Council of the European Union

Brussels, 27 November 2026
(OR. en)

16127/26

TELECOM 572
CYBER 492
JAI 1508
DATAPROTECT 387
COMPET 1455
MI 1283
CONSOM 346

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	AOB for the meeting of the Transport, Telecommunications and Energy Council of 1 December 2026: Smart glasses with integrated cameras and microphones: towards a coordinated European approach to privacy and transparency - Information from Belgium, Germany, France, the Netherlands and Spain

Smart glasses with integrated cameras, microphones and AI assistants are rapidly moving from niche devices to everyday consumer products. They offer valuable opportunities, for instance for persons with a visual impairment and for hands-free professional use. At the same time, they raise specific questions as regards privacy and transparency. The aim of this paper is not to call this technology into question, but to help ensure that these devices can develop in a way that Europeans can trust.

The central challenge for smart glasses lies in the fact that the persons who are recorded are not those who choose to use the device. Bystanders may find it difficult to tell whether a pair of glasses is recording, and have limited practical means to be informed, to object or to exercise their rights. A small indicator light, where there is one, may not always be a sufficient safeguard.

Belgium raised the issue at European level in May 2026 by asking the European Data Protection Board (EDPB) to reflect on smart glasses and similar devices that make it possible to record or identify persons without their knowledge.[1]

Several national authorities have also responded. In May 2026, the French data protection authority (CNIL) issued a call for vigilance and launched an action plan on smart glasses.[2] In September 2026, the Hamburg data protection authority concluded that a widely sold model can hardly be used lawfully in public spaces, citing the limited visibility of the recording indicator and indications of preparation for facial recognition.[3] Dutch authorities have also issued warnings and indicated that organisations may restrict use through house rules while awaiting EDPB guidance. Norway has announced a temporary and localised ban.

On 13 October 2026, the EDPB adopted a first statement on smart glasses.[4] It confirms, in particular, that the household exemption must be interpreted strictly, that manufacturers and providers cannot rely on the user to discharge their own obligations towards third parties, and that visible indicators should not be easy to circumvent. It also encourages sectoral standards and awareness-raising.

Meanwhile, market actors have also taken action: in early October 2026, a chain of opticians suspended the sale of a leading model in Belgium and the Netherlands.

However, these responses are taking place separately, on different legal bases and with different outcomes. Without coordination, there is a risk of divergent national approaches, legal uncertainty for citizens, manufacturers and sellers, and uneven protection within the internal market.

1 Press release of Minister Vanessa Matz, 27 May 2026.
2 CNIL, “Les lunettes connectées : la CNIL appelle à la vigilance” (Smart glasses: the CNIL calls for vigilance), 11 May 2026 (public alert and action plan; survey of 2,128 adults, 22–29 January 2026).
3 Hamburg Commissioner for Data Protection and Freedom of Information, report on a widely sold model of smart glasses, September 2026.
4 EDPB, Statement 1/2026 on smart glasses, adopted on 13 October 2026.

The existing European framework already provides important, if partial, safeguards. Whilst the GDPR does not apply to processing by a natural person in the course of a purely personal or household activity, it does apply to controllers or processors which provide the means for such processing. Furthermore, the AI Act prohibits certain biometric practices and requires deployers of emotion recognition or biometric categorisation systems to inform the natural persons exposed to them. Product safety, consumer protection and market surveillance rules are also relevant. These instruments were, however, not designed specifically for cameras integrated into everyday eyewear, and supervision is shared between different authorities across the Member States.

Smart glasses are also connected devices that capture and transmit audio-visual data, including data relating to third parties. Their cybersecurity is therefore directly relevant to the protection of bystanders and society in general: a compromised device or insufficiently secured associated services could expose such recordings to unauthorised access.

Way forward

We would welcome an exchange of views on a coordinated, proportionate and risk-based European approach to smart glasses, building on the work of the EDPB. Such an approach could address in particular:

- guidance on the application of the GDPR, the AI Act and product and consumer legislation to camera-equipped smart glasses, while preserving legitimate uses, in particular for accessibility;
- transparency by design, including recording indicators that are clearly visible and difficult to circumvent;
- cooperation between data protection, consumer protection and market surveillance authorities as regards wearable devices;
- attention to the cybersecurity of smart glasses and their associated services, in line with the Cyber Resilience Act;
- particular attention to biometric functionalities in consumer wearables, such as facial recognition, as well as the protection of minors and uses in sensitive environments.

Belgium, Germany, France, the Netherlands and Spain stand ready to contribute to this work.