Upholding information rights

Queen Elizabeth House, Sibbald Walk,
Edinburgh, EH8 8FT
T. 0303 123 1115 E. scotland@ico.org.uk

Consultation on the Use of Body Worn Video
Strategy, Insight & Innovation: Research & Insight
Police Scotland

By email only

31 August 2021

Dear Sir / Madam

The Information Commissioner's Office response to Police Scotland's public consultation on the Use of Body Worn Video

We are pleased to respond to Police Scotland's public consultation on the national roll out of Body Worn Video (BWV) to all operational police officers, staff and special constables in Scotland. Whilst the ICO recognises the operational value in the use of BWV, both for the public and police, it is critical that the data protection implications from using the technology are acknowledged and that the governance of the information collected is paramount whilst being at the forefront of any roll out.

As well as monitoring and enforcing the UK General Data Protection Regulation ('UK GDPR') and Data Protection Act 2018 ('DPA 2018'), the Information Commissioner's functions include promoting public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data.

This correspondence and any response received do not prejudice the potential future use of the Commissioner's regulatory powers should any infringements of data protection law come to light.

Many of the consultation questions fall outside of the scope of the Information Commissioner's regulatory role as they are directed towards members of the public and ask for their view on the use of BWV and confidence in the police. For this reason, key data protection points are addressed below rather than using the survey.

Information Commissioner's Office (Head Office)
Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113

It is not clear from the consultation the circumstances in which BWV would be used but, presumably, due to the statement that *'all operation police offices, staff and special constables'* would be provided with BWV, where funding allows, we assume that it could, potentially, be used wherever an operational police officer, staff member or special constable is present. This does not necessarily mean that BVW is always on, but rather there is the potential for BWV to be used at any time.

We have, in tangent with this consultation, read the published information at Body Worn Video - Police Scotland.

It will be key to involve Police Scotland's Data Protection Officer (DPO) as plans to use BWV develop. The DPO will be best placed to provide expert advice on compliance with data protection law in the context of Police Scotland's functions and powers and in respect of the personal data that Police Scotland will be processing.

As you may already be aware the ICO is a member of the Independent Advisory Group on Emerging Technologies in Policing. Further information can be found here. Outputs and learning from this group will be of relevance.

Does the processing fall under Part 3 of the DPA 2018 or Part 2 / UK GDPR?

Police Scotland should consider whether the proposed processing falls under Part 2 (general processing) or Part 3 of the Data Protection Act 2018 (DPA 2018) (processing by a competent authority for a law enforcement purpose).

We note the reasons, or purposes, for the use of BWV are listed on the consultation page and are as follows:

- *improve the quality of interactions with the public;*
- *reduce and resolve complaints;*
- *increase officer safety;*
- *reduce delays to justice; and*
- *lead to greater public transparency.*

Part 3 only applies to competent authorities processing for law enforcement purposes. Any processing carried out by a competent authority which is not for

the primary purpose of law enforcement is covered by the general processing regime under Part 2 of the DPA 2018 (read with the UK GDPR).

As you will be aware the law enforcement purposes are defined under section 31 of the DPA 2018 as:

> *'The prevention, investigation detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'*

Therefore Police Scotland will need to make the determination as to whether some or all of the proposed processing falls under Part 3 of the DPA 2018 or Part 2 / UK GDPR. Our response includes references to both regimes; 'law enforcement processing' will be used when referencing processing under Part 3 DPA 2018 and 'general processing' to refer to processing under Part 2 DPA 2018 / UK GDPR.

Data protection by design and default

Data protection by design and default is about considering data protection and privacy issues upfront and in a consistent manner, prior to any deployment.

Data protection by design and default features in both regimes (for law enforcement processing s57 of the DPA 2018 and general processing Articles 25(1) and 25(2) of the UK GDPR). Police Scotland therefore, has a general obligation to implement appropriate technical and organisational measures to show that it has considered and integrated all of the principles of data protection into the processing activities. This requirement will be particularly important for the roll out of BWV because of the privacy risks posed by the contexts in which it may be used and the sensitive nature of the information that will be collected. This means that this type of surveillance has the potential to be much more intrusive then traditional, fixed CCTV.

Further, prior to purchasing any surveillance system, Police Scotland should make decisions based on the technology's ability to provide a compliant solution to a problem (or problems), and not purchase a system because it is new, available, affordable or purely in the belief that it will gain public approval.

The DPIA process is a core component for Police Scotland in meeting the obligations around Data Protection by Design and Default which we will now go on to discuss.

Data Protection Impact Assessments (DPIA)

There is a specific legal obligation on controllers to undertake a DPIA where any proposed processing is likely to result in a high risk to the rights and freedoms of individuals (for law enforcement processing - s64 DPA2018 and for general processing Article 35 UK GDPR). Where such a risk cannot be mitigated, the data controller must consult with the ICO prior to the processing commencing (s65 DPA2018 or Article 36 UK GPDR). Our understanding is that Police Scotland have begun preparing a DPIA for the roll out of BWV and given the privacy risks posed by BWV we are pleased that this is the case. The DPIA should be continually updated as the project evolves.

Although intended for organisations in England and Wales, the guidance prepared by the Surveillance Camera Commissioner along with the ICO for carrying out a data protection impact assessment on surveillance camera systems and its associated template may be a particularly useful resource. These documents explain the legal obligations with regards to DPIAs in the context of introducing surveillance systems and act as a guide through the process to help identify whether the use of BWV is appropriate for the problem(s) that need to be addressed.

The DPIA should clearly set out the pressing need that Police Scotland are aiming to address with BWV. It is our understanding that Police Scotland may be seeking to address multiple needs with the use of BWV. If that is the case each purpose should be considered separately in the DPIA as it is possible that BWV may be necessary and proportionate in certain circumstances and for one purpose but not another. The DPIA should specifically set out how function creep will be managed.

It should also explore what other options may be available to achieve the same purpose and why it has been determined that BWV is necessary and proportionate in the circumstances.

The use of audio is particularly intrusive. If there is an intention to use audio recording as well as visual recording Police Scotland will need to be able to justify why this is necessary and proportionate and, whether this rationale is applicable to all circumstances or limited to specific contexts.

A DPIA helps to systematically assess the risks attached to the project and also acts as a record of any decision making.

For the purposes of using surveillance systems, if Police Scotland fail to take a 'data protection by design and default' approach and do not conduct a DPIA that fully explores necessity and proportionality and the potential risks, then it may be that data protection problems arise further down the line that could be avoided at an early stage.

Consultation is a core component of any DPIA process and the responses to this consultation will be useful in fully considering and addressing the risks associated with BWV in the DPIA.

Governance

A strong and comprehensive governance regime must be established for the use of information recorded by BWV, and for any subsequent processing of information post deployment. This should include, but not be limited to: ongoing reviews of effectiveness, necessity and proportionality of use, the retention periods for recorded footage, how the information is securely stored with appropriate access controls in place, and strict rules around the onward disclosure of footage to third parties. Some disclosures to third parties may be unlawful and qualify as an offence under data protection law if the disclosure was made knowingly or recklessly without the consent of Police Scotland.

If it is intended for recorded information to be shared with third parties, Police Scotland must ensure that any disclosure of information from the surveillance system is controlled and that the disclosure itself is consistent with the purpose(s) for which the system was set up. Further, appropriate data sharing agreements should also be in place where necessary and be readily available if requested by a regulatory authority.

Individual's information rights

Individuals have information rights afforded to them under data protection law and should be considered in advance of the roll out, specifically how the rights will be promoted and facilitated, particularly the right of access and the right to be informed (see further detail below).

Right of access

Subject to exemption, the right of access (for law enforcement processing s45 DPA 2018 and for general processing Article 15 UK GDPR) is a fundamental right for individuals and helps them understand how and why their data is being used,

and to check it is done lawfully. The right of access gives individuals the right to obtain a copy of their personal data, as well as other supplementary information.

In practice, requests for CCTV or BWV footage can be a complex area and each request should be approached on a case by case basis. Police Scotland should however ensure that the design of any surveillance system allows the controller to easily locate and extract personal data in response to such requests.

Responding to the right of access may involve providing information that relates both to the requester and another individual. As a controller's obligations are to provide a copy of the information about the requester rather than a complete version of footage, a controller may have to consider removing or redacting footage of third parties. To facilitate this, controllers may need to build on existing governance and use specialist software to redact visual and audio data, such as that used for video forensics or media productions. Police Scotland should ensure that relevant members of staff are appropriately trained to use such software, e.g. to process footage for other purposes or to respond to requests efficiently within the statutory timescales. Police Scotland should consider the risks associated with the further use of footage, whether BWV or CCTV, by individuals once they have been provided with a copy, especially with the prevalence and increasing use of social media, and we would recommend that that these risks are assessed and addressed in the DPIA.

Right to be informed

Individuals have the right to be informed about the collection and use of their personal data and the need for transparency is a fundamental aspect of data protection law. Controllers must inform individuals when they are capturing personal data, especially via overt surveillance unless exemptions apply. Police Scotland should ensure that this right is considered and facilitated for instance by using clear signage, or verbal announcements or lights/indicators on the device itself and have readily available privacy policies that individuals are able to access. Police Scotland may wish to have a number of privacy policies that are tailored to various audiences, including vulnerable adults and children. Controllers may also wish to incorporate infographics or videos to explain the use of such technologies. We note in Police's Scotland published information on BWV it states:

> *It is routine to inform the public when we are using body worn video cameras. Where operationally viable, a camera is not turned on unless the member of public is made aware by the police officer. That will continue to be the policy wherever possible. It will not be used covertly or for surveillance.*

It is recognised that the use of surveillance systems often present challenges for providing individuals with privacy information, but controllers should seek innovative ways to do so. The circumstances in which BWV may be used and how privacy information will be provided to individuals in each circumstance should be set out in the DPIA and in operational guidance materials. Any risks that an individual's right to be informed may not be met in specific circumstances e.g. in emergency situations should be considered, assessed and addressed in the DPIA. We would recommend that this information and advice to the public is further developed as the project evolves and any guidance and training for staff and officers that utilise BWV is consistent across Scotland.

The ICO is currently working on revising our CCTV Code of Practice. This will primarily focus on the application of UK GDPR in a non-law enforcement capacity, however the guidance will remain applicable for law enforcement agencies as the good practice recommendations are transferrable across data protection regimes. We will let Police Scotland know once this is published. In the interim our existing CCTV Code of Practice is still a useful resource and which has a section on BWV.

Further, it is recommended that Police Scotland liaise with the wider policing community, such as leads within the National Police Chiefs' Council (NPCC) in order to learn from their experiences when deploying BWV, both from a practical perspective but also to gain insight on current governance issues.

I trust this response is helpful. However, if you would like clarification on any of the points above or advice on any new or emerging data protection issues as the roll out of BWV is further developed please do not hesitate to get in touch.