Statement 01/2026 on Smart Glasses

Adopted on 13 October 2026

The European Data Protection Board has adopted the following statement:

1 Introduction

1 As smart glasses become widely available and more frequently used, they create new opportunities for communication, assistance, and innovation, while also raising significant questions for the protection of personal data and the rights of individuals. This statement sets out the EDPB's preliminary reflections on the privacy implications of smart glasses, with particular regard to their capacity to process personal data in ways that may be difficult for data subjects to perceive or control.

2 For the purposes of this document, smart glasses are defined as wearable devices which often look like regular glasses or sunglasses, and which incorporate computing capabilities and features such as cameras, speakers, microphones, and software or applications, including artificial intelligence systems for various purposes (e.g. translation or object identification). They may connect to the internet, external devices, or mobile applications to enable additional functionalities. They may be operated through voice command or other input technologies, such as wristbands detecting hand gestures.

3 Where smart glasses capture, collect, record, adapt, store, or otherwise process any information relating to an identified or identifiable natural person, they process personal data, and the processing is therefore subject to the GDPR[1].

2 Use Cases and Specific Risks of Smart Glasses

4 Functionalities vary between smart glasses on the market. Common use cases include listening to music, making or receiving a phone call, taking photographs or recording videos, accessing real-time translation services, and live streaming. Some smart glasses may also provide 'augmented' experiences by displaying information to the wearer.

[1] Except in cases listed in Article 2(2) GDPR, such as where the processing is carried out by a natural person in the course of a purely personal or household activity (see also section III of this document)

5 These functionalities may be used, for example, as a hand-free tool for a wide range of needs and in various personal or professional contexts, such as for communication, navigation, disability aid (for example by providing audio assistance and real-time hazard awareness), documentation of events, or the creation of content for social media platforms[2]. New functionalities continue to emerge as the technology develops.

6 However, some of the most common uses of smart glasses, particularly recording, live streaming, and the sharing of footage online, may give rise to specific and significant concerns for the protection of personal data[3], and also other rights and freedoms[4] such as the rights to privacy, security, freedom of expression and freedom of movement.

7 This is due to the way in which smart glasses are worn and operate. Unlike many other recording devices, they allow a near invisible or hidden collection, storage, and other forms of processing of personal data since they can be difficult to distinguish from ordinary eyewear. Therefore, they can facilitate the non-authorised recording of data subjects. In addition, some smart glasses may have advanced microphones, which can record background conversations to which the user is not participating. In addition, their possible use together with facial or voice recognition systems raises unprecedented questions regarding societal choices and poses a high risk to the rights and freedoms in public spaces.

8 Even if the device could be identifiable as smart glasses, individuals may still oppose being filmed or recorded, including because they are uncomfortable with the possibility of this taking place[5]. This could also result in a subtle social effect, where individuals alter their behaviour, suppress spontaneity, and conform to social norms perceived to be more socially acceptable due to their perceived threat of unvetted surveillance.

9 Users of smart glasses should always ensure that they respect the privacy and dignity of other individuals, and that they do not undertake any actions that could cause prejudice to them with their smart glasses. Explicitly informing other individuals of the use of smart glasses is relevant in this respect.

10 The use of smart glasses may also be especially sensitive in certain contexts, such as in a medical facility, schools and other places where minors are present, changing rooms, swimming pools or beaches, toilets, or other private or intimate situations. Use in the workplace may raise concerns about employee monitoring and the confidentiality of the entity's information (including trade secrets and intellectual property). In such situations, recording or audio capture may be inappropriate, or prohibited under national law or local rules[6].

---

[2] Compendium of Approaches on Smart Glasses, G7 Data Protection Authorities, June 2026, p. 2, https://www.cnil.fr/sites/default/files/2026-06/g7_dpas_compendium_of_approches_on_smart_glasses.pdf

[3] Working Paper on Extended Reality, International Working Group on Data Protection in Technology, 16 June 2026, available at https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20260616-WP-Extended-Reality.html?nn=253562
See also Press release of the Conference of Data protection authorities of the Federal Government in Germany and the Länder of 24.09.2026: https://www.datenschutzkonferenz-online.de/media/pm/DSK_PM_3_Zwischenkonferenz_2026.pdf

[4] See Charter of fundamental rights of the European Union

[5] Swedish Authority for Privacy Protection (IMY), 'Smart glasses', https://www.imy.se/en/individuals/camera-surveillance/to-be-a-controller-of-personal-data/smart-glasses/

[6] For example, this has prompted some establishments to restrict the use of smart glasses on their premises. See the compendium of Approaches on Smart Glasses, G7 Data Protection Authorities, June 2026, p. 2, https://www.cnil.fr/sites/default/files/2026-06/g7_dpas_compendium_of_approches_on_smart_glasses.pdf

3 General Considerations for Compliance with Data Protection Law

3.1 Identification of the controller

11 Depending on the circumstances, responsibility for processing personal data through smart glasses may arise for different actors, including the user of the smart glasses, the producer of the device, or the provider of a linked application or service (including AI systems). In some cases, one actor may act as sole controller; in others, two or more actors may qualify as joint controllers. The assessment will depend on who determines the purposes and means of the processing[7].

12 The qualification of the user under the GDPR depends on their use of the smart glasses.

13 The user of the smart glasses is not subject to the GDPR, provided that the user's actions are carried out in the course of a purely personal or household activity, outside any professional or commercial context (household exemption[8]). This is the case, for example, when the user shares a photo or video with a family member or a friend only[9], or uses the device for personal translation in a private context.

14 This exemption must, however, be narrowly construed[10] and be considered on a case-by-case basis in light of the circumstances of the processing. For example, it would not apply if the photo or video is shared to an indefinite number of persons on a public social media account[11], or if smart glasses are used in the course of official, professional, political or other non-personal activities. In these situations, the user would qualify as a controller or joint-controller and therefore has to comply with all of the obligations foreseen by the GDPR, notably transparency.

15 In any case, the user who is recording voice or images with their smart glasses might be subject to other laws. For instance, some uses may be subject to criminal law.

16 It is important to note that the GDPR does still apply to controllers or processors which provide the means for processing personal data for such personal or household activities[12], such as the producer of the smart glasses or the provider of a linked application or service (including AI systems).

17 The producer of the smart glasses or the provider of a linked application or service (including AI systems) may be considered as independent or joint controllers, where they determine, alone or jointly, the purposes and means of the processing. This is notably the case when the provider of the AI functionalities of the smart glasses processes personal data in order to

---

See also a further initiative in the Free and Hanseatic City of Hamburg, Germany, to propose a ban on smart glasses in public transport and swimming pools (here);

[7] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, adopted on 7 July 2021

[8] Article 2(2)(c) GDPR

[9] EDPB Guidelines 3/2019 on processing of personal data through video devices Version 2.0, adopted on 29 January 2020

[10] Case C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů*, ECLI:EU:C:2014:2428

[11] Case C-101/01, *Lindqvist*, ECLI:EU:C:2003:596 and Case C-345/17, *Buivids,* ECLI:EU:C:2019:122

[12] Recital 18 GDPR

provide the user with an answer about its surroundings, for example by analysing an image from the glasses' camera feed in which other persons appear.

18 Where such actors are controllers, they are responsible for the compliance of their processing operations with the GDPR. Consequently, they should not rely on the users' actions to meet their own GDPR obligations, such as transparency toward other individuals whose data might be processed when the smart glasses are being used.

19 Additionally, where they further process personal data for a new purpose, controllers must ensure that this new purpose remains compatible with the purpose for which the data was originally collected.[13] In assessing compatibility, particular attention should be given to the context in which the personal data was collected, especially when the data subjects have no relationship with the controller.

3.2 Transparency

20 Compliance with the transparency requirements of the GDPR[14] presents a major challenge in the context of smart glasses. Transparency is essential to make data subjects, whether they are users or bystanders (also referred to as 'non-users'), aware that their personal data are being processed, and to what extent.[15] Such information is a necessary precondition for individuals to be able to exercise their rights as data subjects.

21 The discreet nature of smart glasses means that non-users may be unaware that personal data relating to them is being processed[16], by whom it is carried out, and for what purposes. Some functions, such as translation services or use of AI features, may also be particularly invisible to bystanders.

22 The current state of the art with regards to indicators on smart glasses leave many non-users unaware that their data is being processed.

23 Traditional transparency notices, which can be used to inform users and usually contain information about the data processing, do not seem sufficient or appropriate to inform non-users in the context of smart glasses. This is particularly true when the controller is the producer of the smart glasses or the provider of a linked application or service (including AI systems), and they process personal data relating to non-users, since they have no relationship with these persons and are not able to contact them.

24 Given the current state of the art, controllers and producers should consider combining a broad range of transparency mechanisms when designing and developing smart glasses, including measures that provide by default in-the-moment transparency that processing is taking place[17].as well as providing the required information under GDPR[18]. Measures relevant to

[13] Articles 5(1)(b) and 6(4) GDPR
[14] Articles 12 and 13 GDPR
[15] Recital 39 GDPR
[16] Compendium of Approaches on Smart Glasses, G7 Data Protection Authorities, June 2026, p. 6, https://www.cnil.fr/sites/default/files/2026-06/g7_dpas_compendium_of_approches_on_smart_glasses.pdf
[17] Such measures should be impossible or difficult to disable (taking into account the state of the art) and easy for bystanders to notice in practice
[18] Such as the information required under Articles 12, 13, and 14

inform non-users that processing is taking place (and that may not necessarily address all relevant transparency challenges) may include among others, a combination of:

- **Visual or LED indicators** – To be effective, such indicator[19] should be visible in many lighting conditions and sufficiently noticeable to attract the attention of individuals within the field of collection. It should be activated long enough to make sure individuals understand that the smart glasses are recording or capturing images/video for processing by an AI assistant. The indicator could function in different ways depending on the functionality being used (for example: a prolonged activation when recording images or sound; flashing when a picture is being taken; etc.), and it should not be possible to record information when the indicator is covered.
- **Audio indicators** – Audio indicators and voice activation requirements (i.e. requiring the user to dictate the command out loud) could also increase the awareness of bystanders, as used on other photo or video devices (for example: a click sound when a picture is being taken[20]).
- **Smartphone based proximity notification**– Several mobile applications detect nearby smart glasses by recognising broadcasted Bluetooth identifiers associated to glasses manufacturers. Currently this type of signal can only be used to detect nearby glasses (whether they are recording or not), but device manufacturers could also consider sending specific signals when devices are recording, therefore allowing nearby users to be notified. In any case, such notifications should not be the sole method of providing transparency, as this would exclude individuals who do not have such an application active at all times, and also because it should always be possible for an individual to accept or refuse to receive such a notification on their device. Additionally, this application should be designed in a way that it cannot lead to the tracking of the smart glasses' users.
- **Design of the smart glasses –** In addition to indicators when functionalities of the smart glasses are activated, other clues in the design of the glasses could be envisaged to help non-users distinguish smart glasses from regular glasses[21].

25 Whenever compliance with the transparency requirements of the GDPR relies on technical measures, it is necessary to ensure that they are effective, impossible or difficult to circumvent, and updated whenever necessary.

26 The EDPB recommends the development of industry-wide standards and awareness raising campaigns to ensure that individuals identify smart glasses and understand what type of data processing may be occurring in different situations.

3.3 Legal basis

[19] Producers should also consider that LEDs might be difficult or impossible to notice for individuals who are visually impaired, and that a white LED generally could be mistaken for a reflection or solar glare.

[20] Japan's Ordinance on the Healthy Development of Juveniles, which was amended in 2015, even bans the muting of shutter sounds on smartphones.

[21] As per Recital 78 GDPR, producers of the smart glasses and providers of linked applications or services are encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, make sure that controllers and processors are able to fulfil their data protection obligations.

27 Any processing within the scope of the GDPR must have a valid legal basis under Article 6(1) GDPR[22]. Given the complexities and variations of data processing via smart glasses, the validity of any chosen legal basis is likely to require a case-by-case assessment taking into account the local applicable laws, the specific processing and its context, and any further use of the data.

28 Consent under article 6(1)(a) GDPR may be the legal basis of the processing, where the conditions of Article 7 GDPR are fulfilled[23]. Some national laws protect the right to one's image, which requires obtaining consent of a person for the reproduction and public distribution of their image: in these situations, consent will likely be the most appropriate legal basis for the processing.

29 However, where the controller is the producer of the smart glasses or the provider of a linked application or service (including AI systems), and they process personal data relating to non-users with whom they have no relationship, it would be difficult to obtain their freely given, specific, informed and unambiguous consent as required under Article 7 GDPR.[24] Consent obtained after collection, for example following the recording, would not be valid as the legal basis must exist prior to and during any processing.

30 Reliance on Article 6(1)(f) legitimate interests as a relevant legal basis would require a careful case by case analysis in light of data subjects' rights, freedoms, and reasonable expectations[25]. Considering the nature of the data, the context of the processing and the current insufficient transparency, which negatively impacts the reasonable expectations of non-users[26], sufficient mitigating measures will need to be put in place in order to achieve a fair balance between the interests involved. This would be particularly difficult to demonstrate for further processing for commercial purposes that go beyond providing the service explicitly requested by the end-user, or for AI training[27], which bystanders wouldn't expect, especially if they are not aware of the initial data collection. Even if the conditions of Article 6(1)(f) are met, controllers would also need to ensure that all data subjects are able to object[28] at any time, which can prove difficult in many cases.

3.4 Other data protection aspects

[22] One of the exemptions under Article 9(2) GDPR should also apply if special categories of data are processed.
[23] EDPB Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, adopted 4 May 2020
[24] Ibid. ; see also Data Protection Commission, Guidance on the Use of Body-Worn Cameras and Action Cameras, January 2020, https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20on%20Body%20Worn%20Cameras%20or%20Action%20Cameras_Jan20.pdf
[25] To rely on Article 6(1)(f) GDPR, three cumulative conditions must be fulfilled, namely (i) the interest pursued must be legitimate, (ii) the processing must be necessary, and (iii) the legitimate interest must not be overridden by the interests or fundamental rights and freedoms of the data subject. See EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0, 8 October 2024.
[26] In relation to reasonable expectations, meeting transparency requirements does not, in itself, mean that data subjects can reasonably expect the processing, particularly for further processing such as AI training.
[27] EDPB Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, adopted 18 December 2024; See also case C-252/21, *Meta v. Bundeskartellamt*, ECLI:EU:C:2023:537, para. 123
[28] Article 21(1) GDPR

31 The use of smart glasses may also raise questions under other provisions and principles of EU data protection law, depending on the specific functionality, context of use, and type of data processed. In this respect, a number of the questions associated with smart glasses also arise in relation to other technologies: for example, video doorbells, dash cams, consumer body worn cameras[29], and voice assistants (which can be in a home, or embedded on a phone, or on smart watches[30]). Moreover, like with any video-recording technology, footage can be shared on public social media accounts, and is sometimes used for behavioural analysis and profiling, or for a secondary purpose including AI training[31].

32 Without addressing these issues in detail, the EDPB recalls in particular that controllers and, where applicable, processors must also take account of other relevant obligations, including data protection by design and by default, security of processing[32], the processing of special categories of data[33], the use of processors and sub-processors[34], and transfers of personal data outside the European Union[35], and the protection of children. Particular attention should be paid to the protection of children, who may be less aware of the presence or implications of smart glasses and therefore more vulnerable to covert or intrusive processing of their personal data. Additionally, in some circumstances[36] smart glasses may be regarded as terminal equipment to which the ePrivacy framework may also be applicable. This is the case specifically when sensors collecting, locally storing and processing information (e.g. images, videos or sound) are embedded in the device, or where the information is by default made available to a remote server (e.g. a social network profile or a webpage).

33 In addition, controllers should help ensure that data subjects can effectively exercise their rights and retain meaningful control over their personal data[37]. The EDPB encourages the use of additional technical measures that could mitigate risks for data subjects, including:

- Data minimisation measures, such as limiting continuous recording, live streaming, or retention periods. In particular, a user should not justify their continuous or indiscriminate recording of other individuals solely by a general or hypothetical concern for their personal safety.

[29] EDPB Guidelines 3/2019 on processing of personal data through video devices, Version 2.0, adopted on 29 January 2020; see also Article 29 Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things, 16 September 2014, p. 34, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf; and EDPB Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, adopted on 4 May 2020

[30] EDPB Guidelines 02/2021 on virtual voice assistants, Version 2.0, adopted 7 July 2021

[31] EDPB, Guidelines 3/2019 on processing of personal data through video devices, Version 2.0, adopted on 29 January 2020; EDPB, Guidelines 8/2020 on the targeting of social media users, Version 2.0, adopted on 2 September 2020; Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, adopted on 3 October 2017, as last revised and adopted on 6 February 2018

[32] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, adopted on 20 October 2020

[33] Case C-184/20, *OT v Vyriausioji tarnybinės etikos komisija*, ECLI:EU:C:2022:601

[34] EDPB Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s), adopted on 7 October 2024; EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, adopted on 7 July 2021

[35] EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, adopted on 18 November 2021

[36] EDPB Guidelines 2/2023 on the technical scope of Art. 5(3) of ePrivacy Directive, Version 2.0, adopted on 7 October 2024; and directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37

[37] WP29 Opinion 8/2014 on the on Recent Developments on the Internet of Things, adopted on 16 September 2014

- Other privacy-friendly settings and protective measures by default, in line with the principle of data protection by design and by default, including measures to blur/obscure or avoid processing the identity of bystanders, pseudonymisation, or anonymisation before sharing or re-use. Where possible, this processing should happen on-device. In addition, where smart glasses are designed primarily to provide real-time assistance, persistent storage of captured audio, images, or video may not be necessary and should therefore be disabled by default, unless required for the intended functionality or deliberately activated by the user, subject to appropriate safeguards.
- Technical restrictions, including where appropriate location-based limitations (geofencing) in contexts that are likely to be particularly sensitive in order to reduce unnecessary collection of personal data.
- Introduction of 'privacy frictions' that slow down sharing on social media platforms.

34 Finally, the use of smart glasses may raise concerns going beyond data protection law alone. Users of connected glasses should be mindful of any applicable Union, national or local laws. Depending on the circumstances, some uses might be prohibited under national criminal[38], civil, or labour law, as well as other sector-specific rules[39]. Failure to comply with such rules may also, depending on the circumstances, call into question the fairness of the processing of personal data under Article 5(1)(a) GDPR.

4 Conclusion

35 As smart glasses and related use cases continue to evolve, further guidance may be useful to address data protection issues comprehensively, and raise awareness among producers, users, data controllers and third parties.

36 The EDPB notes the importance of providing timely and concise guidance that is accessible, easy to understand, and practical for data protection matters in line with a risk-based approach. The EDPB will further analyse and work on the privacy concerns raised by smart glasses, including in connection with other video devices which raise similar legal questions.

For the European Data Protection Board

The Chair

(Anu Talus)

[38] For example, in some situations and jurisdictions the filming of facilities with protected status, indoors in a home, in a dressing room, or for harassment purposes may be an offence. In addition, sharing such captured data may be a separate or additional offense.

[39] The EDPB notes that some other countries are discussing legislative proposals applicable to wearable recording devices (see https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260SB1130).