Upholding information rights

3rd Floor, 14 Cromac Place, Belfast, BT7 2JB
Tel. 0303 123 1114
www.ico.org.uk

Northern Ireland Ambulance Service Health & Social Care Trust
Body Worn Video Public Consultation
Equality & Public Involvement Office
Site 30
Knockbracken Healthcare Park
Saintfield Road
BELFAST
BT8 8SG

**By email only: consultation@nias.hscni.net**

14 February 2022

Dear Sir / Madam

**The Information Commissioner's Office response to the Northern Ireland Ambulance Service's public consultation on the principle of introducing Body Worn Video**

We are pleased to respond to the Northern Ireland Ambulance Service (NIAS)'s public consultation on the principle of introducing Body Worn Video (BWV) for the primary purposes of violence prevention and reduction against NIAS staff. Whilst the Information Commissioner's Office ('ICO') recognises the operational value in the use of BWV, 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.

Some 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 their views on the current levels of violence against NIAS staff and future levels of safety. For this reason, we have outlined the key data protection

points relating to BWV below rather than responding via the consultation questions.

**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.

Under Articles 25(1) and 25(2) of the UK GDPR, NIAS has an 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 context 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 than traditional, fixed CCTV.

Prior to purchasing any surveillance system, NIAS 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 Data Protection Impact Assessment (DPIA) process is a core component for NIAS in meeting the obligations around Data Protection by design and default which we will now go on to discuss.

**Data Protection Impact Assessment**

Article 35 of the UK GDPR sets out 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. Where the controller identifies a high risk to individuals that cannot be mitigated against, they must consult with the ICO prior to the processing commencing in accordance with Article 36 of the UK GDPR.

It is helpful that a draft DPIA has been completed by NIAS as part of the BWV proposals and that it was published along with the consultation document. From the draft DPIA, it appears that NIAS have not identified any high risks that cannot be mitigated against that would require formal consultation with our office.

We have not undertaken a detailed review of the DPIA, having instead focused on the consultation document with a view to providing feedback in advance of the consultation deadline. However, we have set out below some general initial feedback on the draft DPIA for your consideration as the DPIA develops:

- The DPIA should set out why it has been deemed necessary and proportionate that the introduction of BWV will address the needs facing NIAS. If there are multiple needs to be addressed, 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 explore what other options have been considered by NIAS that may achieve the same purpose, which is connected to the point above to ensure the DPIA fully sets out why BWV is necessary and proportionate in the circumstances.
- The DPIA should further explore the lawful bases that will apply to the processing. If legitimate interests is proposed to be relied upon, it would be useful to have an outline of the legitimate interests assessment that is required for reliance on this lawful basis, along with an explanation as to how NIAS, as a public authority, has deemed this lawful basis to apply. This is important given that public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority. In addition, if special category data is envisaged to be captured within the footage as the DPIA suggests, it should further set out the applicable condition for processing such data under Article 9 of the UK GDPR along with an explanation as to why that particular condition(s) will be relied upon.
- The DPIA should detail why the use of audio recording as well as visual recording is necessary and proportionate, and whether this rationale is applicable to all circumstances or limited to specific contexts.
- The DPIA should clearly set out the individual risks associated with the proposed introduction of BWV and what the likelihood and severity assessment of each of those individual risks is. In addition, the risks identified within a DPIA should fully set out the potential impact on individuals within the risk description.
- The DPIA should be amended to reflect all the responses from consultees, with consultation being a core component of any DPIA process and assisting NIAS to fully consider and address the risks associated with BWV in the DPIA.

We would encourage you to keep the DPIA under review as this consultation exercise develops and the proposals evolve. It will also be key to involve NIAS's Data Protection Officer (DPO) as the plans to use BWV develop and the DPIA requires amendment accordingly. The DPO will be best placed to provide expert advice on compliance with data protection law in the context of NIAS's functions and powers and in respect of the personal data that NIAS will be processing.

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 as you update your DPIA. 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.

If NIAS 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 of using a BWV surveillance system, then it may be that data protection problems arise further down the line that could have been avoided at an early stage.

**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 NIAS. If it is intended for recorded information to be shared with third parties (aside from sharing footage with PSNI as evidence of a potential crime having been committed) NIAS 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. You

may find it useful to refer to our Data sharing code of practice for further information on this area.

**Individual's information rights**

Individuals have rights afforded to them under data protection law. These should be considered in advance of the roll out of BWV, with specific focus on 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 under Article 15 of the 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. NIAS 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. NIAS 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. NIAS 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 these risks are assessed and addressed in the DPIA.

**Right to be informed**

Individuals also 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. NIAS should ensure that this right is considered and facilitated, for instance by using clear signage, or verbal announcements or lights/indicators on the device. NIAS should also have readily available privacy policies that individuals are able to access (for example, on your website) in the event that it is not operationally viable for fair processing information to be provided before recording is commenced. NIAS may wish to have a number of privacy policies that are tailored to various audiences, including vulnerable adults and children, and to incorporate infographics or videos to explain the use of such technologies.

It is recognised that the use of surveillance systems often presents 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 that guidance and training for NIAS staff who will be utilising BWV is provided and regularly refreshed.

The ICO is currently working on revising our CCTV Code of Practice and we will let you know once this is published. In the interim our existing CCTV Code of Practice is still a useful resource and includes a dedicated section on BWV.

Further, it is recommended that NIAS liaise with its counterparts and other public authorities who have implemented BWV 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 considered, please do not hesitate to contact us.

Yours sincerely,

Caroline Mooney
Regional Manager
ICO (Northern Ireland)

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice