

Data Protection Advisory: Smart Glasses

Smart glasses, such as Meta's Ray-Ban and Oakley ranges, let the wearer take photographs, record video and capture audio from their own point of view, and some can pass what they capture to an AI assistant. Used well, they offer real benefits, especially for people with disabilities.

But smart glasses also make it easy to record other people without their knowledge or consent. This sits uneasily with our right to a private life and, by extension, with the data protection principles of fairness and transparency.

The risk is not just theoretical: there is documented evidence of smart glasses being used to record people covertly in everyday places, from the street to the gym, and to share that footage online, where it can expose them to further harassment. While media investigations and civil society research highlight that this covert recording disproportionately impacts women and girls, data protection law protects all individuals: people should not be recorded, identified, shared or profiled in ways that are unfair, opaque or harmful.

Recordings may not stay only on the device, either. Meta has confirmed that when AI features are used (such as voice queries about visual surroundings) captured media can be transmitted to its cloud servers reviewed by staff or contractors and used to improve its systems. Meta says it applies automated filters, such as face blurring and the removal of identifying information, before human review.

However, reporting involving third-party contractors suggests that these safeguards may not always work as intended, particularly in poor lighting or more complex recording conditions. Where that happens, reviewers may still see private or unintended footage. Photos and videos captured in the standard way and saved locally in the companion app remain on the user's device unless the user chooses to share them. Together, these features raise real risks to people's privacy and data protection rights.

Each of the three Crown Dependencies has its own data protection legislation: the Data Protection Act 2018 in the Isle of Man, the Data Protection (Bailiwick of Guernsey) Law 2017, and the Data Protection Authority (Jersey) Law 2018.

These laws are technology neutral. Data protection law applies regardless of whether personal data is collected using a computer, mobile device, telephone, camera, CCTV, body-worn camera or smart glasses. Where data protection law applies, those processing personal data must comply with their data protection obligations.

The Isle of Man Information Commissioner's Office, the Bailiwick of Guernsey Office of the Data Protection Authority, and the Jersey Office of the Information Commissioner have joined forces to raise awareness of the data protection and privacy considerations arising from the use of smart glasses.

This Joint Data Protection Advisory provides advice to our residents and expectations to organisations on what the law says and the steps they can take to protect themselves and others, and to use these devices responsibly.

For members of the public

What the law says

While the fact that a person is in a public place does not, by itself, mean that their personal data can be recorded and used without restriction, data protection law does not generally stop an individual from taking a photograph or a video for their own personal use.

This kind of personal activity typically falls outside data protection law altogether, under what is known as the personal or household exemption. In everyday terms, recording something in public purely for yourself does not require you to consider the data protection law. Although we urge you to respect people's right to privacy at all times.

That position of falling outside of the data protection law may change if the recording is shared more widely. Posting a photo, video or audio clip of an identifiable person on social media, in a group chat or on a public platform may no longer be a purely personal activity. In those circumstances, data protection law may apply. For example, if you are purporting to act on behalf of an organised group or entity, that group or entity will become responsible for how that personal data is used.

Other laws may also be relevant, even where data protection law does not apply. Recording someone in a place where they would reasonably expect privacy, such as a changing room, a bathroom or inside their home, can raise concerns under criminal laws. Creating or sharing intimate images of a person without their consent, and creating or sharing indecent images of a child, can be criminal offences, regardless of the technology involved. Persistently recording or targeting a particular person can also amount to harassment.

What you can do

Learn to recognise when a device is recording. Meta states that its glasses show a white LED light when the camera is active, and that the camera will switch off if the light is covered or tampered with. The light may be hard to see in bright daylight, and not everyone knows what it means, so it is worth knowing to look for it. If you see the light, or someone tells their glasses to take a photo or video, a recording may be taking place.

Take extra care with children and in private spaces. Children's personal data needs extra protection. If you believe a child or vulnerable person is being recorded or targeted by someone using smart glasses, and it is safe to do so, remove them from the situation, note relevant details where appropriate, and contact the relevant safeguarding authority.

Know your rights and how to raise a concern. Data protection law gives people rights over their personal information, including the right to be informed about how it is used, to access it, and in some cases to have it deleted. Children have these rights too, and parents or guardians may be able to exercise them on a child's behalf. If your or your child's personal data is misused, or harmful content is created or shared, you can report it to the platform or service involved and ask for it to be removed, and you may also be able to raise a concern with your local data protection authority. If you have concerns regarding potential criminal activity, you should also report it to the police.

Recording for yourself is usually fine but think carefully before you share. If you capture other people while filming, remember that sharing that footage more widely can bring you within data protection law and can affect the people in it. Before you post or forward something, consider whether the people in it know they were recorded, whether they would reasonably expect it to be shared, and whether sharing it could cause harm or embarrassment. A useful test is to ask how you

would feel if it were you in the recording. Where you can, tell people what you are recording, why, how it will be stored and who is likely to see it, and check that they are content with what you plan to do.

Respect privacy in public places. Being in a public place does not automatically remove a person's privacy or data protection rights. Where data protection legislation applies, individuals may have rights in relation to recordings of them, including the right of access. Even where there is no legal requirement to do so, respecting people's privacy is the responsible approach.

Expectations for organisations

What the law says

Where an employee uses smart glasses in a work context, the organisation may be acting as a controller for the personal data that is recorded and is responsible for making sure the law is followed. Many of the requirements that apply to CCTV and body worn video apply here too.

What you can do

Decide whether smart glasses have any place in your organisation.

Think carefully about whether smart glasses are genuinely needed.

As well as your obligations under data protection law, you owe a duty of care to your staff and customers, and restricting or banning these devices may be a sensible risk mitigation measure.

Therefore, if the glasses are not necessary for your operations, put a clear policy in place restricting their use for work, explain to employees why, and make a notice available to customers where relevant. Include this in your policies and procedures, for instance your Acceptable IT Use policy.

If you have a clear business use for smart glasses, make sure you are meeting your data protection obligations as outlined below.

Understand where the data goes.

The particular risk with these devices is what happens to a recording after it is captured. When a recording is uploaded to the manufacturer's cloud service, or when a wearer asks the manufacturer's AI to analyse what the glasses have captured, the personal data in that recording may be disclosed or transferred to the manufacturer. They may store it, may allow their own staff or contractors, including reviewers in other countries, to access it, and may use it to train their AI systems.

For an organisation, that means personal data leaving your control and being handed to a company outside the Island, without the contract or the safeguards that data protection law requires when you share personal data with a third party or send it overseas. In practice, using consumer smart glasses to capture work information could amount to an unlawful transfer of personal data to the manufacturer. As the controller, you remain responsible for that personal data and for the fulfilment of individuals' rights in relation to it, even where it is handled by a third-party provider.

The risk is greater still where recordings capture sensitive material, for example client or customer details, health information, financial records, confidential business information, or special category data, which the law protects more strictly and which your organisation may also be under a separate duty to keep confidential. Once such data has been sent to the manufacturer, and potentially seen by reviewers located around the world, you can no longer guarantee where it is or who has seen it.

Therefore, before any smart glasses are introduced, establish whether the device transmits recordings to the manufacturer's cloud systems or to third parties, whether the manufacturer may itself be acting as a separate controller or processor, whether data is transferred outside the Crown Dependencies, and whether appropriate safeguards are in place for any such transfer. Be sure to establish appropriate controller/processor contracts and address the international transfer requirements.

Carry out a Data Protection Impact Assessment first.

A Data Protection Impact Assessment (DPIA) will be required before processing begins wherever the proposed use is deemed to be high risk. This is likely to include, for example, systematic or continuous monitoring of employees or the public; large-scale or routine recording; use of facial recognition or other biometric identification; processing involving children or other vulnerable individuals; or combining recordings with other datasets to build profiles of individuals.

In practice, if you are using smart glasses in the workplace, you will need to complete a DPIA before processing begins, as you would for CCTV or any other surveillance device.

Be transparent and identify a lawful basis before recording people.

Where recording is permitted, use signage to inform the public that it may take place, and give clear disclosure, verbal or written, to the public and to other staff before any recording begins.

Organisations must also identify and document an appropriate lawful basis before processing personal data. Depending on the circumstances and jurisdiction, this may include consent, contractual necessity, legal obligations, vital interests, public tasks or legitimate interests.

Where consent is relied upon, it must be freely given, specific, informed and unambiguous, and capable of being withdrawn where applicable. The person must understand the purpose of the recording, where it will be stored, who can access it and how long it will be kept. If an individual does not agree or withdraws consent, recording must not take place for that person. Organisations cannot switch to an alternative lawful basis once consent has been requested and refused. Lawful bases should be determined prior to capturing anything.

Support individuals exercising their rights.

Under the law, individuals have rights to the information held and processed about them.

Organisations should have procedures for dealing with objections to recording and requests to exercise data protection rights, including Subject Access Requests (SARs).

Train your staff.

Make training readily available and keep employees up to date with local data protection requirements. All staff who handle personal data should understand how to handle, store and dispose of it safely, and should know your organisation's rules on smart glasses. Guidance for employers is available on each authority's website.

Handling special category data.

Smart glasses may capture or generate special category data, which the law protects more strictly. This includes health information, information about racial or ethnic origin, religious or philosophical beliefs, political opinions, sexual orientation and biometric data used for identification.

This information may be captured incidentally. For example, a recording could reveal a person's health condition or religious beliefs, while facial recognition may involve biometric data.

Special category data is subject to greater protection, and there are stricter requirements before it can be processed. Those requirements, and how they must be met, differ between the three Crown Dependencies. Organisations should check the position under the law that applies to them and identify and document the relevant basis or condition before processing.

Smart glasses are becoming more common, and the technology behind them is advancing quickly. Used responsibly, they hold real promise. But the ease with which they can record people, and the fact that those recordings may leave the wearer's control, mean we all have a part to play, members of the public, businesses and wearers alike, in using them lawfully and with respect for other people's privacy.

Quotes

"Smart glasses can be a real help and for people with disabilities especially, they open up the world in ways older technology never could. But the same features that make them useful also make them easy to misuse. We know from experience that women and girls are disproportionately the ones filmed without consent, whether by a stranger on the street or someone at a party. It takes only a glance to record someone, and that footage can end up anywhere including with a company beyond our shores. Our message is simple: think before you share, and ask yourself how you'd feel, or how a woman in your life would feel, if it were her in that footage."

Dr Alexandra Delaney-Bhattacharya, Isle of Man Information Commissioner

With any technology, there are benefits and risks. In the case of smart glasses such as those described, there are clear advantages in their use. However, there are also considerable privacy risks of which the general public and users of these glasses need to be fully aware. As with any recording device, whether that be CCTV, dashcam, helmet cam, video doorbell, or even a mobile phone, the user is expected to act responsibly and consider the privacy impacts of its use on other people. Equally, those affected must also feel able to exercise their statutory rights under data protection laws and feel empowered to challenge users who have not been transparent about the use of the technology.

Paul Vane, Information Commissioner for Jersey

"Public spaces do not erase privacy rights. While smart glasses can empower individuals to navigate their lives, especially those with disabilities, they can and must be used in a manner that respects the dignity and rights of others."

Brent Homan, Data Protection Commissioner, Bailiwick of Guernsey