CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Smart glasses

Compendium of G7 data protection and privacy authorities approaches

Table of Content

Introduction 2
Description of smart glasses technologies 3
Utilisation cases of smart glasses 3
Professional use-cases 3
Personal use-cases 4
Privacy concerns and questions 5
Privacy recommendations 7
Legal proceedings before the courts within the G7 9
G7 Data protection authorities' supervisory activities 9

Introduction

As part of its presidency of the G7 Data Protection and Privacy Authorities Roundtable in 2026, the Commission nationale de l'informatique et des libertés (CNIL, France) has made the issue of smart glasses one of its priorities.

Smart glasses have seen steady progression from highly publicised early prototypes in the 2010's to the sophisticated, integrated devices available today. Due to the decrease in costs, the market has shifted towards a broader audience. Manufacturers are currently focusing on discreet designs that are intentionally indistinguishable from ordinary glasses, embedding advanced sensors and artificial intelligence capabilities into daily-use objects.

That shift has prompted some institutions, regulators and even lawmakers to issue targeted regulations in specific environments to protect the integrity of proceedings and the privacy of individuals. Various establishments (for instance exam rooms[1], or court rooms[2]) have implemented their own internal rules to restrict the use of such eyewear within their premises. These institutional responses reflect a broader set of legal, security, and ethical considerations. The challenges smart glasses pose are also being reflected in the media. A growing number of reports claim that content regulation workers may view extremely sensitive and intimate content filmed by smart glasses[3].

Around the globe, data protection and privacy authorities (DPAs) have been considering the risks and appropriate responses associated with smart glasses in terms of privacy and data protection for several years[4]. This compendium provides a high-level overview of current developments in each G7 jurisdiction. Looking across jurisdictions can provide valuable insight into common concerns and

[1] https://japannews.yomiuri.co.jp/society/general-news/20240711-198135/; All website links were last accessed on 11/06/2026.
[2] https://www.nbcphiladelphia.com/news/local/philadelphia-courts-ban-all-smart-ai-eyeglasses-violators-could-face-arrest/4374128/; https://www.bbc.com/news/articles/cj6d4k65ky5o
[3] Including scenes of nudity, sexual acts, or individuals using the bathroom, likely without the user's explicit awareness that a human is reviewing the data: https://www.bbc.com/news/articles/c0q33nvj0qpo
[4] Certain quoted documents may depict a situation that has evolved in the last years. Yet, they provide valuable descriptions and perspectives.

approaches and has the potential to help develop future common positions to address this global challenge.

Description of smart glasses technologies

Smart glasses involve integrating digital technologies into a pair of glasses. The objective is to both facilitate the use of digital technologies by making them more ergonomic and to avoid the simultaneous use of connected devices, ranging from computers to mobile phones.

Several types of models can be identified:

- Basic models have a minimal level of functionality, such as making phone calls or listening to music. Most of them do not use AI technologies.
- Standard models integrate AI technologies in addition to the features of basic models, enabling the use of voice assistants and other smart features. They can also be equipped with cameras capable of capturing images and videos. These are the most common consumer models available today.
- Augmented reality models share the same aesthetic and technical features as standard models, but have also an integrated screen that displays information (notifications, messages, etc.) or videos, creating an immersive experience for the user.
- Mixed reality models offer the features of augmented reality as well as a three-dimensional specialization experience that increases the level of immersion through the interaction of virtual objects with the physical world.

Smart glasses use-cases

Professional use-cases

Professional use cases of smart glasses often involve augmented reality (AR) in order to optimise effectiveness, productivity, and safety[5].

In healthcare, smart glasses can provide clinical and surgical assistance, allowing doctors to access information in real time during procedures without using their hands. They can also support people with disabilities and be used in rehabilitation or therapeutic contexts[6]. For instance, smart glasses can support people with peripheral vision loss by augmenting their remaining vision and providing real-time hazard awareness[7]. They can also provide auditive help[8].

Moreover, smart glasses can live stream the surgical field from the operating surgeon's perspective to a remote expert surgeon, or to medical students[9].

In computer science, smart glasses help develop technologies related to human–computer interaction (HCI). HCI is being facilitated through natural language voice command, side-mounted touchpads or head motions for instance. Smart glasses go beyond simple photography by using sensor fusion, a computer science phenomenon where data from disparate sources (cameras,

[5] EDPS Tech Report on smart glasses
[6] Applications of Smart Glasses in Applied Sciences: A Systematic Review | MDPI
[7] A Hazard Detection and Tracking System for People with Peripheral Vision Loss using Smart Glasses and Augmented Reality
[8] https://www.cnil.fr/fr/lunettes-connectees-appel-a-la-vigilance
[9] Evaluation of Google Glass Technical Limitations on Their Integration in Medical Systems p.2

microphones, GPS, and inertial sensors) is combined to create a precise understanding of the environment[10] (object recognition, biometric recognition and analytics). One of the key features of smart glasses is the ability to visualise digital data without requiring the user to look away from the physical world through heads-up displays or augmented reality overlays.

In industries, smart glasses can assist workers during maintenance or complex technical tasks. For instance, instructions, warnings, or technical information can be broadcasted directly in the worker's field of vision. These devices are employed for order-picking processes, helping workers identify items and navigate storage areas more efficiently[11]. They are also used for training simulations in engineering tasks[12].

Lastly, in education, smart glasses can enhance immersive learning experiences. For example, they can be used in medical training to visualize anatomical structures in 3D, or to replace or supplement the physical presence of a tutor in the operating room. In sports training, they can be used to provide real-time performance feedback. In physics courses, they can illustrate complex concepts and processes through augmented reality[13].

Personal use-cases

Personal use cases of smart glasses include multimedia, convenience and lifestyle-tracking uses.

In the framework of multimedia and social media uses, smart glasses allow users to capture photos and videos of personal events for sharing privately or on social networks.

Users can access search engines or interact with voice-activated assistants for hands-free help with daily tasks.

Smart glasses can also track physical activities, sleep patterns and health indicators such as heart rate, breathing rhythms and calories burned[14]. Some models even use sensors to assess the wearer's stress levels or mood[15].

Other leisure use cases include AR gaming, where the device can tailor the experience based on user characteristics (like age or gender), or reading digitally enhanced books[16]. Modern models support features such as voice dictation (speech-to-text), motion tracking, and the ability to pilot drones[17].

---

[10] EDPS Tech Report on smart glasses
[11] EDPS Tech Report on smart glasses
[12] EDPS Tech Report on smart glasses
[13] Applications of Smart Glasses in Applied Sciences: A Systematic Review
[14] WP29 Opinion 8/2014 on the Recent developments on the Internet of Things, p. 5
[15] Berlin Group Working Paper on Privacy and wearable computing devices
[16] Berlin Group Working Paper on Privacy and wearable computing devices ; EDPS Tech Report on smart glasses
[17] EDPS Tech Report on smart glasses

Privacy concerns and questions

This section summarizes the positions and concerns expressed by data protection authorities and their cooperation networks regarding the processing activities carried out by smart glasses users and providers.

In 2014, the European Union's Article 29 Data Protection Working Party (WP29)[18] and the Information Commissioner's Office (ICO)noted[19] that smart glasses raise concerns around lawful grounds under certain frameworks, including "domestic purposes" or "household exemption", if the user use of the device is limited to purely personal or household activities[20]. However, this exemption will generally not apply if the user makes recordings publicly online or shares them in a public forum. In such cases, the user will usually be acting as a data controller for that processing and must identify a valid lawful basis for processing the personal data of others.

Additionally, because smart glasses connect to the internet, they are considered "terminal equipment" making them subject to the ePrivacy Directive (Article 5(3)) in the European Union, and to PECR rules in the UK which requires prior consent for storing or accessing information on a user's device[21].

These devices raise wider questions about the nature of privacy in private and public spaces[22], due to the nearly invisible nature of the recording process, which may take place without an individuals' knowledge. By enabling users, at relatively low cost, to capture video and images in almost any setting (private, public, workplace, school, etc.) without being detected, these devices raise important concerns around the ability for individuals to maintain privacy as they go about their daily lives. The CNIL states that anyone using smart glasses must respect the privacy of individuals whose image or voice may be captured by the glasses and, where necessary, obtain their consent[23].

The WP29 opinion on IoT, the Berlin group in its Working Paper on Privacy and wearable computing devices in 2015 and the European Data protection Supervisor (EDPS) in its dedicated Tech Report on Smart Glasses in 2019 have identified transparency concerns, as smart glasses lack the traditional cues associated with recording, such as holding up a smartphone. It makes it difficult for both users and bystanders to know when data is being captured[24]. While manufacturers use LED indicator lights to signal recording, some DPAs have questioned their efficacy, noting a lack of comprehensive field-testing to prove that these lights provide sufficient notice to the public. For miniaturised devices, the Berlin Group has suggested that transparency should be provided by non-visual means, such as broadcasting a signal[25].

Companies may wish to use recordings captured by smart glasses to improve AI models. They need to take into consideration that this wasn't the primary purpose for the data collection and ensure that they have the right legal grounds to process them for a different purpose, as pointed out by WP29[26]. The ICO recalls that they also need to inform users that their recordings will be used in this

---

[18] WP29 Opinion 8/2014 on the Recent developments on the Internet of Things, p.13
[19] Guidance for consumer Internet of Things products and services, ICO
[20] Guidance for consumer Internet of Things products and services, ICO; WP29 Opinion 8/2014 on the Recent developments on the Internet of Things
[21] Guidance for consumer Internet of Things products and services, ICO.

[23] https://www.cnil.fr/fr/lunettes-connectees-appel-a-la-vigilance
[24] Berlin Group Working Paper on Privacy and wearable computing devices, p.6;
[25] Berlin Group Working Paper on Privacy and wearable computing devices; p.3
[26] WP29 Opinion 8/2014 on the Recent developments on the Internet of Things

way[27]. The question is also relevant from the perspective of individuals appearing in the recordings. In this regard, the WP29 highlights the issue of information asymmetry[28].

The WP29, the Berlin Group and the EDPS express their concerns regarding consent: The use of smart glasses raises concerns around the ability for users and companies capturing and processing smart glasses data to obtain valid consent from individuals whose personal information is being captured by the device. Moreover, in several jurisdictions, explicit consent is strictly required for the processing of sensitive data, such as biometric or health information[29]; which smart glasses might be used to capture depending on the feature they include (such as facial recognition) or on the context in which they are being used (such as medical contexts). In scenarios involving connected devices, the overall quality of one's consent may be questioned as it is bundled with general terms or offered as a mandatory precondition for using the device[30]. Furthermore, in some situations, it can be practically impossible to obtain the consent of non-users (bystanders) captured in the background of recordings.

In many jurisdictions, individuals have rights to access, rectify, and erase their data. WP29 notes that the discreet nature of smart glasses can pose a challenge to these rights. On the one hand, individuals other than the wearer of the glasses may be unaware their data was collected[31] and therefore not seek to exercise those rights. On the other hand, while individuals wearing and using smart glasses themselves can often see data captured by the glasses after it has been interpreted and displayed by an app, they are rarely granted access to the raw sensor data, and this limits their ability to verify accuracy or switch to competing services (data portability)[32].

The WP29 and the EDPS both note that smart glasses utilise a high volume of sensors (cameras, microphones, GPS, accelerometers, and gyroscopes) to capture a constant stream of "raw" data[33] [34]. The WP29 for instance highlights the critical importance of minimization, requiring data controllers to limit collection to only what is required by the declared intent to ensure the protection of individuals' fundamental rights[35]. Raw data should in theory be deleted as soon as it has been processed into an extracted format[36]. Collecting and storing data "just in case" it might be useful later is prohibited in different jurisdictions[37] as pointed out by the ICO[38].

The WP29 and the EDPS point out the risks linked to inferences from Raw Data: "Raw" sensor data (from accelerometers or gyroscopes) can be used to infer a wider range of sensitive data about users, such as their mood, physical health status, or driving habits[39]. In some cases, the possibility of inferring this information, and the privacy risks involved, may not be clear to users.

---

[27] Guidance for consumer Internet of Things products and services, ICO
[28] WP29 Opinion 8/2014 on the Recent developments on the Internet of Things p.6
[29] WP29 Opinion 8/2014 on the Recent developments on the Internet of Things
[30] WP29 Opinion 8/2014 on the Recent developments on the Internet of Things
[31] Berlin Group Working Paper on Facial recognition Technology p. 21
[32] WP29 Opinion 8/2014 on the Recent developments on the Internet of Things
[33] WP29 Opinion 8/2014 on the Recent developments on the Internet of Things
[34] Guidance for consumer Internet of Things products and services, ICO; WP29 Opinion 8/2014 on the Recent developments on the Internet of Things
[35] WP29 Opinion 8/2014 on the Recent developments on the Internet of Things p.16
[36] WP29 Opinion 8/2014 on the Recent developments on the Internet of Things
[37] WP29 Opinion 8/2014 on the Recent developments on the Internet of Things
[38] Guidance for consumer Internet of Things products and services, ICO
[39] EDPS Tech Report on smart glasses WP29 Opinion 8/2014 on the Recent developments on the Internet of Things

The EDPS[40] and the Berlin Group[41] point out that smart glasses, like smartphones and other connected and wearable devices, are exposed to malware, data theft, spying and attacks that can disrupt or take control of the device. Limited processing power and battery life can restrict the use of strong security measures like encryption. In addition, their portability increases the risk of loss or theft, while lifecycle management and software updates are often harder to maintain securely.

Privacy recommendations

Different authorities have highlighted specific strategies or requirements based on their legal frameworks and technical assessments:

Personal information Protection Commission (PPC): The Japanese authority has published recommendations regarding notification of purpose of use, security managing measures and related matters when using camera system with a face identification function as well as on points to be noted when displaying customized advertisements based on facial images of individuals captured by cameras installed in electronic bulletin board, etc. The PPC considers that camera images can fall within the scope of the Act on the Protection of Personal Information, if they can identify a specific individual[42]. When camera systems extract facial features for identification, they require greater attention than ordinary video surveillance: the purpose of use must be specified so that an identifiable person can predict and assume that advertisements will be distributed based on attribute information extracted from the face image, and the face image must be used within the scope of that purpose of use along with notifying or publicizing the purpose of use[43]. If an advertising display with a built-in camera captures a face image that can identify a person, extracts attributes such as age or gender, and then shows personalized advertising, the key question is whether this processing complies with purpose limitation and information obligations. Even if captured images are deleted immediately, distributing ads based on attributes extracted from face images requires that the stated purpose clearly covers the distribution of advertisements based on those extracted attributes, and that the face image must be used only within that stated purpose, together with notification or public disclosure of the purpose[44] Retention of camera images and facial data should be limited to what is necessary for the stated purpose. The PPC does not prescribe a fixed retention period. Instead, the retention period should match the intended purpose. Businesses handling personal information must endeavour to delete or anonymize data without delay once that purpose has been achieved.

Information Commissioner's Office (ICO): The UK Authority has published Guidance for consumer Internet of Things products and services[45]. The guidance outlines expectations for data protection to manufacturers and developers of IoT products, including requests for consent and providing transparency on products with different interfaces as well as how to ensure that multiple users of products can exercise their rights. Moreover, in 2022, the ICO published its Tech Horizons Report which featured a chapter on Immersive Technologies. In this chapter, the ICO stresses the need for privacy by design, especially given the sensitivity of data collected (e.g. biometric signals like eye tracking or facial movements).

---

[40] EDPS Tech Report on smart glasses p.8
[41] Berlin Group Working Paper on Privacy and wearable computing devices p.7
[42] Q&A on the "Guidelines on the Act on the Protection of Personal Information", Q1 – 12, available on PPC website (in Japanese)
[43] Ibid. Q 1 -14
[44] PPC guidance; Guidebook for the Utilization of Camera Images ; Q1-16
[45] Guidance for consumer Internet of Things products and services, ICO

Office of the Privacy Commissioner of Canada (OPC): The OPC released guidance for manufacturers of Internet of Things devices in 2020. The guidance provides practical information for manufacturers to help ensure that their devices and business practices are privacy protective and compliant with legal requirements. The OPC also issued guidance for individuals on smart devices and privacy, which includes practical advice for users, such as limiting registration information to the minimum required, disabling Wi-Fi, Bluetooth, and other functions when not needed and favouring devices with physical mute buttons or "slide covers" for cameras to ensure that recording is physically disabled[46].

European Data Protection Supervisor (EDPS): In its Tech Report, the EDPS recommends that manufacturers and data controllers integrate privacy by design and default by applying strict data minimisation[47]. Given the discreet nature of smart glasses, they should develop innovative transparency tools to inform both users and bystanders, while providing specific controls for reviewing data before it is shared on social networks and ensuring long-term security through regular updates[48]. For policymakers, the report stresses that highly intrusive uses by law enforcement, such as facial recognition in public spaces, must be governed by specific parliamentary legislation that passes rigorous necessity and proportionality tests[49].

Commission nationale de l'informatique et des libertés (CNIL): The CNIL has issued a first set of recommendations for users[50] to ensure a respectful and privacy-conscious use of smart glasses. CNIL recommends them to prioritize transparency and contextual awareness by informing those in their immediate vicinity when the device is active and avoiding use in sensitive locations where recording is unexpected. They should deactivate recording functions as soon as they are no longer necessary and comply with local restrictions by switching off the glasses in certain areas where mobile phones are prohibited. Finally, users must obtain explicit consent from bystanders before using such images (publishing their images on social media for instance) and carefully consider the potential long-term consequences of sharing any captured content. Other useful publications by the CNIL linked to smart glasses include recommendations on securing connected devices[51], on the development of AI systems[52] and LINC's IP Report," The Body: The New Connected Device"[53].

Article 29 Working Party (WP29): The WP29 emphasized, in relation of Internet of Things products, the use of innovative transparency tools like "Privacy Proxies" (to manage consent preferences when interacting with sensors) and "Sticky Policies" (where privacy rules are attached to the data itself)[54]. They also recommend using random identifiers (MAC addresses) to prevent the tracking of users' locations[55].

The "Berlin Group": The International Working Group on Data Protection in Technology recommends that the use of smart glasses in the workplace must be voluntary; employees should not be adversely affected if they choose not to participate in programs involving these devices.

---

[46] *"Take advantage of mute buttons or software toggles that serve as "do not collect" switches."*
[47] EDPS Tech Report on smart glasses p 8.
[48] EDPS Tech Report on smart glasses p 8.
[49] EDPS Tech Report on smart glasses p 14.
[50] https://cnil.fr/fr/lunettes-connectees-appel-a-la-vigilance
[51] https://www.cnil.fr/fr/objets-connectes-noubliez-pas-de-les-securiser
[52] https://www.cnil.fr/fr/developpement-des-systemes-dia-les-recommandations-specifiques
[53] https://linc.cnil.fr/cahier-ip2-le-corps-nouvel-objet-connecte
[54] *"Interestingly, some recent developments in this field are trying to empower data subjects by giving them more control over consent management features, for example through the use of sticky-policies or privacy proxies."*
[55] *"To prevent location tracking, device manufacturers should limit device fingerprinting by disabling wireless interfaces when they are not used or should use random identifiers (such as random MAC addresses to scan wifi networks) to prevent a persistent identifier from being used for location tracking."*

They also advocate for the right of individuals to challenge the accuracy of data generated by these devices.[56]

Legal proceedings before the courts within the G7

In California, United States, a class action lawsuit has recently been filed against Meta[57], over the claim that Meta violated federal and state laws by failing to disclose that its AI smart glasses transmit videos to third-party contractors for human review. This lawsuit follows the revelation that subcontracted workers may view extremely sensitive and intimate content filmed by smart glasses, including scenes of nudity, sexual acts, or individuals using the bathroom, often without the user's explicit awareness that a human is reviewing the data.

In Japan, several cases are of potential interest in terms of the issues raised by smart glasses. Case-law tends to dismiss complaints against fixed surveillance cameras, if they are not installed for the purpose of tracking and photographing a specific individual. Unlike fixed cameras, smart glasses, when combined with AI, facial recognition, and location data, allow for the mobile tracking of an individual, which is a key factor in determining a privacy violation.

A 2017 Supreme Court ruling regarding GPS trackers[58] emphasizes that such data collection becomes problematic when it is conducted without a warrant, since such a method of investigation inevitably involves the continuous, comprehensive monitoring of the person's activities, and may invade personal privacy.

Therefore, if the use of smart glasses enables this level of behavioural surveillance, it may warrant civil penalties such as the payment of damages or an injunction to cease the activity (removal of the device or cessation of recording). Analysis via artificial intelligence and coordination with geolocation data transform a simple visual recording into a sophisticated surveillance tool, which may increase the likelihood of a civil tort claim.

G7 Data protection authorities' supervisory activities

In the UK, the ICO has accepted an innovative augmented reality (AR) app designed for smart glasses into its Regulatory Sandbox in in September 2024[59]. Regulatory Sandbox is a free service developed by the ICO, to support organisations who are creating products and services which utilise personal data in innovative and safe ways.

The app overlays the real world with computer-generated information, creating an enhanced version of reality. It is designed to provide reminders to users about tasks and objects around the house, and to recall information to aid memory retention. The app uses a hybrid of edge computing to process data and local and cloud processing for more intense data processing such as scene segmentation to distinguish backgrounds, objects, or people for computer labelling.

---

[56] "*The use of wearable devices in the employment sector raises additional issues with regard to employee's free choice. Employees who opt not to participate in any programs based on wearable devices should not be adversely affected by their decision.*"

[57] https://dockets.justia.com/docket/california/candce/3:2026cv01897/465369

[58] https://www.courts.go.jp/english/Judgments/search/1518/index.html

[59] https://ico.org.uk/for-organisations/advice-and-services/regulatory-sandbox/current-projects/#Animorph

The CNIL has announced its intention to bring the topic of smart glasses at the national, European and international levels[60].

The EDPB has commissioned a report on the social acceptability of smart glasses[61].

[60] https://www.cnil.fr/fr/lunettes-connectees-appel-a-la-vigilance
[61] https://www.politico.eu/article/new-privacy-frontier-europe-eyes-crackdown-smart-glasses/