27 August 2026

Blinded by the LED: smart glasses, GDPR, and the illusion of hardware indicators

by Peter Craddock

Smart glasses are attracting much attention these days. Already significant sales seem to pale in comparison to the explosion of social commentary on them, just as the segment of camera-enabled wearables is growing also in terms of form factors and devices, with AI-powered pins, portable speakers and even headphones around the corner. A few months ago, I wrote an in-depth piece about incidental processing and whether the General Data Protection Regulation or GDPR should even apply to it – a very important topic also for wearables in relation to bystanders. But with the summer focus on smart glasses, it seemed to be time to tackle some of the key data protection questions that are bubbling up.

Is the use of smart glasses legal under the GDPR? Are they covert surveillance devices? Who is responsible under data protection rules – the user or the manufacturer – and for what? What about the LED indicator, is it useful or even required under data protection law?

Here is a summary of the in-depth analysis that follows. Stay for the entire ride, there is quite a bit of history and nuance to cover.

Smart glasses, like many other devices on the market (e.g. smartphones, camera-enabled doorbells and more) are dual-use devices, not covert surveillance equipment. The fact that certain people misuse them does not change the legality of the technology itself.

Under EU data protection law, much of the information captured may not constitute personal data due to identifiability issues, and the user acts as controller for most processing activities that might remain.

LED indicators do not provide the degree of transparency required under the GDPR, and risk even becoming ineffective in case of overuse (such as if their activation is required even without evidence of processing of personal data).

Instead, it is important for authorities to enforce existing laws against misuse and to improve awareness rather than imposing restrictive obligations on manufacturers.

Let's look at each of these points in turn. This analysis is also available **on datalaws.net** (with handy table of contents and other readability & reference features).

I. Context of this analysis 2

II. Covert recording equipment restrictions, and the German case for not banning smart glasses 3

III. Allocation of responsibilities between manufacturer and user 7

III.1. The user as controller, and household exemption scope 7

III.2. Practical challenges are not a reason for a different conclusion 9

III.3. User, manufacturer/provider: who determines the purpose of processing? 9

IV. Is it all even processing of personal data? 11
IV.1. Relative identifiability 11
IV.2. Ambient data capture and patterns relevant for AI training & functioning 13
IV.3. Biometric identification versus biometric data: EU AI Act & GDPR 14
IV.4. Voice capture, and syllables as equivalent to tokenisation 14
IV.5. Non-personal data from the manufacturer's perspective as controller 15
IV.6. Bystanders & non-personal data from the user's perspective as controller 16
IV.7. Dissemination of footage and (re)identification 16
V. Transparency obligations and the purpose of indicators 17
V.1. GDPR transparency requirements 17
V.2. Smart glasses and how to provide transparency 18
V.3. Indicator meaning and LED fatigue 19
VI. Better solutions for information and to tackle abuse 20

I. Context of this analysis

Authorities across the European Union are examining whether a product category that has recently grown in size internationally, smart glasses, should even be banned. This has followed reports of individuals misusing smart glasses to record their interactions with other people without their knowledge, even publishing them afterwards online. Some of the debate surrounding such AI-powered wearable devices has focussed on the issue of transparency vis-à-vis bystanders, and whether a visible status LED should be required by law anytime the camera (or any optical sensor) is active. Others have even claimed such products should be simply banned based on the potential for abuse.

This type of concern is nothing new.

As the U.S. legal scholars Samuel Warren and Louis Brandeis wrote in 1890[1]:

> *"the latest advances in photographic art have rendered it possible to take pictures surreptitiously"*

Their article came just two years after the Kodak portable camera was launched, raising privacy concerns. As mentioned in an article of the Smithsonian Magazine:

> *The camera's first great age—which began in 1888 when George Eastman debuted the Kodak—is full of stories like [one of a person not consenting to her portrait appearing on an ad]. Beyond the wonders of a quickly developing art form and technology lay widespread lack of control over one's own image, perverse incentives to make a quick buck, and generalized fear at the prospect of humiliation and the invasion of privacy.*

[1] S. Warren and L. Brandeis, "The Right to Privacy", *Harvard Law Review.* Vol. IV, December 15, 1890, No. 5.

Similar concerns have been voiced at different stages of technological innovation. A decade ago, drone photography was being criticised as enabling "creepshots". Before that, "camera phones" (predecessor to the smartphone) raised privacy concerns as well. Previously came the debates about portable cassette recorders (such as the Sony Walkman's recording feature) and home video cassette recording, which touched both on the right to privacy (and surreptitious audio or video recording) and other rights (such as intellectual property rights).

A general trend with these technologies seems to be a first attempt to get the technology banned, before gradual recognition that **these technologies are not inherently unlawful – instead, it is the choice by a given user to use the technology in a certain way that can make that specific use unlawful**.

That is not to say that concerns of surreptitious photography, often with a sexual harassment or voyeurism angle, are irrelevant. There are very legitimate concerns of women, young parents and others who consider that this is yet another tool that can lead to abuse, and there are anecdotes of such abuse. However, banning may not be the right answer if the problem is one related to misuse by users themselves. Moreover, as discussed further, the availability of actual covert surveillance equipment in various EU Member States, often at lower prices than smart glasses, raises additional question regarding the appropriateness of directing such concerns at smart glasses.

In this context, it seems worth looking at how to best manage liability and role allocation in the context of such "dual-use" products, i.e. ones who can have entirely legitimate use cases but whose use in certain contexts can be unlawful.

The particular focus here is related to the data protection angle, notably from the perspective of transparency, data protection roles and risk – including the question of whether indicators make any sense, and if so, in which precise situations. Before examining those questions, though, it is important to examine the question of covert recording equipment as a separate regulatory issue.

It is also worth noting that other wearables with cameras are regularly being announced, such as camera-equipped headphones. While the analysis hereunder is focussed on smart glasses, much of the reasoning is equally applicable to other AI-powered wearables with optical and audio sensors.

II. Covert recording equipment restrictions, and the German case for not banning smart glasses

Smartphones *can* be used to take photos and recordings without this being apparent to every person. Raising a phone with two hands and away from the user might be a tell that there is a likelihood of recording or a photo, but it remains possible to take photos or videos far more discreetly. Audio recording features can be used in an invisible manner.

Yet the law did not evolve to require device makers to implement visual or audio cues (except perhaps in countries such as Japan). Instead, laws appear to focus on regulating how the general principles of

liability apply to such scenarios, and where the provider's responsibility ends, and the user's own responsibility begins.

Due to their possibility of use in different contexts, such products do not face the same type of restrictions as e.g. button cameras or other spy cameras hidden in everyday objects – whose use is prohibited in general in certain countries, such as under the German Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz or TDDDG.

While the TDDDG's prohibition of covert audio and video equipment appears unique to Germany, discussions as to whether smart glasses fall within that same category appear significant in order to assess what a pan-EU debate might examine, and it is worth examining the TDDDG's prohibition briefly.

The scope of the TDDDG's ban at a hardware level concerns the following: *"telecommunications equipment […] which is disguised with objects of daily use and which, because of these circumstances or because of its manner of functioning, is particularly suited and intended […] to covertly record the image of another person"*[2] (rough translation). The key criteria are therefore (i) disguise with an object of daily use and (ii) suitability **and** intent for covertly recording images.

The TDDDG further explains what that 'intent' covers: *"A telecommunications device is considered to be intended for the covert eavesdropping or recording of an image, in particular, if on the occasion of the intended use of the device its eavesdropping or recording function is not clearly recognisable to the person concerned"*[3].

Intent goes beyond mere suitability and the covert nature of recording, but covers visibility of the lens itself as camera lens. If the criterion had been "people generally do not expect it or recognise it today", then *anything* to which a camera is ever added would have been considered as at least initially falling within the scope of that prohibition – making it impossible to ever add a camera to any existing form factor.

Yet this is precisely the debate that occurred over two decades ago. Our smartphones today would not exist without the camera phone, which itself was a phone to which a camera was added – and when they first launched, a few years after the predecessor to Section 8 TDDDG had been adopted (in 1996), not everyone would have expected or recognised the camera on the phone due to the novelty of such devices.

The parliamentary materials having led to Section 8 TDDDG's predecessor, (then) Section 90 of the Telekommunikationsgesetz or TKG, already gave clues as to where the discussion should go: dual-use products, i.e. products whose primary purpose is not covert surveillance but something else, are not intended to be covered.

---

[2] TDDDG, §8(1). Original in German: *"Telekommunikationsanlagen […] die mit Gegenständen des täglichen Gebrauchs verkleidet sind und aufgrund dieser Umstände oder aufgrund ihrer Funktionsweise in besonderer Weise geeignet und dazu bestimmt sind, […] das Bild eines anderen von diesem unbemerkt aufzunehmen".*

[3] TDDDG, §8(2). Original in German: *"Als zum unbemerkten Abhören oder Aufnehmen eines Bildes bestimmt gilt eine Telekommunikationsanlage insbesondere, wenn ihre Abhör- oder Aufnahmefunktion beim bestimmungsgemäßen Gebrauch des Gegenstandes für den Betroffenen nicht eindeutig erkennbar ist."*

> *Section 90 is a provision accompanying Section 201 of the Criminal Code. The extension of Section 90 to cover other telecommunications equipment is necessary because, as technology has advanced, eavesdropping devices have become commercially available which no longer rely on the functions of microphones in conjunction with transmitting equipment, but instead utilise different operating principles. At present, particular mention should be made of so-called laser microphones, which can convert the vibrations in other objects – such as window panes – generated by the sound waves of spoken words back into intelligible speech. The provision is drafted to be as technology-neutral as possible. The addition in paragraph 1, stipulating that devices must not only be suitable but also intended for the purpose of eavesdropping on speech not uttered in public without being noticed, or of recording the image of another person without their knowledge, is intended to prevent the scope of the prohibition from becoming excessive. As has been the case to date, the scope of the prohibition is to be limited to those devices which, from the outset, serve no legitimate purpose but are clearly intended solely for the covert eavesdropping on conversations or the covert recording of images of another person.* ***Devices which, whilst suitable for covert eavesdropping or covert image recording due to their mode of operation, are not intended for this purpose – such as mobile phones – should not fall within the scope of the prohibition***. [machine translation, emphasis mine][4]

Mobile phones were thus permitted to enter the German market, as were later on camera phones and other devices.

A judgment of 9 April 2020 of the Cologne Higher Regional Court[5] provides an interesting assessment of the state of legislative interpretation, and it remains to be seen whether German claims regarding smart glasses could lead to a dramatic shift:

> *According to the legislature, a transmission system is 'intended' for recording if, from the outset, it serves no legitimate purpose but is clearly intended solely for the (covert interception of conversations or the) covert recording of images of another person […] The purpose intended by the law must therefore be understood in objective terms* [machine translation][6]

Drawing comparisons with criminal law, the Cologne Higher Regional Court then stated that specific laws *"[s]imilar to Sections 90(1), first sentence, and 148(1)(2) TKG, Sections 202c(1)(2) and 263a(3) of the Criminal Code (StGB) criminalise the creation of relevant computer programs as acts constituting a preparatory stage to the spying on and interception of data or to computer fraud respectively"*[7]. Even under these provisions of criminal law, the dual-use nature of devices is taken into account: *"[i]f, given the functionality of these computer programs, a use other than the one in question is (also) conceivable, the primary, essential or actual purpose*

---

[4] Deutscher Bundestag, 4 May 2011, Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen, Drucksache 17/5707, pages 78-79.

[5] OLG Köln, decision of 9 April 2020, 1 RVs 74/20.

[6] Machine translation. Original in German: *"Zum Aufnehmen "bestimmt" ist die Sendeanlage nach den Vorstellungen des Gesetzgebers, wenn sie von vornherein keinem anerkennenswerten Zweck, sondern offensichtlich nur dem (heimlichen Abhören von Gesprächen bzw. dem) heimlichen Anfertigen von Bildaufnahmen eines anderen dient […] Die vom Gesetz gemeinte Zweckbestimmung ist daher objektiviert zu verstehen".*

[7] Machine translation. Original in German: *"Vergleichbar mit §§ 90 Abs. 1 S. 1, 148 Abs. 1 Ziff. 2 TKG stellen §§ 202c Abs. 1 Ziff. 2 und 263a Abs. 3 StGB mit der Herstellung pp. entsprechender Computerprogramme Handlungen im Vorfeld des Ausspähens und Abfangens von Daten bzw. des Computerbetrugs unter Strafe".*

shall be decisive"[8]. The Cologne Higher Regional Court considered that *"[i]t stands to reason that these considerations should be applied to Sections 90(1), first sentence and 148(1)(2)(a) TKG"*[9] – i.e. focus on the "primary, essential, or actual purpose" of the device.

The court's conclusion is that *"[w]hether the primary purpose of the device is covert eavesdropping or recording is then determined on the basis of the intentions of those who developed, manufactured or distributed it, in so far as these have manifested themselves in a manner that is objectively discernible from the outside and indicate an intended use, or a use that was certainly foreseen, for the purpose of recording or eavesdropping without being detected"*[10].

No manufacturer of smart glasses appears to have manifested any intentions on its own part for their devices to be intended to be used *"for the purpose of recording or eavesdropping without being detected"*. On the contrary, anti-tampering measures regarding LED indicators – indicators whose very existence raises other issues of relevance, as I will explain below – demonstrate a clear intent to **prevent** or at least **limit** the possibility of such covert use. The existence of such measures is therefore a **confirmation of the dual-use nature** of smart glasses, supporting the conclusion that smart glasses are **not** intended as covert eavesdropping or recording devices.

In this context, while the debate regarding the (non-)applicability of Section 90 TDDDG appears to be important from a legal perspective, it is unclear on which basis a ban would be reasonable, in particular if the intent is to avoid significant knock-on effects on any novel attempt to add in the future a camera or recording function to any other type of device whose primary purpose is not covert surveillance.

It is worth stressing two additional points regarding perception.

First, the less obvious nature of recording capabilities may often be a result of evolving consumer awareness. Mass (dual-use) consumer devices such as camera-equipped phones, camera-equipped doorbells and camera-equipped glasses are not intended to be covert spying equipment but are well publicised devices with different primary purposes. The primary intent of niche surveillance products such as a button camera is clearly the taking of photos in a surreptitious manner, even hiding the appearance of a camera entirely. The primary intent of smart glasses appears to be otherwise, namely enabling the user (the wearer) to complement or replace a smartphone's functionalities, for instance through live captioning, translations, navigation support **and** photography. Widespread communication regarding smart glasses, by manufacturers and by detractors, is precisely of a nature to increase global awareness of the fact that these devices have another primary function than covert recording.

---

[8] Machine translation. Original in German: *"Kommt nach der Funktionalität dieser Computerprogramme (auch) eine andere als die inkriminierte Verwendung in Betracht, entscheidet der primäre, wesentliche oder eigentliche Zweck"*.

[9] Machine translation. Original in German: *"Es liegt nahe, diese Überlegungen auf §§ 90 Abs. 1 S. 1, 148 Abs. 1 Ziff. 2 lit. a) TKG zu übertragen"*.

[10] Machine translation. Original in German: *"Ob der primäre Zweck der Anlage das heimliche Abhören oder Aufnehmen ist, beurteilt sich alsdann nach den Vorstellungen derjenigen, die sie entwickelt, hergestellt oder vertrieben haben, soweit sich das nach außen hin objektiv erkennbar manifestiert hat und auf eine beabsichtigte oder als sicher vorausgesehenen Nutzung zum unbemerkten Aufnehmen oder Abhören hinweist"*.

Second, the very low price of button cameras for instance reveals a practical reality: if a person truly wishes to take photos of someone else surreptitiously, there are more "suitable" options for a fraction of the price. From high-resolution for 100+ EUR to lower resolution ones for around the 20-50 EUR mark, covert photography or video recording equipment is cheap(er), accessible and – as opposed to smart glasses – clearly designed with surreptitious recording as the primary intent and feature. Spending more money on smart glasses is not rational if the primary purpose of the user is covert image recording. If an individual truly wishes to use a device for covert image recording, there are other options.

III. Allocation of responsibilities between manufacturer and user

The dual-use nature of smart glasses (just like smart doorbells, smartphones, camera phones, drone cameras and many more) means that illegality is not presumed and global restrictions should be set aside. In addition, the manufacturer is not presumed to be liable for all actions undertaken by a user. On the contrary: due to the several ways in which smart glasses can be used, any unlawful use is carried out at the user's own discretion.

Much of the debate surrounding smart glasses revolves around privacy and data protection rules, and the issue of what precisely the manufacturer should do, compared to the user. After calls for bans, the next reaction is to attempt to place obligations squarely on the shoulders of the manufacturer.

Yet the allocation of responsibilities under the General Data Protection Regulation or GDPR does not depend on policy wishes regarding who *ought* to be responsible. Instead, it depends on facts, namely the extent to which a given person or entity influences the purposes and means of processing of personal data.

III.1. The user as controller, and household exemption scope

The judgment of the Court of Justice of the European Union (CJEU) has had several cases in which it appears to have at least implicitly considered that private individuals using certain technologies can act as controller under data protection rules.

First, in *Lindqvist*[11], the CJEU held that *"the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data wholly or partly by automatic means"* within the meaning of data protection rules (*Lindqvist,* para. 27 – which refers to the GDPR's predecessor, Directive 95/46/EC).

While the CJEU did not explicitly state that the person in question, Mrs Lindqvist, acted as controller, the case is built on that premise. Mrs Lindqvist's own data processing activities were being examined from the perspective of the material scope of application of data protection rules, and the CJEU

[11] CJEU, 6 November 2003, *Lindqvist*, C-101/01, EU:C:2003:596.

concluded that her own activities did not meet the conditions for any of the exceptions to that scope[12]. The explicit recognition by the CJEU that Mrs Lindqvist's processing activities were not limited to *"activities which are carried out in the course of private or family life of individuals"*[13] amounts itself to recognition that Mrs Lindqvist's own role as controller was not brought into question.

In *Ryneš*[14], the CJEU was led to examine the scope of that "household exemption" further, i.e. Article 3(2), second bullet of Directive 95/46/EC (the equivalent to Article 2(2)(c) GDPR), which excludes the application of Directive 95/46/EC (today: the GDPR) to the processing of personal data *"by a natural person in the course of a purely personal or household activity"*.

In that case, which concerned video surveillance where a private security camera also monitors a public space, the CJEU first stressed that this exemption must (as is generally the rule regarding exemptions) be interpreted restrictively:

> *"the processing of personal data comes within the exception […] only where it is carried out in the purely personal or household setting of the person processing the data" (Ryneš, para. 31)*

The CJEU specifically rejected the application of this exception to cameras facing public spaces:

> *"To the extent that video surveillance such as that at issue in the main proceedings covers, even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, it cannot be regarded as an activity which is a purely 'personal or household' activity […]" (Ryneš, para. 33)*

As a result, any use even by private individuals of tools such as cameras in a public setting would go beyond the household exemption if it leads to the processing of personal data of other persons.

In this context, the CJEU also acknowledged that the individual can act as controller: *"the application of Directive 95/46 makes it possible, where appropriate, to take into account […] legitimate interests pursued by the controller, such as the protection of the property, health and life of his family and himself, as in the case in the main proceedings"* (*Ryneš*, para. 34). Its reference in its conclusion to the fact that the camera was *"installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners"* (*Ryneš*, para. 35) further confirms the fact that he was the person who determined the purpose of processing.

While the focus of these cases was thus not specifically the question as to whether a user of a technology is the *sole* controller for a processing activity (or the role of the technology provider), the CJEU clearly operated on the assumption that a user **is a controller** in those cases.

The lessons of *Lindqvist* and *Ryneš* for smart glasses are clear: the user (i.e. the wearer) **is** a controller if he/she decides to use the smart glasses for own purposes, and the household exemption does **not** apply

---

[12] *Ibid.*, paragraphs 37-48.

[13] *Ibid.*, para. 47.

[14] CJEU, 11 December 2014, *František Ryneš*, C-212/13, EU:C:2014:2428.

(i.e. the GDPR obligations apply in full) if a data processing activity is carried out by or on behalf of the user that targets *"a public space and is accordingly directed outwards from the private setting of the [user]"* (*Ryneš*, para. 33).

III.2. Practical challenges are not a reason for a different conclusion

Before examining the precise role of the technology provider compared to that of the user, it is important to tackle a practical concern. In the case discovery of processing *after* the fact, for instance if the user decides to upload a video of a passer-by and that passer-by is identified or identifiable (i.e. a data subject whose personal data is being processed), there is the question of how the passer-by can get to the identity of the user with a view to exercising his/her rights.

In practice, the passer-by will have additional means of getting to the user's identity in the case of a fixed security camera (e.g. by finding the house to which it is fixed and checking the name on the doorbell or even ringing it), as opposed to a wearer of smart glasses. The same consideration applies in relation to other portable devices, though, such as smartphones and drones.

Yet these concerns regarding **ease of exercise of data subject rights** as well as **enforceability of data protection rules** are irrelevant to the legal assessment of who acts as controller, which is instead an **objective, factual assessment** based not on ease of exercise of data subject rights but rather based on **who actually determines the purposes (and means) of processing**.

III.3. User, manufacturer/provider: who determines the purpose of processing?

As highlighted in my previous analysis regarding incidental processing, CJEU case law on the notion of controllership has helped specify the conditions for a person or entity to be considered as (sole or joint) controller:

- **influence** on the purposes and means of processing is important[15];
- the determination of the purposes and means can come from **common or converging decisions** with a tangible impact on that determination[16];
- joint controllership is **not always equal responsibility** in case of different degrees of involvement[17].

[15] CJEU, 10 July 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, para. 68.

[16] CJEU, 5 December 2023, *Nacionalinis visuomenės sveikatos centras*, C-683/21, EU:C:2023:949, para. 43.

[17] CJEU, 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388, para. 43.

[see my analysis of Principles regarding controllership]

A device comes from a manufacturer or provider (I will refer collectively to them as the "manufacturer"), who is involved in making decisions regarding the device's design and functionality as well as the needs it is supposed to meet. The user, in turn, is involved in selecting the tool and deciding how to use it in practice.

In the case of smart glasses, the manufacturer does not impose its use of smart glasses upon the user. Instead, the user is the person who chooses to use smart glasses – and which ones to select. Without the user's choice of device and without the user's decision to deploy such a device, the video, image, recording etc. would not exist. Any "processing" – if it is indeed processing of personal data (see below IV) – solely exists because the user enabled it. By choosing the device (i.e. smart glasses, and why kind of smart glasses more specifically), the user determines the means; by choosing to deploy the device (by putting the smart glasses on the user's face and activating certain functionalities), the user pursues a particular goal and thus determines the purpose.

This points towards **the user being a controller** by default, but the way in which the processing is configured, **certain processing activities may lead to different roles**, also for the manufacturer.

For instance, where a device's processing happens locally (i.e. stays within the physical smart glasses themselves), it may be that there is no processing at all by (or on behalf of) the manufacturer, such that any "processing of personal data" is likely entirely under the sole control of the user.

However, if any (part of the) processing takes place remotely, through the servers of the manufacturer or on its behalf, the assessment can become more complex:

- The manufacturer will typically be **sole controller** for the processing of usage data for the purposes of service improvement and for the security of a service, as the processing in question is not for the sole purposes of delivery of the service to the user;

- For the purposes of delivering the service to the user, the manufacturer could even be considered as **processor** for any processing that is carried out purely on behalf of the user (as the manufacturer does not determine why, when or how a user might decide to capture video or audio regarding an identified or identifiable bystander);

- Finally, based on CJEU case law[18], there may be a very limited form of **joint controllership** purely for the specific phases of collection and transmission of data by the user to the manufacturer, excluding any processing carried out for the user (as controller) by the manufacturer (as processor) as well as any processing carried out by the manufacturer for own purposes, i.e. as sole controller.

In practice, if a user instigates the processing (by the manufacturer) of personal data of others in support of the service to the user (for instance, cloud uploads of videos for backup purposes, live transcription or translation), the processing is at least primarily for purposes determined by the user. The result is that the

[18] CJEU, 29 July 2019, *Fashion ID*, C-40/17, EU:C:2019:629, para. 96.

user must be deemed as controller and the manufacturer as processor, except to the extent that the personal data in question is also processed separately for other purposes by the manufacturer.

The fact that the manufacturer has envisaged that the product could be used for various purposes does not make it a joint controller for the user's own processing as holding otherwise would risk transforming a large range of service providers that merely facilitate processing into joint controllers. For example, a cloud hosting provider designs a hosting service with a view to helping customers achieve certain processing activities; should a user select that provider, it uses the provider's hosting service for its own purposes, not for purposes that converge with those of the provider. The same reasoning applies to smart glasses: the manufacturer designs the product with a view to helping users achieve certain processing activities, and a user selecting that manufacturer's smart glasses uses their processing capabilities for its own purposes.

IV. Is it all even processing of personal data?

A frequent issue regarding AI-enabled devices is that there is a general assumption by the public and authorities that **everything** that they do involves the processing of personal data, and that everything that the smart glasses capture (audio and video) will be used to train AI models, including the content of any conversation.

Such an assumption does not necessarily reflect technical or economic realities regarding the functioning of smart glasses. High-definition video being transmitted constantly would entail an enormous cost for bandwidth and storage, and it would drain the battery of the smart glasses very rapidly.

In addition, the core type of information being processed is ambient information, based on various sensors, but it does not all relate to natural persons who are identified or identifiable from the manufacturer's perspective – a core assessment that case law has shown to be entity-specific and to require moving away from assumptions. The unfortunately frequent presumption that imagery or audio involving natural persons generally constitutes personal data is hard to reconcile with the issue of identifiability, as explained by Recital 26 of the GDPR and CJEU case law.

In this context, it is not only important to define which person or entity should be viewed as controller in relation to certain processing of personal data, but also to carve out from the analysis any information regarding which the range of data protection obligations do not even apply.

The distinction made above between the user's perspective and the manufacturer's perspective becomes critical here.

IV.1. Relative identifiability

For information to be "personal data", it must relate to an "identified" or "identifiable" natural person, according to Article 4(1) GDPR.

In its essence, "identifiable" means "capable of being identified", and "identified" must in my view be considered as the combination of the following:

(i) the ability to attribute certain information to a **natural person**,

(ii) the ability to **distinguish** that person from any other persons (= i.e. so it is a **specific** natural person, not just any natural person) and

(iii) that distinction must be of such a nature as to make it possible to **act upon or in relation to such person**.

The European Data Protection Board (EDPB), in its Anonymisation Guidelines that it opened up for public consultation in July 2026[19], has taken a largely similar view in theory:

> *"To identify a natural person means to distinguish them from others within a given context, consequently making it possible to treat them differently from those other people."*

As set out in my critical analysis of those Anonymisation Guidelines, the EDPB is not consistent in its own application of those criteria throughout those same Guidelines. Yet they do provide confirmation that in theory at least, supervisory authorities consider that the mere linking of information with a natural person is insufficient; some form of action must also be possible.

Identification and identifiability, however, are **relative** notions, as confirmed by Recital 26 GDPR and case law of the CJEU (in particular the *Breyer*[20], *OC v Commission*[21] and *SRB*[22] judgments). Whether information is "personal data" thus depends on the perspective of the person or entity being examined and whether that person or entity is capable of identifying the data subject.

As I wrote in my analysis regarding incidental processing:

> *When examining whether a potential controller is indeed processing personal data, one must first assess whether that potential controller (i) has (lawful) means of identifying a natural person or (ii) has (lawful) means of obtaining additional information from a third party in order to identify the natural person. If these conditions are not met, information is not personal data from that potential controller's perspective – even if that information seems to relate to a natural person.*
>
> *In addition, the "reasonableness" of those means signifies that* ***merely hypothetical means are irrelevant****. Proportionality dictates that these means of identification must be realistic, not dependent upon the alignment of a wide range of other conditions.*

[19] European Data Protection Board, Guidelines 02/2026 on Anonymisation of 7 July 2026.

[20] CJEU, 19 October 2016, *Breyer*, C-582/14, EU:C:2016:779.

[21] CJEU, 7 March 2024, *OC v European Commission (OLAF)*, C-479/22 P, EU:C:2024:215.

[22] CJEU, 4 September 2025, *EDPS v SRB*, C-413/23 P, EU:C:2025:645.

This means that data being collected by way of smart glasses has to be examined from two perspectives:

- **Identifiability from the user's perspective**, with the user as controller: any information being collected that relates to natural persons who are identified or identifiable from the user's perspective is "personal data" from the user's perspective, and the user's obligations as controller apply to all (but only) information that clears this threshold.

- **Identifiability from the manufacturer's perspective**, with the manufacturer as controller: insofar as the manufacturer acts as controller, information that it processes for "own" purposes (e.g. AI training, service improvement) is only subject to data protection rules if it is personal data from the manufacturer's perspective, i.e. taking into account means reasonably likely to be used.

Where the manufacturer acts as processor, its own perspective is irrelevant, due to the fact that the processing occurs **on behalf of the user** and under the user's authority. In this context, identifiability is assessed purely from the user's perspective. The EDPB confirms this point of view, stating in its Anonymisation Guidelines that *"the applicable perspective used for a particular entity depends on whether they themselves determine the means and purposes of the processing"* [para. 15].

As regards the manufacturer's perspective, it is also important to stress that so far, at least two supreme administrative courts (in the Netherlands[23] and in Poland[24]) have held that **the classification of information as personal data cannot be presumed, but must be demonstrated** by a supervisory authority. In other words, it is not enough to assume that if a smart glasses manufacturer has other services involving the processing of personal data (e.g. social media, e-mail, identity or other services) it will be lawful for the manufacturer to use data from elsewhere to enable identification. For those subject to the Digital Markets Act or DMA, there are even restrictions on the combination or cross-use of personal data between services.

IV.2. Ambient data capture and patterns relevant for AI training & functioning

A first category of information that is of a nature to escape the "personal data" classification is that of ambient data.

In the case of AI vision models, for instance, the data captured to help a user of smart glasses navigate around a city is a combination of user location (which can be personal data) with other data, such as geometric shapes and objects within the field of vision of the smart glasses. Assistive technology intended to help the user understand that a car is approaching does not need information about who is within the car in question; navigational assistance does not need to register the faces of passers-by but merely needs to register the fact that there are passers-by walking near the user.

[23] Dutch Council of State, decision of 29 July 2026, 202401622/1/A3, NL:RVS:2026:4403.

[24] Polish Supreme Administrative Court *(Naczelny Sąd Administracyjny)*, 16 October 2025, III OSK 2595/22 - Wyrok NSA.

As a result, the manner in which they work does not require personal data.

This observation is equally relevant in relation to information that could otherwise be classified as "special category" personal data, commonly called "sensitive" data (e.g. a passer-by with a prosthetic limb; a sneezing person; someone wearing a religious symbol; people attending a political rally). The manufacturer's use of ambient data is not made with the purpose of analysing who was attending the political rally, nor is there even any attempt to identify any natural person. The actual manner of working is detached from identification in such a way that it is not personal data to start with (here: from the manufacturer's perspective), let alone a special category of personal data.

IV.3. Biometric identification versus biometric data: EU AI Act & GDPR

This difference between object capture and identification has moreover been recognised by the EU legislator.

The EU's AI Act (Regulation 2024/1689) defines as a "remote biometric identification system" any *"AI system for the purpose of identifying natural persons, without their active involvement, typically at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database"* (Article 3(41) AI Act), a category that is highly restricted for law enforcement purposes and that is a "high-risk AI system" covered by Annex III, paragraph 1 of the AI Act.

The GDPR similarly includes in the more highly regulated "special categories of personal data" the processing of *"biometric data for the purpose of uniquely identifying a natural person"* (Article 9(1) GDPR).

In other words, identification based on the recording or analysis of images cannot be automatically assumed. Were that the case, there would have been no need for the EU legislator to make a distinction between biometric systems or data in general and biometric systems or data **for identification purposes**.

Therefore, capturing a person's likeness by way of a photo or video recording is not biometric identification.

IV.4. Voice capture, and syllables as equivalent to tokenisation

This reasoning does not merely apply to photography and video, but also to audio. Some concerns have been voiced in relation to voice capturing, alleging that features built around ambient sensing for e.g. real-time translation or transcription risk giving a manufacturer access to private oral conversations.

Language processing does not work based on the identification of the speaker, but rather on breaking down sounds and then converting them into blocks to enable their interpretation. The key focus lies then on understanding the meaning (the words themselves) rather than getting a readout of the voice itself. In other words, the focus is not voice recognition but word recognition.

In the context of the analysis of whether the training of large language models involved the processing of personal data, I previously wrote that the tokenisation process changes the nature of the information "processed", such that it is no longer "information relating to an identified or identifiable natural person" but a series of small blocks of text.

A similar observation can be made in relation to the way in which audio is processed: by breaking it down into sounds and recomposing meaning, any "identifying" aspects of the initial audio (the voice's characteristics – pitch, rhythm, intonation, timbre etc.) being immediately stripped away to focus on the barebones building blocks of the content.

While some may claim that this stripping away of acoustic characteristics is processing of personal data, it bears reminding that "personal data" requires the information to relate to an **identifiable or identified** natural person, and such assessment is made differently for the user and for the manufacturer. From the manufacturer's perspective, identification of the speaker is disproportionately complex (likely even unlawful if the DMA applies to the manufacturer) without the user's intervention and thus not "reasonable".

As for the content itself of the conversation, the observations made regarding large language models apply equally: these become textual tokens, just as the audio was broken down into acoustic tokens.

In other words, who said something is of no relevance to the process of transcription, nor is an actual understanding by the AI system (or manufacturer) of what was said; what matters is which sounds were made and how they fit together.

Importantly, this process is not unique to smart glasses, in the light of the broad availability of transcription tools (e.g. on smartphones) and dedicated audio recording devices.

As in the case of image or video processing, one should avoid assuming that all processing of audio involves the processing of personal data.

IV.5. Non-personal data from the manufacturer's perspective as controller

These various elements point to an important observation: for the manufacturer, the information it is led to process for its own purposes may not even be personal data.

This stems from the fact that the information does not relate to a natural person who is reasonably identifiable from the manufacturer's perspective, whether:

- because identification is prohibited by law (e.g. where the DMA prevents combination or cross-use, which could have otherwise contributed to identification),
- because identification would require disproportionate effort (in which case it is not "reasonable" in accordance with *Breyer* and *SRB*) or
- because identification requires access to additional information in the hands of the user (who has no reason – and may potentially not even be permitted – to share such additional information with the manufacturer).

In other words, the actual processing of personal data takes place on the user's side (or on the user's behalf).

IV.6. Bystanders & non-personal data from the user's perspective as controller

Even the scope of processing by the user can be significantly more limited than one might assume, when taking into account the fact that **bystanders may not be identified or identifiable from the user's perspective**. This will notably be the case for the majority of passers-by on the street, or members of a broader crowd.

As I wrote in my previous analysis on incidental processing:

> *"If a camera is used to film a singer on the metro, a particular passenger might be invisible to the camera until he or she gets up to leave the metro at the next stop. The appearance on camera of this bystander clearly relates to a natural person, but is it an identifiable natural person? Without additional information about the person, identifiability will in practice not be possible.*
>
> *It may for instance be that the person behind the camera knows the bystander, or that by chance the camera captures the name and professional details (company, role) of the bystander on film in the form of a name tag or lanyard. Such circumstances cannot be presumed, however.*
>
> *Similarly, if a journalist interviews a public figure in a restaurant, the interview's audio recording might pick up on background chatter or even on the moment when a fellow diner asks the interviewee for an autograph. This information, the audio recording, clearly relates to natural persons, but aside from the interviewee, the other natural persons cannot be said to be identifiable for the interviewer.*
>
> *The same issues arise in the case of tool-assisted live translations or text transcriptions, such as through the use of smartphone apps or smart glasses to interpret or transcribe one person's speech. The information being captured incidentally regarding other persons, such as neighbours in the audience, is not meant to be captured, but without additional information they are themselves not identifiable."*

As a result, much of the information regarding bystanders is not personal data, even from the user's perspective.

IV.7. Dissemination of footage and (re)identification

All of the above means that much of the data being processed through smart glasses **is not covered by the GDPR**, even from the user's perspective.

Yet the user's actions may create the circumstances for identification to become possible. For instance, publication of footage increases the likelihood of a recipient being able to identify the natural person.

This has legal consequences. In accordance with the CJEU's *Scania*[25], *OC v Commission*[26] and *SRB*[27] judgments, the making available of information to a third party can indirectly make a natural person identifiable, if that third party does in turn have means reasonably likely to be used to enable identification.

In other words, publication can in certain circumstances transform the handling of non-personal data (due to non-identifiability) into processing of personal data.

V. Transparency obligations and the purpose of indicators

Today, several smart glasses come with a visual indicator in the form of a light-emitting diode, an LED, that lights on when optical or audio sensors are active. Whether such an LED is legally required or even desirable, however, is a more open and complex question than it may seem.

Ultimately, the issue of LEDs or other indicators comes down to the question of **transparency**, one of the key data protection principles alongside e.g. data minimisation and security.

It is worth noting first that Article 50 of the AI Act is not relevant in this particular respect. While it is an important obligation in terms of transparency regarding AI systems, its scope is limited to AI systems *"intended to interact directly with natural persons"*, *"generating synthetic audio, image, video or text content"* or *"generat[ing] or manipulat[ing] image, audio or video content constituting a deep fake"*, as well as to any *"emotion recognition system or a biometric categorisation system"* – none of which is appropriate in the context of smart glasses. For instance, while the **user** of smart glasses may be interacting directly with an AI system, it is harder to claim that any person within the field of vision of the camera or within range of the audio sensors is "interact[ing] directly" with the AI system, as smart glasses do not provide any output to them but rather to the user.

V.1. GDPR transparency requirements

Articles 12 to 14 of the GDPR, on transparency, require the controller (not anyone else) to provide data subjects with clear and comprehensive information, including:

- the identity and contact details of the controller;
- the purposes of the processing and its legal basis;
- the categories of personal data processed:
- the recipients or categories of recipients;
- the retention period; and
- information about data subject rights.

---

[25] CJEU, 9 November 2023, *Scania*, C-319/22, EU:C:2023:837, para. 49.

[26] CJEU, 7 March 2024, *OC v European Commission (OLAF)*, C-479/22 P, EU:C:2024:215, para. 48.

[27] *SRB*, paras. 84-85.

Pursuant to Article 12(1) GDPR, this information must be provided in a **concise, transparent, intelligible, and easily accessible form**, using clear and plain language.

The GDPR does not impose any specific technical or formal requirement regarding the manner in which transparency must be achieved. Regulators have filled that space by suggesting ways to ensure transparency, by notably suggesting ways in which to make layered information permissible. The Article 29 Working Party (WP29), predecessor to the EDPB, suggested in its Transparency Guidelines (later endorsed by the EDPB) that *"a layered approach may be followed by controllers where they opt to use a combination of such methods while ensuring that the most important information […] is always conveyed in the first modality used to communicate with the data subject"*[28], with such "most important information" needing to include *"the details of the purposes of processing, the identity of controller and a description of the data subject's rights"* and having to be *"directly brought to the attention of a data subject at the time of collection of the personal data"*[29].

Controller identity and purposes must therefore be made clear in a first layer or set of information made available to data subjects.

V.2. Smart glasses and how to provide transparency

As noted above, while the manufacturer may in theory appear to be acting as controller, the reality of the way in which data is used by the manufacturer for own purposes is that the information does not constitute personal data from its perspective, or at most, only a minor proportion of the data might be personal data.

Similarly, while the user may in theory appear to be acting as controller, practical issues regarding identifiability make much of the data captured through smart glasses non-personal data – at least as long as the data remains private and not disseminated.

In this context, transparency from a GDPR perspective appears to be required mainly if the user intends to make any footage or recordings available to third parties.

Parallels can be found in this respect in the way in which photography and filming are handled in a public setting. Photographers, in particular professional photographers, will reach out to identifiable bystanders, but hobbyist photographers or people taking holiday photos are unlikely to reach out if the intention is to keep the photos private.

It is not necessarily a widespread reflex. Smartphone users pretending to be browsing or gaming on the metro or bus while actually filming covertly do not go around telling people of their identity and the purposes of their processing; even those clearly pointing their phone camera at a singer on the street, a brawl, or a scene do not necessarily walk around informing passers-by of their identity. Yet the issue then becomes one of **education, awareness and civic behaviour**: if a user of a device with recording

[28] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01, 11 April 2018, page 21.

[29] *Ibid.*, p. 19.

capabilities, whether a smartphone, smart glasses or smart headphones intends to capture anything with a view to further dissemination, reaching out is not only legally required but also good manners.

Indicators such as LEDs are not the answer from a GDPR perspective, though, and their use can even create more confusion.

V.3. Indicator meaning and LED fatigue

For the reasons set out above, smart glasses are not "continuous surveillance" devices. The data collected is not personal data from a range of perspectives, and the user's perspective on identifiability and the intended use (e.g. dissemination) contribute to the possibility to consider it as personal data in certain regards.

Yet they are devices that *can* record. Should there then be some form of visual indicator?

Nothing in the GDPR requires such an indicator. It is even unclear on which basis data protection regulators could require a manufacturer to include such an indicator, both in relation to processing of non-personal data and in relation to processing of personal data for which it is not the controller (situations to which Article 25 GDPR, i.e. data protection by design and by default, does not apply).

Part of the issue is that from the perspective of the GDPR, an LED **does not reveal anything regarding the identity of the controller or the purpose of processing**. It is therefore **not** a substitute for the provision of information under Articles 13 & 14 of the GDPR.

Moreover, it is **unhelpful and even misleading** from the perspective of awareness of processing of personal data. As explained above, there are a range of situations in which the optical sensor – the camera – is **not triggering the processing of personal data but rather data concerning unidentifiable natural persons**. In other words, the fact that identifiability is itself relative means that the manufacturer cannot determine in advance in which scenarios the user's use of functionality of smart glasses will trigger the processing of personal data.

Activating the LED anytime a certain functionality is on therefore risks **creating incorrect expectations of applicability of data protection rules**.

The broader consequence is that **LEDs become meaningless**, because they are used to indicate processing of personal data when there is actually none.

Even if one were to hold that LEDs need to be activated just in case the information might be personal data, this will have another perverse effect, namely LED fatigue. LEDs will then be on almost permanently, such that bystanders will become used to seeing LEDs on, even as they become aware of the fact that an active LED does not necessarily mean that there is processing of personal data.

Put differently, alerting bystanders to the possibility of processing of personal data in too many scenarios that do *not* involve such processing degrades awareness and alertness rather than enhancing it.

This is not merely hypothetical, as even in healthcare the phenomenon of "alarm fatigue" or "alert fatigue" is widely studied, whereby repeated exposure to warnings gradually reduces attention (in that

case, attention of healthcare professionals who, confronted with "frequent or non-actionable alarms", can get desensitised or become less responsive to alarms[30] and increases the chance that patients will be harmed[31]). If alarm fatigue can happen in healthcare, a critical sector, LED fatigue must not be dismissed as unlikely.

VI. Better solutions for information and to tackle abuse

The above analysis shows that (i) smart glasses are dual-use devices, not covert surveillance equipment; (ii) the user is the controller for the actual use of the smart glasses; (iii) the data captured is in many instances not personal data, from the manufacturer's perspective and even in many cases from the user's perspective; (iv) LEDs are an inadequate and even misleading means of informing data subjects about the processing of personal data.

This does not mean, however, that any use of smart glasses is permitted, that abuse can be carried out with impunity or that no information ever needs to be provided to individuals whose voice or likeness is captured.

Yet bad faith or unlawful use of smart glasses cannot be presumed. Data protection rules require accountability as well as transparency and regulatory oversight as a means of tackling compliance; they do not demand that every situation of potential processing of personal data be regarded with suspicion or assumed to be unlawful.

In this context, one must consider a broader approach:

- The misuse of smart glasses for voyeurism is already unlawful from many perspectives, be it under specific criminal law provisions on voyeurism, under laws on image rights or the right of personal portrayal or under data protection rules.

- If law enforcement is underequipped to handle complaints in this respect, there is a broader societal debate to be had about resources for policing, but nothing in data protection law warrants product bans as a means of tackling such abuse.

- Data protection authorities can handle complaints and fine individuals for their own non-compliance with data protection rules – and this has already been the case in many if not most EU Member States. If a user uses smart glasses to record an identifiable natural person but does not comply with e.g. the transparency obligation, handling such a complaint is not just possible – it is desirable with a view to promoting good and lawful practices in relation to transparency for the processing of personal data.

---

[30] See e.g. Michels EAM, Gilbert S, Koval I, Wekenborg MK. Alarm fatigue in healthcare: a scoping review of definitions, influencing factors, and mitigation strategies. BMC Nurs. 2025 Jun 20;24(1):664. doi: 10.1186/s12912-025-03369-2. PMID: 40542361; PMCID: PMC12181921.

[31] See Alert Fatigue. PSNet [internet]. Rockville (MD): Agency for Healthcare Research and Quality, US Department of Health and Human Services. 2019.

- The greatest burden should lie on the user, provided the manufacturer can show that it has taken measures to limit the probability of it processing personal data for own purposes *or* that it has taken measures to enable data subjects to be aware of the processing of personal data that it actually carries out.

- Transparency should not be achieved by way of LEDs, nor should LEDs even be required due to the true risk of dilution of their message as a result of overactivation in scenarios that do not involve the processing of personal data.

- Instead, users should be educated by governments and regulators to understand the rules regarding transparency, both from a legal perspective and good social etiquette (for instance: "ask before sharing"). This is a far broader issue than solely regarding smart glasses, and there is no legal justification for requiring manufacturers to assume responsibility for improving awareness thereof.

Data protection law should not be itself twisted to tackle abuse of a dual-use technology. Education and enforcement, not a shift in responsibilities, are the better answer.