondern auch darin, welche Daten sie aus ihrer Umgebung erfassen und wie diese verarbeitet werden.

Eine wichtige Unterscheidung ist daher, ob ein Gerät seine Umgebung überhaupt visuell erfasst, ob Bilder oder Töne gespeichert werden oder lediglich flüchtig für eine bestimmte Funktion verarbeitet werden und ob eine solche Erfassung für andere Personen erkennbar ist.

So lassen sich insbesondere folgende Gerätekategorien unterscheiden:

Kategorie	Technische Merkmale	Rechtliche Relevanz (ggf. für unterschiedliche Personen)
Smart Audio-Brillen (ohne Kamera)	Klassische Brillenbauform mit Lautsprechern und Mikrofonen; Telefonie, Musik, KI-Sprachassistenz. Keine Bilderfassung.	Ausschließlich Audioverarbeitung. Kamerabezogene Fragestellungen (Kennzeichnung, Recht am eigenen Bild, § 201a StGB) sind gegenstandslos; Sprach- und Umgebungsdaten können dennoch personenbezogen sein und DSGVO-Pflichten auslösen; das unbefugte Mitschneiden nicht öffentlich gesprochenen Wortes ist nach § 201 StGB strafbar.
Smart Glasses / AI Glasses (mit Kamera, ohne Display)	Klassische Brillenbauform mit nach vorn gerichteter Kamera und KI-Sprachassistenz. Keine Bildeinblendung. Auslösung durch Tastendruck, Sprachbefehl oder aktivierte Funktion.	Kern der aktuellen Diskussion in Deutschland. Maßgeblich ist der intendierte Zweck und die Unterscheidung zwischen gespeicherter Aufnahme und flüchtiger Verarbeitung. Bei Dritten offen kommunizierten

Kategorie	Technische Merkmale	Rechtliche Relevanz (ggf. für unterschiedliche Personen)
		Aufnahmen, etwa nicht abschaltbarer Aufnahme-LED und Manipulationserkennung, ist ein Gerät nicht als getarntes Aufnahmegerät im Sinne des § 8 TDDDG einzuordnen. Es fehlt bereits am Merkmal des Vortäuschens eines anderen Gegenstands sowie an der Bestimmung zum unbemerkten Aufnehmen (§ 8 Abs. 1, Abs. 2 TDDDG); hinzutreten können je nach Sachverhalt § 201a StGB sowie DSGVO-Pflichten.
Smart Glasses mit Display (Assisted Reality)	Zusätzliche Einblendung von Informationen in einem Ausschnitt des Sichtfelds – Benachrichtigungen, Navigation, Untertitel einer Live-Übersetzung. Nicht räumlich verankert.	Wie vorstehend; hinzu kommt die Verarbeitung, die zur Erzeugung der eingeblendeten Inhalte erforderlich ist. Diese zusätzlichen Verarbeitungen (z. B. Live-Übersetzung, Texterkennung) sind separat zu prüfen und lösen ggf. eigene Pflichten aus (z. B. unter der DSGVO, bei sensiblen Inhalten kann Art. 9 DSGVO einschlägig sein).
AR-Brillen (Augmented Reality)	Räumlich in der Umgebung verankerte virtuelle Inhalte; erfordert kontinuierliche Umgebungserfassung zur Positionsbestimmung (SLAM/Mapping).	Entscheidend ist, dass die Erfassung der Darstellung dient und nicht der Erstellung einer speicherbaren Aufnahme. Das SLAM/Mapping erzeugt jedoch räumliche Umgebungsdaten, die unter Umständen personenbezogen sein können; daraus folgen dann ggf. DSGVO-Pflichten. Auch Kennzeichnungspflichten der KI-VO können einschlägig sein.
VR-/MR-Headsets (XR-Devices)	Geschlossene Headsets; Umgebung wird vollständig ersetzt (VR) oder kameravermittelt durchgeblendet (Passthrough/MR).	Bauform und Trageszenario schließen eine unbemerkte Nutzung im öffentlichen Raum praktisch aus. Die Datenschutzpflichten bleiben dennoch bestehen: Eye- und Motion-Tracking können Art. 9 DSGVO berühren, z. B. wenn sie zur Identifizierung genutzt werden, Passthrough erfasst die Umgebung; eine DSFA nach Art. 35 DSGVO kann erforderlich sein.

Kategorie	Technische Merkmale	Rechtliche Relevanz (ggf. für unterschiedliche Personen)
Weitere Wearables	Smartwatches und Fitness-Tracker (Vital- und Standortdaten, regelmäßig ohne Kamera), intelligente Kopfhörer und Hearables, Ringe, Sensor-Textilien.	Schwerpunkt auf Gesundheits-, Vital- und Standortdaten; wobei es sich je nach Kontext um Daten besonderer Kategorien nach Art. 9 DSGVO handeln kann. Z. B. Gesundheitsdaten sind nur bei Vorliegen eines Tatbestands des Art. 9, Abs.2 DSGVO mit ausdrücklicher Einwilligung verarbeitbar; medizinische Zwecke können die MDR und KI-Auswertungen die KI-VO auslösen.

Die entscheidenden Unterscheidungsmerkmale sind nicht die Produktkategorie, sondern:

- (i) ob durch eine Funktion überhaupt eine Audio- oder Bilderfassung erfolgt,
- (ii) ob dies dem unbefugten Abhören oder der verdeckten Bildaufnahme anderer Personen oder einem anderen Zweck dient,
- (iii) ob eine Aufnahme dauerhaft gespeichert wird oder die Verarbeitung flüchtig zur Funktionserbringung dient und ob die erhobenen Daten ausschließlich für eigene Zwecke verarbeitet oder an Dritte übermittelt beziehungsweise öffentlich geteilt werden,
- (iv) ob, soweit das Abhören oder eine Aufnahme anderer Personen intendiert ist, dies offen erkennbar ist oder ob die besondere Bauform die Aufnahmefunktion verbirgt.

Die Weitergabe an Dritte oder öffentliche Zugänglichmachung von Aufnahmen ist rechtlich eigenständig zu bewerten – unabhängig vom aufnehmenden Gerät und nach ähnlichen Maßstäben, wie sie für Smartphone-Aufnahmen gelten.

Eine Regulierung, die an der Produktkategorie »Brille« ansetzt, statt an diesen Merkmalen, erfasst zwangsläufig auch Anwendungen ohne Privatsphärenrelevanz und lässt umgekehrt echte Umgehungsgeräte unberührt.

Die aktuelle Debatte um kamerabasierte Smart Glasses sollte deshalb nicht ohne Weiteres auf alle smarten Brillen oder Wearables übertragen werden. Umgekehrt können vergleichbare Fragestellungen auch bei ganz anderen Geräten entstehen, sobald diese ihre Umgebung über Kameras, Mikrofone oder andere Sensoren erfassen.

Kamera ist nicht gleich Aufnahme: Speichern oder verarbeiten?

Für die technische und rechtliche Einordnung smarter Geräte ist eine Unterscheidung zentral, die in der öffentlichen Debatte häufig zu kurz kommt: Eine Kamera kann

unterschiedliche Funktionen erfüllen. Nicht jede Nutzung einer Kamera zielt darauf ab, ein Foto oder Video zu erstellen und dauerhaft zu speichern.

Anwendungsfälle

Grundsätzlich lassen sich drei Anwendungsfälle unterscheiden:

- **Aktive Aufnahme:** Die nutzende Person erstellt bewusst ein Foto oder Video. Dabei entsteht eine Bild- oder Videodatei, die gespeichert und gegebenenfalls später angesehen oder geteilt werden kann. Funktional entspricht dies der Nutzung einer Smartphone-Kamera.
- **KI-gestützte Umgebungserfassung:** Die Kamera liefert visuelle Informationen, damit ein KI-System die Umgebung verstehen und eine konkrete Assistenzfunktion ausführen kann – etwa einen Text übersetzen, eine Speisekarte vorlesen oder Gegenstände erkennen. Zweck der Verarbeitung ist hier nicht die Erstellung eines Fotos oder Videos, sondern die gewünschte Assistenzleistung. Die Bildinformationen können dafür lediglich vorübergehend verarbeitet werden, ohne dass eine für die spätere Nutzung bestimmte Aufnahme entsteht.
- **Umgebungserfassung für AR:** Auch Augmented-Reality-Systeme müssen ihre Umgebung erfassen, um beispielsweise Räume, Flächen oder Gegenstände zu erkennen und digitale Inhalte räumlich korrekt zu positionieren. Kameras und andere Sensoren dienen dabei der Orientierung und der Verankerung virtueller Inhalte in der realen Welt, nicht zwangsläufig der Erstellung einer dauerhaften Bildaufnahme.

Beispiel: AR-Museumsrundgang

Eine Besucherin nutzt Smart Glasses während eines Museumsrundgangs. Die technische und rechtliche Bewertung unterscheidet sich je nach Funktion:

1. **Räumliche Verankerung der AR-Inhalte**
   Die Kamera und weitere Sensoren erfassen kurzzeitig Merkmale des Raums, etwa Wände, Bodenflächen oder markante Objekte, um digitale Inhalte räumlich korrekt darzustellen. Diese Informationen werden vorzugsweise auf dem Gerät verarbeitet. Es entsteht kein zur späteren Nutzung bestimmtes Foto oder Video. Personenbezogene Daten können gleichwohl anfallen und das Datenschutzrecht kann anwendbar sein, wenn unbeteiligte Besucherinnen und Besucher erfasst oder identifizierbar sind. Diese Daten sollten daher möglichst früh unkenntlich gemacht, gefiltert oder gelöscht werden.
2. **KI-gestützte Abfrage über einen Cloud-Dienst**
   Die Besucherin lässt sich ein Kunstwerk erklären oder ein fremdsprachiges Informationsschild übersetzen. Das Gerät erfasst hierfür kurzzeitig die erforderlichen Bildinformationen und übermittelt gegebenenfalls nur die für die Funktion notwendigen Daten an einen Cloud-Dienst. Die Antwort wird im Beispielsfall ausschließlich auf dem Gerät angezeigt; die Rohdaten werden nicht dauerhaft gespeichert und nicht für andere Zwecke, etwa das Training von KI-Modellen, verwendet. Auch hier gilt: Werden Personen erfasst, kann eine

Verarbeitung datenschutzrechtlich relevant sein, auch wenn sie nur flüchtig erfolgt.

3. **Bewusst ausgelöste Foto- oder Videoaufnahme**
   Die Besucherin erstellt ein Foto vor einem Kunstwerk oder zeichnet ein kurzes Video auf. Anders als bei den ersten beiden Funktionen entsteht eine dauerhaft speicherbare Aufnahme. Diese kann später angesehen, gespeichert oder geteilt werden. Für diese Funktion kann eine Aufnahmeanzeige gegenüber Umstehenden erforderlich sein, etwa durch ein verlässliches, schwer übergehbares Aufnahmesignal.

Das Beispiel zeigt: Nicht die bloße Existenz einer Kamera entscheidet über die rechtliche Bewertung, sondern welche Daten verarbeitet werden, zu welchem Zweck, ob sie das Gerät verlassen, wo sie gespeichert oder protokolliert werden und wann sie gelöscht werden.

Die Unterscheidung zwischen Erfassung, Verarbeitung und Speicherung sowie Weitergabe und Übermittlung ist deshalb wesentlich. Ein Gerät kann Bildinformationen verarbeiten, ohne daraus ein dauerhaft gespeichertes Foto oder Video zu erzeugen. Auch eine Übermittlung an Dritte oder eine öffentliche Teilung ist rechtlich eigenständig zu betrachten, unabhängig davon, ob eine dauerhafte Speicherung auf dem Gerät erfolgt. Gleiches gilt grundsätzlich für andere Sensoren: Umgebungslicht-, Bewegungs- oder Abstandssensoren erfassen fortlaufend Signale, ohne dadurch eine klassische »Aufnahme« zu erstellen.

Für die Debatte um Smart Glasses und weitere smarte Devices ist diese Differenzierung besonders wichtig: Ob eine Person mit ihrem Device bewusst ein Video aufzeichnet oder ob die Kamera für wenige Augenblicke ein Schild erfasst, um dessen Text zu übersetzen, sind nicht allein wegen der Dauer, sondern vor allem wegen des Verarbeitungszwecks, der Datenminimierung, der Speicherung und einer möglichen Weitergabe technisch und rechtlich unterschiedliche Vorgänge mit unterschiedlichen potenziellen Auswirkungen auf die Privatsphäre. Die Dauer der Erfassung kann dabei ein Indiz sein, ersetzt aber keine eigenständige Bewertung von Zweck, Speicherung und Weitergabe. Eine sachgerechte Bewertung sollte daher nicht allein daran anknüpfen, dass eine Kamera vorhanden oder aktiv ist, sondern daran, was sie erfasst, zu welchem Zweck die Daten verarbeitet werden, ob daraus eine dauerhafte Aufnahme entsteht und ob sowie an wen die Daten übermittelt oder öffentlich geteilt werden.

Rechtliche Einordnung der Unterscheidung

Diese Unterscheidung ist rechtlich erheblich: Das Interesse Umstehender richtet sich auf die Frage, ob eine Aufnahme entsteht, die gespeichert und an Dritte übermittelt bzw. öffentlich geteilt werden kann, und zu welchem Zweck dies geschieht. Wer sich eine Speisekarte übersetzen lässt, erstellt keine solche Aufnahme. Die Erwartbarkeit der Verarbeitung im Sinne der Abwägung nach Art. 6 Abs. 1 lit. f DSGVO und der Schutzzweck möglicher Kennzeichnungspflichten setzen daher an unterschiedlichen Punkten an.

Aus datenschutzrechtlicher Sicht bedeutet dies allerdings nicht, dass eine lediglich flüchtige Verarbeitung grundsätzlich irrelevant wäre. Sobald das Datenschutzrecht

einschlägig ist und sich die verarbeiteten Informationen auf identifizierte oder identifizierbare Personen beziehen, fällt auch eine Verarbeitung ohne dauerhafte Speicherung unter die DSGVO, denn der Verarbeitungsbegriff des Art. 4 Nr. 2 DSGVO setzt keine Speicherung voraus. Für eine Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO sind unter anderem der konkrete Verarbeitungszweck, die Erforderlichkeit sowie die vernünftigen Erwartungen betroffener Personen relevant.

Haushaltsausnahme bei privater Nutzung

Für rein persönliche oder familiäre Tätigkeiten kann allerdings die Haushaltsausnahme nach Art. 2 Abs. 2 lit. c DSGVO greifen. Typische Anwendungsfälle sind etwa familiäre Urlaubsschnappschüsse oder private Familienaufnahmen, die ausschließlich für private Zwecke erstellt und gegebenenfalls einem begrenzten Kreis von Freunden oder Familienangehörigen gezeigt werden.[1] Dass dabei unbeteiligte Dritte sichtbar werden oder die Aufnahme im öffentlichen Raum erfolgt, schließt die Haushaltsausnahme nicht automatisch aus. Die Ausnahme ist jedoch nicht zu weit auszulegen. Sie greift regelmäßig nicht, wenn Aufnahmen im Internet einer unbestimmten Vielzahl von Personen zugänglich gemacht, für berufliche, kommerzielle oder sonstige nicht rein private Zwecke verwendet oder dauerhaft und systematisch nach außen gerichtet erhoben werden.

Bewertung nach §8 TDDDG

Auch für § 8 TDDDG ist die konkrete Funktion entscheidend. Die Vorschrift knüpft daran an, ob eine Telekommunikationsanlage ihrer Form nach einen anderen Gegenstand vortäuscht oder mit Gegenständen des täglichen Gebrauchs verkleidet ist und aufgrund dieser Umstände oder ihrer Funktionsweise in besonderer Weise geeignet und dazu bestimmt ist, das nicht öffentlich gesprochene Wort oder das Bild einer anderen Person unbemerkt abzuhören beziehungsweise aufzunehmen.

KI-Funktionen, die etwa der Übersetzung von Texten oder der Analyse von Objekten dienen, sind typischerweise nicht auf die Aufnahme von Personen gerichtet und daher für die Zweckbestimmung nach § 8 TDDDG nicht ausschlaggebend. Eine pauschale Gleichsetzung jeder kamerabasierten Umgebungserfassung mit einer solchen Aufnahme greift daher zu kurz; maßgeblich ist die konkrete Ausgestaltung und Zweckbestimmung der Funktion.

Liegt eine Aufnahme vor, gilt nach § 8 Abs. 2 TDDDG eine Anlage insbesondere dann als zum unbemerkten Aufnehmen bestimmt, wenn die Aufnahmefunktion beim bestimmungsgemäßen Gebrauch für Betroffene nicht eindeutig erkennbar ist. Genau diese Erkennbarkeit kann etwa durch ein LED-Signal hergestellt werden. Dies hat die Bundesnetzagentur in ihren Hinweisen zu § 8 TDDDG bestätigt.

Bei der Bewertung der Erkennbarkeit kann auch die allgemeine Verkehrsanschauung relevant sein. Ob eine Aufnahmefunktion für Betroffene erkennbar ist, hängt nicht allein davon ab, ob ein technisches Merkmal unmittelbar sichtbar ist. Vielmehr kann auch die allgemein bekannte Funktionsweise eines Geräts eine Rolle spielen:

[1] EDSA, Erklärung 1/2026 zu Smart Glasses, angenommen am 13. Oktober 2026, Rn. 13–18, ↗hier abrufbar.

Bei Smartphones ist heute allgemein bekannt, dass sie Fotos und Videos aufnehmen können. Vergleichbare Erwartungen können sich mit der Verbreitung neuer Gerätetypen entwickeln. Die konkrete Ausgestaltung des Geräts, sein Nutzungszweck und die tatsächliche Wahrnehmbarkeit einer laufenden Aufnahme bleiben jedoch zentrale Beurteilungsmaßstäbe.

Ob die Brille insgesamt als getarntes Aufnahmegerät im Sinne des § 8 TDDDG einzustufen ist, bemisst sich nach einer Gesamtbetrachtung ihrer äußeren Erscheinungsform, ihrer Funktionsweise, ihrer Vermarktung und ihrer tatsächlichen Zweckbestimmung. Maßgeblich ist insbesondere, ob das Gerät aufgrund seiner Tarnung oder Funktionsweise in besonderer Weise geeignet und dazu bestimmt ist, das nicht öffentlich gesprochene Wort oder das Bild einer anderen Person unbemerkt abzuhören beziehungsweise aufzunehmen. Nach § 8 Abs. 2 TDDDG gilt eine Anlage insbesondere dann als zum unbemerkten Aufnehmen bestimmt, wenn ihre Aufnahmefunktion beim bestimmungsgemäßen Gebrauch für Betroffene nicht eindeutig erkennbar ist.

Eine Mehrzweckfunktion schließt die Anwendung des § 8 TDDDG nicht bereits abstrakt aus. Entscheidend ist, ob das Gerät nach seiner Bestimmung gerade zum heimlichen Aufnehmen bestimmt ist. Dabei können sowohl die durch den Hersteller vorgesehene Ausgestaltung und Vermarktung als auch die konkreten Umstände des jeweiligen Einsatzes relevant sein.

Eine objektiv erkennbare, überwiegend auf andere anerkennenswerte Zwecke gerichtete Ausgestaltung und Vermarktung spricht dagegen, dass das Gerät gerade zur unbemerkten Aufnahme bestimmt ist. Eine bloße Zweckentfremdung durch die nutzende Person begründet für sich genommen jedoch keine abweichende Bewertung des Geräts.

Sensorik ist nicht automatisch Aufnahme

Erforderlich ist außerdem eine Unterscheidung zwischen Sensorik und Aufnahme. Nicht jede sensorische Erfassung ist eine Aufnahme im Sinne des allgemeinen Sprachgebrauchs: Ein Umgebungslichtsensor, ein Beschleunigungssensor oder die Erkennung eines Aktivierungsworts verarbeiten Signale, ohne ein speicherbares Abbild zu erzeugen. Eine Regulierung, die pauschal an das Vorhandensein von Sensoren anknüpft, verfehlt daher ihr Schutzziel.

Diese Unterscheidung betrifft jedoch allein die aufnahme- und kennzeichnungsbezogenen Normen wie § 201a StGB und § 8 TDDDG; datenschutzrechtlich können Sensordaten personenbezogene Daten sein, wenn sie Informationen über eine Person beinhalten (Art. 4 Nr. 1 DSGVO). Die Frage, ob und auf welcher Rechtsgrundlage ihre Verarbeitung zulässig ist, stellt sich dann gesondert, insbesondere nach Art. 6 DSGVO.

3 Zentrale Herausforderungen für die Privatsphäre und datenschutzrechtliche Anforderungen

Umfassende Datenerfassung

Smarte Technologien, insbesondere mit Kameras und Mikrofonen, erheben und verarbeiten nicht nur personenbezogene Daten der Trägerin oder des Trägers, sondern auch und gerade Daten von unbeteiligten Dritten.

Außerhalb der Haushaltsausnahme der DSGVO ist die Verarbeitung personenbezogener Daten jedoch nur zulässig, wenn eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO vorliegt.

Smarte Technologien wirken zunehmend im Verbund: Brille und Smartwatch teilen Benachrichtigungen, Wearables greifen auf Smart-Home- und Fahrzeugfunktionen zu, Gesundheitsdaten laufen in Plattformdiensten zusammen. Dadurch werden insgesamt mehr Daten erhoben, kombiniert und ausgewertet. Die maßgebliche Frage verschiebt sich damit von »welches Gerät erhebt welche Daten« hin zu »welche Zwecke sind zulässig, wie lange werden Daten gespeichert und wer erhält Zugriff«. Eine gerätezentrierte Regulierung greift diese Entwicklung nicht auf; ein zweck- und risikobezogener Ansatz ist geeigneter und zugleich technologieneutral.

Neben der DSGVO können auch Vorschriften des TDDDG einschlägig sein. Nach § 25 Abs. 1 TDDDG bedarf es insbesondere dann einer Einwilligung des Endnutzers oder der Endnutzerin, wenn Informationen in dessen Endeinrichtung gespeichert oder Informationen ausgelesen werden, die dort bereits gespeichert sind und dies nicht zur Bereitstellung des in Anspruch genommenen Dienstes erfolgt. Dies kann etwa relevant werden, wenn Smart Glasses auf Informationen eines gekoppelten Smartphones, einer Smartwatch oder eines anderen Endgeräts zugreifen oder dort Daten speichern und dies nicht für den in Anspruch genommenen Dienst erforderlich ist. Die Einwilligung nach § 25 TDDDG ist von der Rechtsgrundlagenprüfung nach Art. 6 DSGVO sowie von der Bewertung nach § 8 TDDDG zu unterscheiden. Eine weitere Ausnahme greift ein, wenn die Speicherung oder der Zugriff allein der Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz dient.

Relevante Rechtsgrundlagen können z. B. die folgenden sein:

- Einwilligung (Art. 6 Abs. 1 lit. a DSGVO): Eine wirksam erteilte Einwilligung nach Art. 4 Nr. 11 DSGVO könnte eine Rechtsgrundlage bilden. Für gezielte Aufnahmen und Verarbeitungen aus dem privaten Umfeld, für die das Datenschutzrecht ausnahmsweise greift, kann das ggf. sichergestellt werden. Im öffentlichen Raum

ist es dagegen regelmäßig praktisch nicht möglich, die Einwilligung sämtlicher Personen einzuholen, die etwa beim Spaziergang über eine Straße potenziell erfasst werden.

- Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO): Die Aufzeichnung unbeteiligter Dritter kann trotzdem zulässig sein, wenn Trägerinnen und Träger der Smart Glasses ein berechtigtes Interesse an der Verarbeitung haben, die Verarbeitung zur Verwirklichung dieses Interesses erforderlich ist und dem keine überwiegenden Interessen, Grundrechte oder Grundfreiheiten der betroffenen Personen entgegenstehen. Die Informationspflichten richten sich nach der Erhebungssituation. Bei unmittelbarer Erhebung bei der betroffenen Person gilt grundsätzlich Art. 13 DSGVO, bei Erhebung aus anderer Quelle gilt grundsätzlich Art. 14 DSGVO, dessen Informationen regelmäßig unter den Voraussetzungen und Fristen des Art. 14 Abs. 3 DSGVO bereitgestellt werden müssen, vorbehaltlich der Ausnahmen in Art. 14 Abs. 5 DSGVO. Die Informationen sind in einer dem Nutzungskontext angemessenen Weise bereitzustellen**.** Nach der Rechtsprechung des EuGH kann eine Verarbeitung auf Art. 6 Abs. 1 lit. f DSGVO nicht gestützt werden, wenn das konkrete berechtigte Interesse nicht rechtzeitig mitgeteilt wird.[2]

Für die Abwägung nach Art. 6 Abs. 1 lit. f DSGVO ist der Verwendungszweck konstitutiv; sein Gewicht ergibt sich erst aus dem konkreten Anwendungskontext.

Typische Einsatzfelder verdeutlichen, warum eine pauschale Bewertung nicht möglich ist. Smart Glasses können etwa Menschen mit Seh- oder Hörbeeinträchtigungen beim Vorlesen von Texten, bei der Orientierung oder beim Verstehen von Gesprächen unterstützen. Weitere Funktionen betreffen die Übersetzung fremdsprachiger Texte und Gespräche, die freihändige Kommunikation sowie Anwendungen, bei denen beide Hände benötigt werden, etwa beim Radfahren, Wandern, Handwerken oder Kochen. Im beruflichen Umfeld können Smart Glasses darüber hinaus für Fernunterstützung, Arbeitsanleitungen, Dokumentation und Prozessunterstützung eingesetzt werden. Schließlich können sie, vergleichbar mit Smartphones oder Kameras, der persönlichen Dokumentation von Reisen, Feiern oder Sportereignissen dienen.

Diese Beispiele zeigen, dass sich das Gewicht eines möglichen berechtigten Interesses erst aus dem konkreten Verwendungszweck, dem Erfassungskontext, der Datenminimierung sowie einer etwaigen Speicherung oder Weitergabe ergibt. Sie begründen für sich genommen weder ein berechtigtes Interesse noch die Anwendbarkeit der Haushaltsausnahme. Insbesondere ist die Haushaltsausnahme nach Art. 2 Abs. 2 lit. c DSGVO auf ausschließlich persönliche oder familiäre Tätigkeiten beschränkt; sie kann etwa private Urlaubsaufnahmen erfassen, auch wenn dabei unbeteiligte Personen sichtbar werden oder die Aufnahme im öffentlichen Raum erfolgt. Sie greift jedoch regelmäßig nicht, wenn Aufnahmen einer unbestimmten Vielzahl von Personen im Internet zugänglich gemacht, für berufliche, kommerzielle oder sonstige nicht rein private Zwecke verwendet oder systematisch zur Beobachtung der Umgebung eingesetzt werden.

[2] EuGH, Urt. v. 9. Januar 2025 – C-394/23, Rn. 46.

Barrierefreiheit als verbindlicher Prüfungsmaßstab

Kamerabasierte Assistenzfunktionen sind für blinde und sehbeeinträchtigte Menschen kein Komfortmerkmal, sondern erschließen Informationen, die anders nicht zugänglich sind. Daraus folgt eine Konsequenz für jede Verhältnismäßigkeitsprüfung: Nutzungsbeschränkungen ohne Ausnahmeregelung, die an der Gerätekategorie ansetzen, treffen faktisch zuerst Menschen mit Behinderungen, weil ihnen die Ausweichmöglichkeit auf ein anderes Gerät häufig fehlt. Dieser Gesichtspunkt ist bei jeder Erwägung von Beschränkungen von Anfang an zu berücksichtigen und nicht erst auf der Rechtfertigungsebene nachzuholen.

Aufklärung und Produktgestaltung statt Produktverbot

Zwischen unregulierter Nutzung und einem Verbot einer Produktkategorie liegen vier sich ergänzende Instrumente:

- erstens technologieneutrale Regelungen, die, soweit Regelungsbedarf besteht, an der schädlichen Handlung ansetzen, etwa bei heimlichen Aufnahmen, digitalem Voyeurismus oder bildbasierter sexualisierter Gewalt, statt an einer einzelnen Produktkategorie;
- zweitens Aufklärung und Medienkompetenz, also Verhaltensleitfäden, Hinweise zur Einrichtung und Nutzung sowie Angebote für Eltern und Erziehende, die im Rahmen der Selbstregulierung entstehen können;
- drittens die konsequente Durchsetzung des bestehenden Rechts gegen Fehlverhalten Einzelner;
- viertens die Produktgestaltung, die zwischen Funktionen differenzieren und dort, wo rechtlich erforderlich oder angemessen, Transparenz technisch unterstützen kann, statt dies allein dem Verhalten der Nutzenden zu überlassen.

Die zugrunde liegenden Privatsphärenfragen sind, wie in Kapitel 3 dargelegt, nicht neu – wohl aber die Chance, sie erstmals zugleich technisch und normativ zu adressieren.

Standort- und Wertschöpfungsperspektive berücksichtigen.

Smarte Technologien sind kein Feld, auf dem Europa nur Absatzmarkt ist. Insbesondere Hardwarebauteile wie Optik, Displaytechnologie, Sensorik, Halbleiter und die zugehörige Forschung sind in Deutschland und Europa vertreten, und der stationäre Fachhandel ist Teil der Wertschöpfung. Regulatorische Unsicherheit trifft daher nicht allein global tätige Anbieter, sondern in besonderem Maße mittelständische Hersteller, Importeure und den Handel, die Geräte im Vertrauen auf eine behördliche Bewertung in Verkehr bringen. Eine Debatte, die auf das Verbot einer einzelnen Produktkategorie zuläuft, erzeugt diese Unsicherheit für das gesamte Ökosystem – während ein zweck- und risikobezogener Ansatz sowohl das Schutzniveau als auch die Planbarkeit erhöht.

Transparenz und Information

Eine gesetzliche Pflicht zu optischen oder akustischen Aufnahmesignalen besteht nicht; weder § 8 TDDDG noch die DSGVO schreiben eine solche Signalisierung vor. Daraus folgt jedoch nicht, dass keine Informationspflichten bestehen: Soweit die DSGVO anwendbar ist, sind auch die jeweils einschlägigen Transparenz- und Informationspflichten zu prüfen. Zudem ist die Erkennbarkeit einer Aufnahmefunktion nach § 8 Abs. 2 TDDDG ein maßgebliches Kriterium dafür, ob ein Gerät als zum heimlichen Aufnehmen bestimmt gilt. Die folgenden Angaben beschreiben die Signale und Schutzmechanismen, über die derzeit am Markt erhältliche Smart Glasses mit Kamera nach Herstellerangaben verfügen.

- Bei den hier beschriebenen derzeit marktüblichen Produkten signalisiert eine Aufnahme-LED an der Vorderseite jede Aufnahme, die in die Galerie der nutzenden Person gespeichert werden kann: bei Fotos kurz, bei Videos für die Dauer der Aufnahme. Sie ist nicht abschaltbar. Eine Manipulationserkennung deaktiviert bei diesen Produkten die Kamera, wenn die LED verdeckt wird; nach Herstellerangaben wird die Erkennung auf physische Beschädigung oder Zerstörung der LED erweitert.
- Bei den hier beschriebenen derzeit marktüblichen Produkten werden Kamera und Mikrofon durch eine bewusste Nutzerhandlung aktiviert. Ob und in welchem Umfang Mikrofon- oder Sprachassistentenfunktionen personenbezogene Daten verarbeiten oder Aufnahmen erstellen, hängt von der jeweiligen Funktion und Konfiguration ab.

Auch die folgende Einordnung ist rein beschreibend. Die genannten technischen Merkmale können die Erkennbarkeit einer Aufnahme unterstützen; sie stellen jedoch keine abschließende Bewertung dar, ob die Aufnahmefunktion im konkreten Fall hinreichend erkennbar ist. Damit erreichen diese Geräte ein Transparenzniveau, das bei vergleichbaren Kameraprodukten wie Smartphones, Action- und Helmkameras, Dashcams, Video-Türklingeln oder vernetzten Fahrzeugen nicht in jeder Hinsicht gegeben ist. Allerdings sind viele dieser Produkte von ihrer ursprünglichen Funktion her gerade auf die Erstellung von Bild- oder Videoaufnahmen ausgerichtet. Ihre Aufnahmefunktion ist daher typischerweise unmittelbar sichtbar und bedarf gegebenenfalls keiner zusätzlichen verdeckungsbezogenen Kennzeichnung; dieser Unterschied darf bei einem Vergleich der Transparenzniveaus nicht ausgeblendet werden. Maßgeblich bleibt in jedem Fall die Erkennbarkeit der Aufnahmefunktion im konkreten Nutzungskontext. Für die Bewertung nach § 8 TDDDG ist dies der maßgebliche Anknüpfungspunkt: Die Norm zielt auf Geräte, deren Aufnahmefunktion bei bestimmungsgemäßem Gebrauch durch die Bauform gerade verborgen werden soll. Die genannten Signale sind insoweit der derzeitige tatsächliche Anknüpfungspunkt und treffen keine Aussage darüber, welche Signalisierung künftig erforderlich oder wünschenswert wäre.

Sicherheitsaspekte

Durch die Nutzung von Smarttechnologie können auch Sicherheitsinteressen tangiert werden. Dies kann sowohl militärische wie auch Sicherheitsinteressen im zivilen, privaten Kontext umfassen.

Militärische Interessen
Sicherheitsrelevante Bereiche sind bereits heute überwiegend handlungs- und ortbezogen geregelt, etwa durch Hausrecht, Zugangs- und Fahrzeugkontrollen sowie Foto-, Film- und Überflugverbote. Diese Instrumente gelten grundsätzlich unabhängig von der jeweiligen Gerätekategorie und können auch auf Smart Glasses und andere smarte Technologien angewendet werden. So gilt in militärischen Sicherheitsbereichen der Bundeswehr beispielsweise ein grundsätzliches Film- und Fotografierverbot mit Erlaubnisvorbehalt; die jeweiligen Standorte können die Maßnahmen lageabhängig anpassen.[3]

Beruflicher und institutioneller Einsatz

Smart Glasses, bei denen sowohl Video- als auch Sprachaufnahmen erstellt werden, können auch sicherheitsrechtliche Aspekte tangieren, sei es in sicherheitskritischen Umgebungen oder hinsichtlich vertraulicher Informationen wie bei Berufsgeheimnisträgern. Hier können unbemerkte Video- oder Bildaufnahmen mit oder ohne Ton sowie reine Tonaufnahmen seitens von Unternehmen, öffentlichen Stellen und anderen Einrichtungen auch unabhängig von Persönlichkeitsinteressen der betroffenen Personen unerwünscht sein.

Demgegenüber stehen die Interessen einer Nutzung zur Ermöglichung einer barrierefreien Teilnahme am beruflichen oder gesellschaftlichen Leben. Die folgenden Aspekte sollen dabei Orientierung geben.

Wahrnehmung des Hausrechts
Um Beeinträchtigungen durch den Einsatz von Smart Glasses auszuschließen, können öffentliche Stellen und Unternehmen aber auch in der Rolle als »Hausherren« und Arbeitgeber auf das Hausrecht zurückgreifen, da sie selbst vorgeben können, in welchen Bereichen und durch wen fotografiert werden darf. Dies kann auch auf die jeweiligen Mittel begrenzt werden, sodass sichergestellt wird, dass die jeweils erforderliche Transparenz gewahrt wird.

Ein Verstoß gegen eine klar beschlossene und kommunizierte Regelung kann dann zu entsprechenden Maßnahmen bzw. Konsequenzen hinsichtlich des Verstoßes durch Besucher bzw. Beschäftigte führen.

Berufsgeheimnisträger
Gerade bei Berufsgeheimnisträgern kann die Verwendung von Smart Glasses durch Berufsgeheimnisträger oder Kunden/Mandanten/Patienten im direkten Austausch oder z. B. im Wartezimmer zu Beeinträchtigungen der Vertraulichkeit führen. Einrichtungen können hierauf mit handlungs- und ortsbezogenen Regelungen

[3] ↗Bundeswehr, 2026.

reagieren, etwa durch Hausrecht, Hinweise zu zulässigen Nutzungsformen sowie Verbote unerlaubter Aufnahmen.

Solche Regelungen sollten an der konkreten Handlung ansetzen, insbesondere an unbefugten Aufzeichnungen, und nicht pauschal an der Gerätekategorie. Bei assistiven Nutzungskonstellationen, etwa zur Unterstützung von Menschen mit Beeinträchtigungen der Seh- oder Hörfähigkeit, sollten angemessene Ausnahmen oder alternative Lösungen vorgesehen werden.

Wartungspartner/technische Dienstleister
Wie soll damit umgegangen werden, wenn Personal von (technischen) Dienstleistern Smart Glasses einsetzen möchte, um beispielsweise komplexe Wartungssituationen mit externer Hilfe zu bewältigen? Dazu sollte bereits bei der Beauftragung eine Regelung getroffen werden, die je nach sicherheitskritischer Umgebung entsprechend ausgestaltet sein kann.

Kollektivrechtliche Regelungen
Hinsichtlich des Einsatzes bzw. des Ausschlusses der Nutzung im dienstlichen Kontext empfiehlt es sich, die jeweiligen Betriebspartner einzubeziehen.

Diskriminierungsfreie Regelungen
Smart Glasses können bei körperlichen Einschränkungen (z. B. bei Seh- oder Hörproblemen) eine berufliche oder gesellschaftliche Teilnahme ermöglichen. Ein denkbarer Zielkonflikt kann dahingehend minimiert werden, dass aufgrund klarer, transparenter Regelungen die Verwendung auch in sicherheitskritischen oder vertrauenswürdigen Situationen durch eine Einzelfreigabe gestattet wird. Dabei sollten Speicherort, Zugriffsrechte und Aufbewahrungsfristen vertraglich und technisch klar festgelegt werden; pauschale Ausschlüsse der Cloud-Verarbeitung sind nicht erforderlich, wenn geeignete Garantien bestehen.

Datenschutzrechtliche Bewertung bei Verstoß
Je nach Ausgestaltung der Nutzung können Beschäftigte im Einzelfall selbst datenschutzrechtlich verantwortlich sein, insbesondere wenn sie Smart Glasses eigenständig für eigene Zwecke einsetzen und dabei über Zweck und Mittel der Verarbeitung entscheiden. Die Rollenverteilung zwischen nutzender Person, Arbeitgeber und Anbieter richtet sich nach der tatsächlichen Entscheidung über Zwecke und Mittel der Verarbeitung.

Ob eine gemeinsame Verantwortlichkeit nach Art. 26 Abs. 1 DSGVO in Verbindung mit Art. 4 Nr. 7 DSGVO vorliegt, richtet sich danach, ob die beteiligten Stellen gemeinsam die Zwecke und Mittel derselben Verarbeitung festlegen. Eine gemeinsame Verantwortlichkeit folgt nicht allein daraus, dass personenbezogene Daten an einen Dienst des Anbieters übermittelt werden. Liegt eine gemeinsame Festlegung von Zwecken und Mitteln nicht vor, kommen je nach konkreter Ausgestaltung eine getrennte Verantwortlichkeit oder eine Auftragsverarbeitung in Betracht. Bei einer Auftragsverarbeitung verarbeitet der Anbieter die Daten ausschließlich nach dokumentierten Weisungen des Verantwortlichen; verfolgt er eigene Zwecke, ist er für diese Verarbeitung eigenständiger Verantwortlicher.

Beschäftigte, die personenbezogene Daten dagegen im Rahmen ihrer dienstlichen Tätigkeit und auf Weisung des Arbeitgebers verarbeiten, sind grundsätzlich keine

eigenen Verantwortlichen, sondern handeln unter der Verantwortung des Arbeitgebers gemäß Art. 29 DSGVO.

Verantwortlichkeit, mögliche Rechtsfolgen und geeignete organisatorische und technische Maßnahmen sind stets anhand des konkreten Einzelfalls zu prüfen. Arbeitgeber sollten klare interne Regeln für die Nutzung von Smart Glasses festlegen, Beschäftigte sensibilisieren und Schulen sowie geeignete und datenschutzkonforme Werkzeuge für legitime Anwendungsfälle bereitstellen.

Datenschutzaufsichtsbehörden können bei Verstößen gegen die DSGVO aufsichtsrechtliche Maßnahmen ergreifen und unter den Voraussetzungen des Art. 83 DSGVO Geldbußen verhängen. Arbeitgeber können ihre Position verbessern, wenn sie nachweisen können, dass sie angemessene technische und organisatorische Maßnahmen umgesetzt haben, etwa verbindliche Nutzungsregeln, Schulungen, Freigabeprozesse, Zugriffsbeschränkungen und Kontrollmechanismen. Dies schließt eine Verantwortlichkeit oder Haftung jedoch nicht automatisch aus.

Das Bedürfnis, beispielsweise Besprechungen zu transkribieren, kann auch durch zentral bereitgestellte Tools des Arbeitgebers erfüllt werden. Dabei sollte der Arbeitgeber insbesondere die Rechtsgrundlage, die Information der Beschäftigten und sonstigen Betroffenen, die Zweckbindung, Löschfristen, Zugriffsrechte, die Einbindung von Dienstleistern sowie gegebenenfalls die Übermittlung in Drittländer prüfen und die Einhaltung der datenschutzrechtlichen Anforderungen organisatorisch und technisch sicherstellen.

4 Handlungsempfehlungen

Smart Glasses und andere smarte Technologien stellen Datenschutz und Privatsphäre nicht vor völlig neue Grundsatzfragen. Viele Herausforderungen sind bereits von Smartphones, Kameras, Dashcams oder anderen sensorbasierten Geräten bekannt. Neu sind vor allem die stärkere Vernetzung, die zunehmende Kontextsensitivität und die Möglichkeit, Schutzmechanismen unmittelbar technisch umzusetzen.

Maßgeblich sollte deshalb nicht die Produktkategorie sein, sondern welche Daten ein System erfasst, zu welchem Zweck dies geschieht, ob Informationen nur verarbeitet oder dauerhaft gespeichert werden, welche Schlüsse daraus gezogen werden und wer anschließend Zugriff auf die Daten erhält. Ebenso wichtig ist die Unterscheidung zwischen einer bewussten Aufnahme und einer lediglich vorübergehenden sensorischen Verarbeitung für Assistenz-, KI- oder AR-Funktionen. Relevant für die jeweilige Bewertung wird die Umsetzung der Anforderungen an eine ausreichende Transparenz der durchgeführten Nutzung sein.

Für Anbieter

Der Begriff »Anbieter« umfasst unterschiedliche Akteure mit unterschiedlichen technischen und rechtlichen Handlungsmöglichkeiten. Dazu gehören insbesondere Hardware- und Betriebssystemhersteller, App-Anbieter, Cloud-Diensteanbieter sowie institutionelle Betreiber, die Smart Glasses etwa als Leihgeräte, Arbeitsmittel oder für Besucherangebote bereitstellen. Nicht jede Schutzmaßnahme kann von jedem Akteur allein umgesetzt werden. Die folgenden Empfehlungen richten sich daher an diejenigen Akteure, die die jeweilige Funktion technisch gestalten, bereitstellen oder betreiben. Die technische Zuordnung ergänzt, ersetzt aber nicht die im Einzelfall vorzunehmende datenschutzrechtliche Prüfung der Rollen und Verantwortlichkeiten.

Privacy by Design, Datenminimierung und Privacy Enhancing Technologies (PETs) konsequent umsetzen

Datenschutz sollte bereits in der technischen Architektur eines Produkts verankert sein. Da leichte Smart Glasses in der Praxis engen Grenzen bei Baugröße, Akkulaufzeit und Wärmeentwicklung unterliegen, können Anbieter eine Verarbeitung auf dem Gerät (On-Device Processing) mit cloudbasierten Trusted Execution Environments (TEEs) kombinieren, wo dies aus Produktsicht sinnvoll ist.

Erstens könnten identifizierende Merkmale unbeteiligter Dritter, etwa Gesichter in Videobildern oder Hintergrundstimmen, bereits auf dem Gerät oder einem gekoppelten Smartphone unkenntlich gemacht, gefiltert oder sonst wie reduziert werden, bevor Daten das Gerät verlassen.

Zweitens kann in Fällen, in denen Cloud-Rechenleistung etwa für eine Echtzeit-KI-Funktion erforderlich ist, die Verarbeitung in einer cloudbasierten TEE erfolgen. Eine TEE ist eine isolierte, kryptografisch abgesicherte Verarbeitungsumgebung, die den Schutz der Vertraulichkeit und Integrität von Daten während der Verarbeitung unterstützen kann. Sie kann insbesondere dazu beitragen, den Zugang des Cloud-Anbieters zu den verarbeiteten Bild- oder Audiodaten technisch einzuschränken.

TEEs ersetzen jedoch die datenschutzrechtliche Bewertung nicht vollständig. Welche Schutzmaßnahmen technisch umsetzbar sind, hängt von der jeweiligen Rolle ab: Hardware- und Betriebssystemhersteller können insbesondere lokale Verarbeitung, Sensorkontrolle, Signalisierung und Sicherheitsarchitektur gestalten; App-Anbieter können Datenminimierung, Zweckbindung, Zugriffs- und Löscheinstellungen umsetzen; Cloud-Diensteanbieter können Verarbeitungsumgebungen, Zugriffskontrollen, Protokollierung und Löschkonzepte bereitstellen. Die beteiligten Akteure sollten die erforderlichen Schnittstellen, Dokumentationen und Nachweise so bereitstellen, dass institutionelle Betreiber und Arbeitgeber die Datenschutz- und Sicherheitslage ihrer konkreten Nutzung bewerten können.

Die jeweiligen Schutzmaßnahmen sollten an der konkreten Funktion und der Rolle des beteiligten Akteurs ausgerichtet sein. Hardware- und Betriebssystemhersteller sollten insbesondere sicherstellen, dass sensible Funktionen deaktivierbar sind, Aufnahmen zuverlässig signalisiert werden und lokale Verarbeitung technisch möglich ist, wo dies funktional sinnvoll ist. App-Anbieter sollten Datenverarbeitung auf den erforderlichen Zweck beschränken, identifizierende Merkmale unbeteiligter Personen möglichst früh

entfernen oder reduzieren sowie klare Einstellungen zu Speicherung, Übermittlung, Zugriff und Löschung bereitstellen. Cloud-Diensteanbieter sollten rohe Bild- und Audiodaten nur für die konkrete Funktion verarbeiten, eine kurze oder keine dauerhafte Speicherung vorsehen, Zugriffe technisch beschränken und eine Verwendung für Sekundärzwecke oder das Training von KI-Modellen nur nach einer eigenständigen datenschutzrechtlichen Prüfung ermöglichen.

Wo relevant, sollten Anbieter prüfen, ob ihre Geräte so gestaltet werden könnten, dass Nutzende eventuelle datenschutzrechtliche Anforderungen praktisch umsetzen können; dies gilt insbesondere für Transparenz, Einwilligung, Zweckbindung, Datenminimierung und die Vermeidung heimlicher Aufnahmen. Wo lokale oder Edge-Verarbeitung technisch und funktional sinnvoll ist, sollte sie als datensparsame Option berücksichtigt werden. Ist eine Cloud-Verarbeitung für die jeweilige Funktion erforderlich, sollten Zweckbindung, Datenminimierung, Speicherdauer und der Schutz identifizierender Informationen berücksichtigt werden.

Für Aufnahmen und sonstige Daten Dritter sollte bereits bei der Produktgestaltung geprüft werden, ob die Verarbeitung technisch vermieden, auf das erforderliche Maß beschränkt oder frühzeitig beendet werden kann.

Dabei sollten nicht nur die ursprünglichen Bild-, Audio- oder Sensordaten berücksichtigt werden. Auch aus diesen Daten abgeleitete Informationen, sogenannte Inferences, können sensibel sein. Erkennt ein System beispielsweise eine bestimmte Person, ordnet ihr eine berufliche Rolle zu oder leitet Interessen und Verhaltensmuster ab, sollten auch für diese Informationen klare Regeln zu Zweckbindung, Speicherung und Weiterverarbeitung gelten.

Aufnahme und Verarbeitung technisch unterscheiden

Es ist zu unterscheiden, ob eine Kamera oder ein Mikrofon gerade eine dauerhaft speicherbare Aufnahme erzeugt oder Sensordaten lediglich kurzfristig für eine konkrete Funktion verarbeitet werden, etwa für Übersetzung, Objekterkennung, Navigation oder die räumliche Platzierung virtueller Inhalte. Diese Unterscheidung sollte sich auch in der technischen Architektur und den Schutzmechanismen widerspiegeln. Insbesondere sollten kurzzeitige Sensordatenverarbeitungen nicht notwendig mit einer speicherbaren oder teilbaren Bild- oder Tonaufnahme verbunden sein.

Für KI-Funktionen sollte zudem klar erkennbar und technisch kontrollierbar sein, ob Daten lediglich zur unmittelbaren Erbringung einer Funktion verarbeitet oder darüber hinaus gespeichert, an externe Dienste übermittelt oder für die Verbesserung beziehungsweise das Training von KI-Modellen verwendet werden. Die nutzende Person sollte über verständliche Einstellungen erkennen und steuern können, welche Daten verarbeitet, gespeichert, übermittelt oder für Trainingszwecke verwendet werden. Außerdem sollten, soweit technisch möglich und risikoadäquat, auch betroffene Dritte erkennen können, ob eine speicherbare oder weiterverwendbare Verarbeitung erfolgt; hierfür kommen insbesondere Signalisierung, Zugangs- und Widerspruchsmöglichkeiten sowie informationelle Begleitmaßnahmen in Betracht. Für die Nutzung von Daten zu Trainingszwecken sollten verständliche Einstellungen und eine eigenständige datenschutzrechtliche Grundlage bestehen.

Aufnahmen für Außenstehende zuverlässig erkennbar machen

Entsteht ein Foto, Video oder eine Audioaufnahme, die gespeichert oder geteilt werden kann, sollte dies für Personen in der Umgebung eindeutig erkennbar sein. Die Signalisierung sollte so ausgestaltet sein, dass sie in typischen Nutzungssituationen wahrnehmbar ist; sie sollte durch weitere Transparenzmaßnahmen (Produktinformation, Verhaltensleitfäden) flankiert werden.

Entscheidend ist die tatsächliche Wahrnehmbarkeit des Signals, nicht die konkrete technische Umsetzung. Denkbar sind optische, akustische oder kombinierte Signale. Die Signalisierung sollte verlässlich und nicht ohne Weiteres durch die nutzende Person deaktivierbar sein. Technisch erkennbare Ausfälle oder Manipulationen des Signals sollten von der tatsächlichen Wahrnehmung durch Umstehende unterschieden werden. Wird ein Ausfall oder eine Manipulation technisch erkannt, kann die Speicherung oder Teilbarkeit der Aufnahme als mögliche Schutzmaßnahme eingeschränkt werden. Datensparsame Funktionen, die keine speicherbare Bild- oder Tonaufnahme erzeugen, etwa Navigation, Übersetzung oder räumliche Verankerung, können gegebenenfalls weiterhin verfügbar sein.

Die Wirksamkeit der Signalisierung sollte anhand nachvollziehbarer Kriterien geprüft werden. Dazu können insbesondere die Erkennbarkeit aus üblichen Nutzungsentfernungen, bei unterschiedlichen Blickwinkeln und Lichtverhältnissen sowie eine barrierearme Wahrnehmbarkeit gehören. Die Prüfkriterien sollten die konkrete Geräteform, den vorgesehenen Einsatzkontext und die tatsächliche Wahrnehmbarkeit durch Umstehende berücksichtigen, müssen aber praktikabel bleiben.

Transparenz verständlich und risikoadäquat gestalten

Transparenz sollte für Außenstehende klar und leicht verständlich sein. Bei aktiven Anwendungen wie Fotos, Videos oder Livestreams, die gespeichert oder geteilt werden können, sollte die Aufnahme zuverlässig erkennbar sein. Darüber hinaus sollten Anbieter die Nutzenden durch leicht zugängliche Funktionen und Informationen dabei unterstützen, betroffene Personen bereits vor der Aufnahme über den Verantwortlichen, die Zwecke der Verarbeitung und die einschlägigen Kontaktdaten zu informieren. Eine technische Anzeige ersetzt diese erforderliche Information nicht. Für KI-Assistenzfunktionen sind risikoadäquate Datenschutzmechanismen vorzusehen. Die konkrete technische Umsetzung sollte ergebnisorientiert und technologieoffen bleiben. Je nach Funktion und Einsatzkontext können insbesondere Maßnahmen in Betracht kommen, die die Erfassung und Verarbeitung personenbezogener Daten unbeteiligter Personen begrenzen, etwa durch nutzerseitige Steuerung, Einschränkungen bestimmter Funktionen oder Hinweise zu besonders sensiblen Kontexten.

Funktionen zur Identifizierung oder Einordnung von Personen sowie Verarbeitungen in besonders sensiblen Kontexten können ein erhöhtes Risiko für betroffene Personen begründen. In solchen Fällen sollten Anbieter geeignete Schutzmaßnahmen prüfen, etwa eine eingeschränkte Funktionsverfügbarkeit, klare Nutzerhinweise oder das

Unterlassen bestimmter Verarbeitungen, soweit dies technisch möglich und verhältnismäßig ist.

Dafür könnten langfristig herstellerübergreifend verständliche Licht-, Farb- oder andere Statussignale entwickelt werden. Solche Signale können die Transparenz unterstützen, sollten aber nicht als Ersatz für eine nach den Umständen erforderliche vorherige Information oder eine ggf. erforderliche Einwilligung verstanden werden.

Technische Präferenz und Widerspruchssignale erforschen

Perspektivisch könnten Mechanismen geprüft werden, mit denen Personen Präferenzen gegenüber Aufnahmen oder Veröffentlichungen ausdrücken können. Solche Signale ersetzen keine rechtlich erforderliche Einwilligung und müssten technisch belastbar sowie datensparsam ausgestaltet sein. Sie sollten daher als ergänzende Schutzmaßnahme entwickelt werden und nicht die Verantwortung der Nutzenden oder Anbieter für eine rechtmäßige Verarbeitung verdrängen. Gegenstand weiterer Prüfung könnte sein, ob und unter welchen technischen Voraussetzungen solche Signale die Wahrscheinlichkeit unerwünschter Aufnahmen oder Veröffentlichungen reduzieren können. Dabei wären insbesondere Fragen der technischen Machbarkeit, der Zuverlässigkeit, der Datensparsamkeit, der Missbrauchsresistenz sowie der praktischen Umsetzbarkeit in unterschiedlichen Nutzungskontexten zu berücksichtigen.

Datenschutzkonforme Werkzeuge für legitime Anwendungsfälle

Anbieter sollten für legitime Anwendungsfälle datenschutzkonforme Betriebsmodi bereitstellen. Dies gilt insbesondere für berufliche Anwendungen wie Übersetzungen, Navigation, Dokumentation oder die Transkription von Besprechungen. Die Verarbeitung durch die Funktionen sollte, wo aus Produktsicht möglich und sinnvoll, lokal oder unter kontrollierten Bedingungen erfolgen; die Funktionen sollten klare Einstellungen für Zugriff, Speicherung, Löschung, Weitergabe und die Nutzung zu Trainingszwecken enthalten.

Als mögliche Schutzmaßnahmen kommen unter anderem eine gut erkennbare Aktivierungsanzeige, eine einfache Unterbrechungsmöglichkeit, definierte Löschfristen sowie eine Begrenzung der Weiterverwendung zu anderen Zwecken in Betracht. Ob solche Maßnahmen erforderlich sind, hängt von der jeweiligen Funktion, dem Verantwortlichen, dem Einsatzkontext und den einschlägigen rechtlichen Vorgaben ab.

Anbieter können geeignete Informationen bereitstellen, damit Verantwortliche, etwa Arbeitgeber, die datenschutzrechtliche Zulässigkeit, den Einsatz von Dienstleistern sowie mögliche Drittlandübermittlungen bewerten können.

Dies gilt in besonderem Maße für institutionelle Betreiber, etwa Museen, Bildungseinrichtungen oder Unternehmen, die Smart Glasses als Leihgeräte bereitstellen. Diese sollten erkennen können, welche Einstellungen sie selbst oder über die eingesetzte App steuern können und bei welchen Funktionen sie auf den Geräte-,

Betriebssystem- oder Plattformanbieter angewiesen sind. Geräte- und Plattformanbieter könnten hierfür geeignete Konfigurations-, Protokollierungs- und Dokumentationsmöglichkeiten bereitstellen, etwa zur Deaktivierung nicht benötigter Funktionen, zur Steuerung von Cloud-Übermittlungen, zur Festlegung von Löschfristen und zur Nachvollziehbarkeit eingesetzter Dienstleister. Die technische Steuerungsmöglichkeit ergänzt die datenschutzrechtliche Rollen- und Verantwortlichkeitsprüfung im Einzelfall, ersetzt sie jedoch nicht.

Sichere Ersteinrichtung und verständliche Nutzerführung gewährleisten

Nutzerinnen und Nutzer sollten bei der ersten Einrichtung durch die wichtigsten Entscheidungen geführt werden: Privatsphäreeinstellungen, Absicherung des Kontos, Cloud-Nutzung und Deaktivierung nicht benötigter Funktionen. Verständliche Nutzerführung ist im Alltag wirksamer als umfangreiche Dokumentation. Bei Leihgeräten und beruflich bereitgestellten Geräten sollte die Ersteinrichtung zudem ermöglichen, dass der Betreiber datenschutzrelevante Grundeinstellungen zentral vorgeben, einschränken oder dokumentieren kann, soweit dies technisch möglich ist. Nutzende sollten dabei weiterhin erkennen können, welche Funktionen aktiv sind und welche Einstellungen durch die Institution vorgegeben wurden.

Besonders schutzbedürftige Nutzungssituationen berücksichtigen

Dies umfasst insbesondere den Jugendschutz. Kinder und Jugendliche können sowohl selbst Smart Glasses nutzen als auch von deren Funktionen erfasst werden. Als potenziell aufgezeichnete Personen können sie sich gegen entsprechende Aufnahmen häufig nur eingeschränkt zur Wehr setzen. Für Kinder und besonders sensible Kontexte sollten daher strengere Voreinstellungen und besondere Schutzmechanismen vorgesehen werden. Denkbar sind beispielsweise altersgerechte oder von Erziehungsberechtigten administrierbare Modi. Technische Ansätze zur Erkennung minderjähriger Personen können hierfür relevant sein. Sie setzen jedoch gegebenenfalls eine weitergehende biometrische oder altersbezogene Analyse voraus und sind daher am Grundsatz der Datenminimierung sowie an Verhältnismäßigkeit und Zweckbindung zu messen. Der Schutz von Kindern und Jugendlichen kann neben geeigneten technischen Lösungen insbesondere durch altersgerechte Voreinstellungen, Alterskontrollen auf Nutzerseite, zusätzliche Hürden vor einer Veröffentlichung sowie Aufklärung unterstützt werden. Transparenzhinweise zu aktiven Aufnahmen sollten dabei für Kinder und Jugendliche verständlich und zuverlässig wahrnehmbar sein. Zugleich sollten Schutzmechanismen nicht allein darauf setzen, dass betroffene Minderjährige eine Aufnahme erkennen, rechtlich einordnen und ihr widersprechen können.

Klare Nutzungsregeln und Aufklärung bereitstellen

Anbieter sollten in Betracht ziehen, transparent zu vermitteln, in welchen Situationen Aufnahmen unangemessen oder unzulässig sind. Dazu gehören insbesondere Räume mit erhöhter Privatheitserwartung. Auch Eingriffe in technische Schutz- oder

Signalisierungsmechanismen sollten in den Nutzungsbedingungen ausdrücklich ausgeschlossen werden. Ergänzend sollten leicht verständliche Verhaltensleitfäden und Informationsangebote bereitgestellt werden.

Für Nutzerinnen und Nutzer

Nutzerinnen und Nutzer tragen Verantwortung für einen respektvollen und rechtskonformen Umgang mit Smart Glasses. Die technische und rechtliche Bewertung komplexer Datenflüsse können sie jedoch nicht ersetzen. Hersteller und Diensteanbieter müssen die erforderliche Transparenz schaffen und ihre eigenen DSGVO-Pflichten erfüllen.

Die folgenden Empfehlungen helfen dabei, die eigenen Geräte und Funktionen zu verstehen, transparent mit der Umgebung umzugehen und besonders sensible Situationen zu vermeiden.

Das eigene Gerät und seine Funktionen kennen

Nutzerinnen und Nutzer sollten wissen, welche Sensoren und Funktionen ihr Gerät besitzt, wann eine Aufnahme entsteht, wann Daten lediglich verarbeitet werden und ob beziehungsweise wann Informationen das Gerät verlassen. Die Privatsphäreeinstellungen sollten vor der Nutzung geprüft werden.

Anwesende nicht überraschen

Smart Glasses und andere körpernah getragene Geräte können für Außenstehende schwerer einzuschätzen sein als eine sichtbar hochgehaltene Smartphone-Kamera. Ein transparenter Umgang ist daher wichtig. Wird eine Person gezielt aufgenommen, sollte dies deutlich gemacht und ein erkennbarer Widerspruch respektiert werden. Eine gezielte Aufnahme selbst ist dabei nicht automatisch unzulässig; für ihre spätere Verbreitung oder öffentliche Zugänglichmachung gilt jedoch grundsätzlich das Recht am eigenen Bild nach § 22 KUG, vorbehaltlich der Ausnahmen des § 23 KUG.

Aufnahme und Veröffentlichung getrennt betrachten

Dass eine Person Teil einer Aufnahme ist, bedeutet nicht automatisch, dass diese Aufnahme auch veröffentlicht werden sollte. Bei erkennbaren Personen sollte deshalb insbesondere vor einer Veröffentlichung geprüft werden, ob eine Zustimmung erforderlich ist beziehungsweise vorliegt.

Orte mit erhöhter Privatheitserwartung respektieren

Umkleiden, Sanitärbereiche, Saunen, Schwimmbäder, medizinische Einrichtungen und vergleichbare Situationen sind keine Orte für Aufnahmen. Dass ein Gerät technisch aufnehmen kann, bedeutet nicht, dass diese Funktion überall angemessen eingesetzt werden sollte.

Audio sorgfältig behandeln

Auch Gespräche anderer Personen können sensible Informationen enthalten. Audioaufnahmen und die Verarbeitung gesprochener Sprache sollten deshalb sorgfältig behandelt werden. Besondere Vorsicht gilt bei nicht öffentlich gesprochenen Worten: Ihre unbefugte Aufnahme, Verwendung oder Weitergabe an Dritte kann den Straftatbestand der Verletzung der Vertraulichkeit des Wortes nach § 201 StGB erfüllen; auch die öffentliche Mitteilung einer solchen Aufnahme im Wortlaut oder nach dem wesentlichen Inhalt kann erfasst sein.

Bei Kindern besondere Zurückhaltung üben

Aufnahmen von Kindern und insbesondere deren Veröffentlichung erfordern besondere Sensibilität. Technische Möglichkeiten sollten nicht dazu führen, dass Aufnahmen beiläufig entstehen oder geteilt werden.

Situationsbewusstsein wahren

Assistenz- und Displayfunktionen dürfen nicht von der unmittelbaren Umgebung ablenken. Dies gilt insbesondere im Straßenverkehr oder in Situationen, in denen erhöhte Aufmerksamkeit erforderlich ist. Lokale Regeln und Hausordnungen sollten respektiert werden.

Für Aufsichtsbehörden

Smart Glasses und vergleichbare smarte Technologien stellen Aufsichtsbehörden vor die Aufgabe, Datenschutz und Sicherheit wirksam zu schützen, ohne Innovation und praktikable Anwendungsfälle pauschal zu beschränken. Ein risikobasierter Ansatz sollte daher an der konkreten Funktion, dem Verarbeitungskontext und den vorhandenen Schutzmechanismen ansetzen. Zugleich sind Koordination, frühzeitiger Dialog und verständliche Aufklärung zentrale Voraussetzungen für rechtssichere und einheitliche Bewertungen.

Konkrete Funktionen statt Produktkategorien bewerten

Die Beurteilung sollte sich an der tatsächlichen Funktionsweise eines Geräts orientieren: Erfolgt überhaupt eine Erfassung personenbezogener Daten? Wird eine speicherbare Aufnahme erzeugt oder findet lediglich eine flüchtige Verarbeitung statt? Welche Daten werden übertragen? Welche Schutzmechanismen bestehen? Sind Aufnahmen von Dritten für diese erkennbar? Eine pauschale Bewertung anhand der Bauform oder Bezeichnung eines Produkts greift zu kurz.

Maßgeblich ist somit eine funktionen- und risikobasierte Prüfung im jeweiligen Anwendungskontext. Dabei sind die tatsächliche Funktionsweise, die Art der Datenverarbeitung sowie die vorhandenen Schutz- und Transparenzmechanismen zu berücksichtigen.

Zwischen Aufnahme und funktionaler Sensorverarbeitung unterscheiden

Für die regulatorische Bewertung ist entscheidend, ob eine Funktion darauf angelegt ist, ein Bild oder Video dauerhaft zu erzeugen, oder ob Kameradaten beispielsweise lediglich für Übersetzung, Objekterkennung, Navigation oder AR-Anwendungen verarbeitet werden. Nicht jede sensorische Erfassung sollte automatisch wie eine dauerhafte Aufnahme behandelt werden. Zugleich müssen auch flüchtige Verarbeitungen transparent und risikoadäquat geschützt sein.

Technische Schutzmaßnahmen bei der Bewertung berücksichtigen

On-Device-Processing, Datenminimierung, kurze Speicherdauern, nicht abschaltbare Aufnahmesignale, automatische Anonymisierung oder kontextabhängige Gerätefunktionen können ggf. bestehende Risiken erheblich reduzieren. Solche Maßnahmen sollten bei der regulatorischen Bewertung angemessen berücksichtigt werden.

Formelle Stakeholder-Konsultationen durchführen und öffentliche Datenschutz-Aufklärung aktiv fördern

Die Erklärung des EDSA[4] enthält wichtige erste Orientierungen. Bevor daraus verbindliche Leitlinien oder Prüfmaßstäbe entwickelt werden, sollten formelle, strukturierte Konsultationen mit Wirtschaft, Behindertenverbänden, Verbraucherinnen und Verbrauchern sowie der Zivilgesellschaft erfolgen. Zugleich sollten Aufsichtsbehörden öffentliche Aufklärung über die Funktionsweise, Statussignale und den verantwortungsvollen Umgang mit Smart Glasses fördern.

Frühzeitigen Dialog mit Herstellern ermöglichen

Risiken sollten bereits während der Produktentwicklung adressiert werden. Ein kontinuierlicher Austausch über technische und organisatorische Schutzmaßnahmen sollte Bestandteil eines risikobasierten Aufsichtsansatzes sein. Pauschale Verbote sollten erst geprüft werden, wenn weniger eingreifende Maßnahmen nachweislich nicht ausreichen.

Zuständigkeiten koordinieren und widersprüchliche Bewertungen vermeiden

Unterschiedliche Einschätzungen verschiedener Behörden zum identischen Produkt schaffen Rechtsunsicherheit. Dies trifft insbesondere kleinere Hersteller, Importeure und Händler mit begrenzten Ressourcen für parallele regulatorische Verfahren.

[4] Statement 1/2026 of the EDPB on smart glasses, 13. Oktober 2026, ↗hier.

Für die Politik

Die politische Herausforderung besteht darin, die Privatsphäre und Sicherheit betroffener Personen wirksam zu schützen, ohne die Potenziale smarter Technologien für Barrierefreiheit, Produktivität, Teilhabe und europäische Wertschöpfung pauschal zu beschränken. Ein zweck- und risikobezogener Ansatz, der an konkrete Verarbeitungen, Schutzmechanismen und Nutzungskontexte anknüpft, bietet dafür den geeigneten Rahmen. Zugleich sollten Regulierung, technische Standards, Aufklärung und die konsequente Durchsetzung bestehender Regeln zusammenwirken.

Regulierung zweck- und risikobezogen statt gerätebezogen gestalten

Die zentrale regulatorische Frage sollte nicht lauten, ob ein bestimmtes Gerät über eine Kamera, ein Mikrofon oder andere »Computer Senses« verfügt. Entscheidend sollte sein, welche Daten zu welchem Zweck erhoben und verarbeitet werden, wie lange sie gespeichert werden, wer Zugriff darauf erhält und in welcher Weise die betroffenen Personen über die Verarbeitung informiert werden. Eine solche Regulierung ist technologieneutraler und zukunftsfester als Vorgaben für einzelne Bauformen.

Keine pauschalen Produktverbote

Smart Glasses sind nicht lediglich »Kameras in Brillenform«. Pauschale Einschränkungen würden sehr unterschiedliche Anwendungen gleichermaßen erfassen, einschließlich solcher, die keine vergleichbaren Risiken aufweisen. Zudem können sie gesellschaftlich wertvolle Anwendungen behindern.

Barrierefreiheit und gesellschaftliche Teilhabe systematisch berücksichtigen

Kamerabasierte Assistenzfunktionen können für blinde und sehbeeinträchtigte Menschen Texte, Schilder, Fahrpläne oder Informationen über die Umgebung zugänglich machen. Smarte Hör- und Assistenzfunktionen können Menschen mit Hörbeeinträchtigungen unterstützen. Übersetzung, Navigation, Fernunterstützung und freihändige Assistenz eröffnen weitere Möglichkeiten der Teilhabe. Beschränkungen sollten daher stets darauf geprüft werden, welche legitimen Anwendungen sie zugleich verhindern oder erschweren.

Zwischen individuellem Verhalten, Produktgestaltung und Plattformverantwortung unterscheiden

Eine unerlaubte Aufnahme, eine technisch unzureichend gestaltete Kamera und die rechtswidrige Veröffentlichung eines Videos sind unterschiedliche Sachverhalte. Diese Ebenen sollten auch regulatorisch getrennt behandelt werden.

Schutzlücken technologieneutral schließen

Soweit bei heimlichen Aufnahmen, digitalem Voyeurismus oder bildbasierter sexualisierter Gewalt tatsächlich Regelungslücken bestehen, sollten diese an der schädlichen Handlung ansetzen – nicht an einer einzelnen Produktkategorie.

Bestehende geräteunabhängige Regeln konsequent nutzen

Hausordnungen, Badeordnungen, Beförderungsbedingungen und andere bestehende Regelwerke können unerwünschte Aufnahmen bereits heute unabhängig vom verwendeten Gerät untersagen. Dieser handlungsbezogene Ansatz bleibt auch gegenüber neuen Technologien wirksam.

Freiwillige europäische technische Standards entwickeln

Damit Privacy by Design und Transparenzmechanismen herstellerübergreifend funktionieren können, sollte die Entwicklung freiwilliger europäischer Interoperabilitätsstandards gefördert werden. Solche Standards sollten ergebnisorientiert, technologieoffen und risikobezogen sein und keine bestimmte technische Architektur oder Produktfunktion vorgeben.

Ein Verstoß gegen einen freiwilligen Standard begründet für sich genommen keine unmittelbare Sanktion. Rechtliche Folgen können sich jedoch unabhängig davon aus anwendbarem Recht ergeben, insbesondere aus der DSGVO, dem TDDDG oder anwendbarem Produktrecht. Wird ein freiwilliger Standard als harmonisierte Norm im Amtsblatt der Europäischen Union veröffentlicht, kann seine Anwendung zudem eine Konformitätsvermutung mit den von ihm abgedeckten rechtlichen Anforderungen auslösen.

Dabei sollten die Standards ergebnisorientiert und technologieoffen sein: Sie sollten beispielsweise zuverlässige Erkennbarkeit verlangen, aber nicht eine einzelne konkrete LED-Farbe oder technische Umsetzung vorschreiben. Zugleich sollte klar bleiben, dass die Einhaltung eines Standards die Einhaltung der jeweiligen gesetzlichen Pflichten nicht ersetzt, sondern deren Erfüllung technisch unterstützen kann.

Kontextabhängige Gerätefunktionen ermöglichen, statt Fähigkeiten grundsätzlich zu beschneiden

Regulatorische Rahmenbedingungen sollten flexible Nutzungs- und Einsatzkontexte unterstützen, statt Gerätefunktionen pauschal einzuschränken. Im privaten Umfeld können andere Anforderungen und Schutzmaßnahmen angemessen sein als in einem Unternehmen, einer Schule oder einer medizinischen Einrichtung. Solche Unterscheidungen sollten vorrangig durch nutzer- oder betreiberseitig konfigurierbare Richtlinien umgesetzt werden, etwa durch Profile, Berechtigungen und Funktionsbeschränkungen. Ein solcher Rahmen verbindet Schutz und Innovation besser als dauerhaft eingeschränkte Geräte.

Aufklärung und Medienkompetenz stärken

Informationsangebote der Hersteller für Nutzerinnen und Nutzer, Schulen, Eltern und Erziehende sollten neben technischen und regulatorischen Maßnahmen eine zentrale Rolle spielen. Neue Geräte erfordern auch neue gesellschaftliche Konventionen darüber, welche Nutzung in welcher Situation angemessen ist. Hersteller sollten diese Aufklärung maßgeblich mittragen, da sie den unmittelbaren Zugang zu ihren Produkten, deren Funktionen und implementierten Schutzmechanismen haben. Sie sollten daher verständliche Produktinformationen, Onboarding-Hinweise, Datenschutzerklärungen und konkrete Nutzungsempfehlungen bereitstellen. Ergänzend können Bildungsträger, Verbraucherzentralen, Aufsichtsbehörden und zivilgesellschaftliche Organisationen unabhängige Informations- und Schulungsangebote entwickeln; über deren Finanzierung sollte im Rahmen bestehender Förderinstrumente entschieden werden.

Europäische Klärung statt nationaler Sonderwege

Soweit regulatorische Abgrenzungsfragen offen sind, sollten sie möglichst auf europäischer Ebene beantwortet werden. Unterschiedliche nationale Vorgaben erschweren die Entwicklung und Vermarktung neuer Produkte im Binnenmarkt und können insbesondere kleinere Unternehmen belasten.

Standort- und Wertschöpfungseffekte berücksichtigen

Sensorik, Optik, Displaytechnologie, Halbleiter, KI und Forschung sind wichtige Bestandteile europäischer Wertschöpfung. Auch mittelständische Hersteller, Importeure und der stationäre Handel sind von regulatorischen Vorgaben betroffen. Ein klarer, zweck- und risikobezogener Rahmen kann deshalb zugleich das Schutzniveau erhöhen und Investitions- sowie Planungssicherheit schaffen.

Übergreifendes Ziel sollte sein, nicht die Wahrnehmungsfähigkeit smarter Systeme grundsätzlich einzuschränken, sondern wirksame Kontrolle darüber zu schaffen, was Computer sehen und hören, was sie daraus ableiten und was sie mit diesen Informationen anschließend tun dürfen.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 700 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner/in
Dr. Sebastian Klöß | Leiter Märkte & Technologien
+49 30 27576-210 | s.kloess@bitkom.org

Elena Kouremenou | Manager branchenspezifischer Datenschutz & Governance
T +49 30 27576-425 | e.kouremenou@bitkom.org

Verantwortliche Bitkom-Gremien
AK Augmented & Virtual Reality | AK Datenschutz

Autorinnen und Autoren
Alexander Fuchs, Service Owner Expert, Carl Zeiss AG | Anna Graf, Digitale Innovation l AI Lead, Arvato Systems GmbH | Johanna Heberllein, LL.M, Syndikusrechtsanwältin /Legal Counsel, BMW Group | Rudi Kramer, Fachberater Datenschutz, Datev eG | Raphael Kuhlmann, Arvato Systems GmbH | Lutz Mache, Government Affairs and Public Policy Senior Manager, Google Germany GmbH | Stefan Marx, Co-Founder & CEO, Zaubar UG | Anne-Sophie Panzer, Co-Founder & COO, Zaubar UG | Sophie Sohm, Privacy – Policy Manager, Meta | Illya Refael Trubman, Manager Public – Policy, Meta | Manfred Verholen, Corporate Security Manager, Vodafone GmbH

Copyright
Bitkom 2026

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung im Bitkom zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim Bitkom oder den jeweiligen Rechteinhabern.