Upholding information rights

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

Dr Brian Plastow
Scottish Biometrics Commissioner
Bridgeside House
99 McDonald Road
EDINBURGH
EH7 4NL

By email only:

23 December 2021

Dear Brian

The Information Commissioner's Office to the Scottish Biometrics Commissioner's Code of Practice on the acquisition, use and retention of biometric data for criminal justice and police purposes

About the ICO

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.

The Commissioner is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations and taking appropriate action where the law is broken

Introduction

As a statutory consultee, the Information Commissioner's Office (ICO) welcomes the opportunity to respond to the Scottish Biometrics Commissioner's Code of Practice on the acquisition, use and retention of biometric data for criminal justice and police purposes. It is essential that that organisations collecting such data are held to high standards and that the rights of individuals are respected and upheld. These include the standards and rights conferred by data protection law.

The ICO sits on the Scottish Biometrics Commissioner's Advisory Group (SBC) and it is expected that a memorandum of understanding between the ICO and the SBC will be agreed in due course.

Data Protection Law

At the end of the UK's transition period after exiting the EU, the GDPR was incorporated into UK data protection law as the 'UK GDPR' . All references in the Code to the 'GDPR' therefore should be updated to read as the 'UK GDPR'.

The Data Protection Act 2018 (DPA 2018) sets out the data protection framework in the UK, alongside the UK GDPR. It contains three separate data protection regimes:

- Part 2: sets out a general processing regime (the UK GDPR);
- Part 3: sets out a separate regime for law enforcement authorities; and
- Part 4: sets out a separate regime for the three intelligence services.

The Code explicitly states it will cover the processing of biometric data for criminal justice and policing purposes in Scotland. The relevant data protection law is therefore contained in Part 3 of the DPA 2018. There are a number of sections of the draft Code that require revision to reflect this:

- Paragraph 65 sets out the UK GDPR principles but it is the principles in Part 3, Chapter 2 of the DPA 2018 that apply to biometric data processed for law enforcement purposes. Although very similar to the UK GDPR principles, there are some key differences that reflect the nature of law enforcement processing.

- Paragraphs 31 and 67 refer to 'special category' data however under Part 3 of the DPA 2018 this data (which includes biometric data) is referred to as 'sensitive processing'.

- Paragraph 68 covers the lawful processing of special category data. Under Part 3 'sensitive processing' can only be undertaken in two cases; where the individual has given consent (but note that there will be very limited circumstances where competent authorities can obtain valid consent for the processing) or where the competent authority can demonstrate that the processing is **strictly necessary** and satisfy one of the conditions in

Schedule 8 of the DPA 2018. Strictly necessary means that the processing has to relate to a pressing social need that cannot reasonably be achieved through less intrusive means. This is a requirement which will not be met if the purpose can be achieved by some other reasonable means.
The Code should advise on the requirement for an 'appropriate policy document' to be in place, as described in either s35(4)(b) or s35(5)(c) as well as s42 DPA 2018). The document should contain:

☐ an explanation of how the processing complies with the relevant data protection principles; and
☐ an explanation of the controller's policies in relation to retention and erasure, including to give an indication of how long the data is likely to be retained.

Intersection with existing UK frameworks and codes

We note that this Code is to promote good practice, transparency and accountability which is welcomed. We view this Code as an aid to supporting organisations' compliance with the DPA 2018 and promoting best practice.

There is a risk given the volume of guidance and activity in this area that some confusion could arise. To minimise this, we recommend ensuring that it is clear how this Code sits alongside the developing framework in the rest of the UK for policing and criminal justice and that it harmonises with what is going on elsewhere in other UK jurisdictions. This includes data protection law, guidance and Codes from the England and Wales Biometric Commissioner and Surveillance Camera Commissioner, and guidance in relation to live facial recognition from the NPCC/College of Policing.

Clarity and harmony will be particularly important for UK wide bodies who may be caught by the Code when undertaking policing functions in Scotland but caught by Codes relating to England and Wales at other times (as identified in paragraph 23 of the draft Code). These organisations will need to be clear on their responsibilities and the relevant frameworks that govern them in different circumstances.

Scope of the Code

We welcome the clarity of the specific organisations that must comply with the Code, namely Police Scotland, the Scottish Police Authority and the Police Investigations and Review Commissioner.

As you will be aware, there are other Scottish competent authorities who may process biometric data for criminal justice and policing purposes but who are not currently in the scope of the Code. While there is no existing legal obligation on them to comply, it may nonetheless be useful for them to conform to aid compliance with other legislative obligations including those under data protection law.

The Code is silent on whether it would apply to bodies processing biometric data on behalf of public sector bodies or office-holders that are subject to the Code. We recommend that the Code states whether they would be covered. If it was extended to include processors, it would ensure that the entire end to end processing of biometric data for criminal justice and policing purposes would be covered and private sector organisations would be held to the same high standards as those named in the Code.

The Code should address that third party contractors are likely to play a role in the delivery of a biometric processing. It is therefore essential that any governance arrangements:

- build-in sufficient oversight of the processing being carried out by third parties, including Data Protection Impact Assessments (DPIAs) being in place; and
- ensure there is due diligence around transparency and effective purpose limitation safeguards are in place.

The definition of biometric data

Section 35(8) of the DPA 2018 defines biometric data as:

> *"'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".*

This is different to the definition of biometric data in the Scottish Biometrics Commissioner Act 2020.

Page 16 of the Code usefully draws a distinction between the definition of biometric data in the Code and the definition in the UK GDPR and DPA 2018, but it needs to be made clear operationally that the Code includes biological source samples and photographs in this definition as stated in paragraph 21 of the draft Code: *"In addition to computerised biometric data records arising from specific technical processing, the meaning of "biometric data" within the Scottish Biometrics Commissioner Act 2020, and consequentially this Code of Practice includes the source materials from which a corresponding biometric record can be derived. Examples of such materials include blood, saliva, hair etc."*

Under the DPA 2018 blood, saliva, and hair samples may fall under genetic data (biological samples) rather than biometric data by definition. Organisations need to be clear what categories of personal data they are processing for the purpose of data protection law.

Data Protection Impact Assessment

At various points, and in particular at paragraph 69, the Code references the need for organisations to complete a DPIA, it would be useful to expand on this and state when a DPIA should be undertaken, in particular for processing that is likely to result in a high risk to individuals. Paragraph 69 would benefit from further detail, explaining that DPIAs should be based on a risk assessment (include 'risk based' wording from our DPIA guidance). Emphasis on the involvement of the competent authority's Data Protection Officer at an early stage is critical as they will be best placed to give expert advice on data protection obligations that can inform the development of the DPIA. The Code should also mention the ICO prior consultation mechanisms in place under Part 3 DPA 2018. We also recommend that the Code links to the ICO's guidance for conducting a DPIA, including links to our guidance on DPIAs under Part 3 of DPA 2018 and to our more detailed guidance on DPIAs under the UK GDPR.

Commissioner's Opinion On the use of Live Facial Recognition Technology by Law Enforcement in Public Places

The use of Live Facial Recognition (LFR) in Law Enforcement context has received a lot of attention in recent years and has been the subject of a number of court cases in England and Wales. In 2020, the Court of Appeal ruled that a deployment by South Wales Police was unlawful.

Live Facial Recognition is just one example of biometric technology that presents specific privacy and wider risks to individuals and which Police Scotland may consider in the future. In 2019, the then Information Commissioner, Elizabeth Denham, set out in an Opinion that*: '.. the law being relied upon for the use of LFR must have sufficient clarity and foreseeability to meet the standards required by the case law of the Court of Justice of the European Union and the European Court of Human Rights, as contemplated in Recital 33 to the EU Law Enforcement Directive. In other words, could an individual reasonably expect that their image could be processed, and data captured in this way, and understand why this was happening*?'

The ICO is currently working with stakeholders in England and Wales including the College of Policing, Home Office and National Police Chiefs' Council to address this point and to support the existing legal framework in England and Wales with a package of clear guidance and Codes of Practice for forces. This includes new guidance which is being developed by the College of Policing.

Of course, the need for clarity, foreseeability and appropriate privacy protections holds true in Scotland also. The Code of Practice can be a central component but it should also sit alongside more detailed guidance and Standard Operating Procedures that relate to the specific technology in question in order to provide Police Scotland with support and a clear understanding of the measures that need to be in place if using biometric technologies. In turn, these measures should promote regimes which promote public trust and confidence in public services. We have made recommendations below as to how the draft principles could be strengthened but we also suggest that the principles include a requirement to develop clear and detailed guidance governing the deployment of privacy intrusive biometric technologies such as LFR.

The Guiding Principles

We have provided comments below where the principles overlap with existing obligations under data protection law and the previous Commissioner's recommendations in her 2019 Opinion.

We note that there is a fair degree of crossover between the principles and therefore some repetition. For clarity, ease of reading and to aid assessment of compliance, we would recommend that these are developed further so that each principle can be presented as a concise standalone principle. Guidance on what compliance looks like could be more detailed and should provide cross references where appropriate.

1. **Lawful Authority and Legal Basis:** The first data protection principle (Section 35, DPA 2018) says that processing is lawful only to the extent that it is "based on law". This means that the processing must be authorised by either statute, common law or royal prerogative, or under any other rule of law. Recital 33 of the EU Law Enforcement Directive says that: '*such a Member State law, legal basis or legislative measure should be clear and precise and its application foreseeable for those subject to it.*' In addition the processing is only lawful to the extent that it is *necessary* for the law enforcement purposes, or based on consent. Where the processing in question is 'sensitive processing' (most but not all of the data within the scope of this Code will fall into this category), the bar is higher still and the competent authority must be able to demonstrate that the processing is **strictly necessary** and be able to satisfy one of the conditions in Schedule 8 of the DPA 2018. Schedule 1 of the DPA 2018 relates to processing under the UK GDPR and is not relevant here. It is important to be aware that although consent is an available lawful basis, there will only be limited circumstances when competent authorities will, in practice, be able to rely on consent. This is because the bar for valid consent is very high and cannot be met where there is a power imbalance or where it cannot be withdrawn without detriment.

Our recommendation is that this principle is tightened and amended along the following lines:

- That it sets out a requirement that the lawful authority must be based in law and that the law provides a sufficiently clear and foreseeable basis for the processing. Specifically it must have sufficient clarity and foreseeability to meet the standards required by the case law of the Court of Justice of the European Union and the European Court of Human Rights, as contemplated in Recital 33 to the EU Law Enforcement Directive.
- That it emphasises the necessity element (this may simply mean cross referencing with the necessity principle);
- That the wording reflects that although it may be possible for competent authorities to gain valid consent in a few limited circumstances, these will be the exception rather than the rule (currently it reads as if consent is the default);
- Given the above, this wording: '*If biometric data is obtained from a crime victim or witness with their consent and solely for elimination purposes, then such data should only be retained in connection with the*

case to which they relate' should, for the avoidance of doubt, be amended to: *'If biometric data is obtained from a crime victim or witness with their agreement and solely for elimination purposes…'*

- Biometric data should only be retained for as long as is necessary. This may in practice be a shorter time frame than the relevant case file is retained. This principle should make it clear that case files should be regularly reviewed and weeded in line with procedures that comply with the Fifth Data Protection Principle (Section 40, DPA 2018) as is appropriate. See our comments on retention below.
- The principle references biometric data obtained, retained or used under 'other voluntary arrangements' and says that this should only be undertaken with the express consent of the data subject. It goes on to say '*Where consent to the holding of such data under voluntary arrangements is withdrawn, then that data can no longer be retained and should be destroyed as soon as reasonably practicable, providing that such removal will not, at the time of the request, conflict with any evidential requirement concerning the sample, data or information derived from it*.' It is not clear what these 'voluntary arrangements' may be. As identified above however, the bar for valid consent under data protection law is very high and is not met in circumstances where it cannot be freely withdrawn. Seeking express consent in these circumstances would likely infringe both the 'lawful' and 'fair' component of the First Data Protection principle. Individuals do however have the right to request erasure and restriction of the processing of their personal data. It may be therefore that the Code recommends that where such requests are made in relation to data that has been obtained or acquired under 'voluntary arrangements' there is a presumption in favour of erasure or restriction. Our guidance makes it clear that individuals can make this request in writing or verbally. It is also worth noting that there is a statutory timeframe of one calendar month within which rights requests must be responded to.

2. **Necessity:** ICO guidance defines 'strictly necessary' as '*that the processing has to relate to a pressing social need, that cannot reasonably be achieved through less intrusive means.'* As noted above processing may be based on consent, but it is unlikely that there will be many circumstances in which the conditions for valid consent can be met. Given the overlap with obligations under data protection law, it may be useful if the Code uses the same definition.

3. **Proportionality:** It would be useful for competent authorities if the Code expanded on the meaning of proportionality as a principle. Proportionality

under data protection law requires that the benefits of the activity outweigh the adverse impact of such processing on the rights of the individuals whose biometric data it is. It is for the controller to articulate how the processing of biometric data will be effective in meeting the specified law enforcement purpose and in turn the demonstrable benefit to the public. How is the biometric processing, instead of possible other viable alternative means, proportionate to the criminal justice or policing purpose pursued and how will this rationale be documented?

5. Ethical Behaviour: Please note our view on consent above. We recommend that the language is modified here to recognise that consent will be the lawful basis for processing in a minority of circumstances. Transparency is a key obligation under UK GDPR and so we welcome the focus on it. It is important to recognise that in many circumstances competent authorities will be unable to inform individuals when their biometric data is being processed because doing so would prejudice the law enforcement purpose. Nonetheless, relevant authorities should communicate openly and clearly with the public about how they intend to use and deploy biometric data and technology. This supports foreseeability and helps ensure that the processing is fair and within reasonable expectation. This can be done via Privacy Information, public consultation and engagement and other communications tools. In England and Wales, for example, the Surveillance Camera Code of Practice sets out that forces in these jurisdictions must: *'set out and publish (a) the categories of people to be included on a watchlist and (b) the criteria that will be used in determining when and where to deploy LFR, having regard to the need only to do so for a lawful policing purpose'*; Fair processing also means that the processing does not result in an unjustified adverse impact on an individual. We therefore welcome the recognition of the risks associated with the inherent bias in Artificial Intelligence (AI) associated with biometric technologies. It may be helpful to refer competent authorities to relevant ICO guidance including: the explaining decisions made with AI; the guidance on AI and data protection and toolkit for organisations considering using data analytics. These could be linked to within the Code or accompanying guidance/supporting materials. Where AI is being used it is of paramount importance that authorities demonstrate compliance with accountability, fairness and transparency and facilitate access to individual's information rights. In the majority of cases there is a legal requirement to complete a DPIA if you use AI systems that process personal data.

As currently drafted the principle says: "*Biometric data acquired for a specific criminal justice or policing purpose in Scotland should not be shared for non-policing or non-criminal justice purposes in Scotland or with other jurisdictions except in accordance with the Data Protection Act 2018 and the Data Sharing Code of Practice produced by the UK Information Commissioner (ICO). Otherwise, data sharing between Scotland and other UK and International policing and criminal justice jurisdictions is encouraged."* It is welcomed that the Code references our Data Sharing Code of Practice but it would benefit from linking directly to it so that organisations can seek further information prior to sharing personal data. It is important to note here that data sharing with other UK and international policing bodies must still be carried out in accordance with data protection law and, in particular, policing bodies should formalise data sharing agreements for routine data sharing and devise plans that cover ad hoc or emergency data sharing. Data sharing taking place internationally needs to be in accordance with Part 3, Chapter 5 of the DPA 2018 and it could be of benefit to include links to our guidance on Law Enforcement processing and international transfers.

6. Respect for the Human Rights of Individuals and Groups: The second paragraph of principle 6 notes that "data protection rules change when someone dies", however it should be categorical here as data protection legislation only applies to living individuals and therefore data protection laws no longer apply.

7. Justice and Accountability: It would be useful if the Code expanded on the meaning of accountability as a principle. Section 34(3) DPA 2018 requires controllers to be responsible for and demonstrate compliance with Part 3. Specifically it requires the implementation of appropriate technical and organisational measures that ensures and demonstrates that the controller is compliant with Part 3 DPA 2018. It would be of benefit if the Code listed practical and illustrative examples of the specific types of measures that would support and guide controllers with the development of a strong and comprehensive governance regime for the processing of biometric data. Our guidance lists some examples which may be a useful starting point but these would need to be further discussed with the named competent authorities to ensure they are specific and proportionate to the processing activity in question:

- data minimisation;
- pseudonymisation;
- transparency, where appropriate;

- creating and improving security features on an ongoing basis; or
- data protection impact assessments where appropriate.

The draft Code says "*Any finding of a substantive breach of the Data Protection Act 2018 by the ICO may then be considered by the Scottish Biometrics Commissioner as a potential breach of this Code of Practice*." It should state that these processes would be separate and the individual raising the complaint would need to raise a separate complaint with the SBC following the ICO's adjudication, This can be considered within the MOU between the Information Commissioner and the ICO. We would also recommend the publication of documentation about complaints procedures so it is available to members of the public.

8. **Encourage Scientific and Technological Advancement:** We welcome the inclusion of the 8th principle in the Code which considers the adoption of new and emerging technologies in the area of biometrics. Forward planning and early consideration of such technologies can facilitate compliance with data protection by design default and help controllers to mitigate any compliance issues before they arise. This could further ensure that data protection is integrated in the processing activities from the beginning. The completion and continual evaluation of DPIAs will be essential to this process. It is likely that third parties, whether as a supplier or a processor, will be involved in the supply of new technologies and controllers will need to ensure that the supplier can provide the controller with sufficient detail about the proposed technology, particularly around storage, access, security, and risks so the controller understand the technology and can document this appropriately. Identifying and mitigating associated risks will be of particular importance and this could be included as a separate step within the process map at Annex C. Staff training will, as the Code has identified, be essential. Our Accountability Framework, which has a section on Training and awareness, which in turn has a section on Specialised Roles highlights that those staff will require additional training and development.

9. Protection of Children, Young People and Vulnerable Adults: We welcome the development of internal policies and processes to support the protection and safeguarding of children, young people and vulnerable adults. Individuals, under data protection law also have the right to be informed about the collection and use of their personal data and the Code could go further in encouraging the requirement for outward facing documentation that is particularly tailored to certain audiences such as children, young people and adults with additional support needs. This may

require consideration of the language used, the inclusion of infographics, videos, icons or a layered approach. The information a controller must supply about the processing of personal data must be:

- concise, intelligible and easily accessible;
- written in clear and plain language, adapting this to the needs of vulnerable persons, such as children; and
- free of charge

The right to this information is however a qualified right and subject to restrictions that prevent any prejudice to an ongoing investigation or compromise to operational techniques. The reliance on a restriction should be justified and applied as necessary and proportionate, and on a case by case basis. It is important that controllers balance the rights of the individual against the harm disclosure would cause.

12. Retention authorised by law: We would recommend strengthening this principle to include a presumption against indefinite retention periods for biometric data. Indefinite retention periods pose risks for individuals and bring to the data controller a responsibility to ensure the processing is compliant with the principles for its lifetime. Section 39, Part 3 of the DPA 2018 states that "*Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes."* Placing a responsibility on controllers to carry out periodic reviews of retained biometric data will ensure that the data held: is processed fairly (the first principle); adequate, relevant and not excessive (the third principle); accurate and kept up-to-date (the fourth principle); not kept for longer than is necessary for the purpose for which it is processed (the fifth principle); and securely kept, using appropriate technical and organisational measures (the sixth principle).

On page 28, it is stated that "*If a biometric data type has no retention period prescribed in law (for example photographs) then you should apply the same period of retention as you would for other types of biometric data, such as DNA and fingerprints*." We recommend that the retention period is linked to purpose rather than type of data. This would bring this principle in line with data protection law and would be fairer and more proportionate. In all cases the retention of biometric data should be justified (with evidence to support the proposed retention periods) and only be kept for so long as is **necessary** for the **purposes** for which it is processed and this should be emphasised within the Code.

It is not clear why the retention period for biometric data of children aged 16 and 17 would be the same as an adult (noting our concerns about the proposed retention periods for the biometric data of adults). The processing of children's biometric data merits particular protection and particular care should be taken to ensure that it is fair. There should be a strong justification for any lengthy retention of children's biometric data and the risks associated with the processing must be recognised, assessed and managed.

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 this guidance is further developed please do not hesitate to get in touch either with myself or my colleague Regional Manager, at.

Yours sincerely

Head of ICO Regions