

# **ICO submission for the Justice Committee on the Justice Bill**

## **1. About the Information Commissioner's Office (ICO)**

- 1.1 The ICO is the UK's independent public authority set up to uphold information rights and has responsibility for enforcing and overseeing a range of legislation including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and the Freedom of Information Act 2000, among others.
- 1.2 The Information Commissioner is independent from the Government and upholds information rights in the public interest, promotes openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action when the law is broken.
- 1.3 As a UK wide regulator, the ICO has offices across the UK, including one in Belfast where the Northern Ireland Affairs team are based, comprising a small team of policy staff who are responsible for leading engagement with Northern Ireland stakeholders on Northern Ireland issues.

## **2. Introduction and background**

- 2.1 The ICO welcomes the opportunity to provide written evidence to the Committee for Justice on the Justice Bill, in particular the proposals regarding the retention of biometric data. Data protection is an important part of the framework governing the use of biometric data, and the ICO plays a significant and active regulatory role in this complex landscape.
- 2.2 We welcome the Committee for Justice's commitment to provide detailed scrutiny of the proposals contained within the Justice Bill. We have provided our written submissions below, focusing on the parts of the Bill which fall within our regulatory remit. We hope this will aid the Committee in their scrutiny.

## **3. Data protection legislative framework for law enforcement processing**

- 3.1 For the purpose of this submission, it is important to distinguish between the two different legislative frameworks for data protection in the UK.

- 3.2 The UK GDPR relates to the general processing of personal data by organisations and is the UK's version of the EU GDPR.
- 3.3 Sitting alongside this is the DPA 2018, Part 3 of which details the requirements on organisations processing personal data for law enforcement purposes. Part 3 of the DPA 2018 implemented the EU Law Enforcement Directive into UK law. The relevant data protection framework concerning the provisions proposed within the Justice Bill is therefore likely to be Part 3 of the DPA 2018.
- 3.4 Part 3, Chapter 2 of the DPA 2018 sets out six data protection principles which comprise the main responsibilities organisations should follow when processing personal data for law enforcement purposes. The six principles are:
- **The first principle:** processing of personal data must be lawful and fair.
  - **The second principle:** the purpose for which personal data is collected must be specified, explicit and legitimate, and must not be processed in a manner that is incompatible with the purpose for which it was originally collected.
  - **The third principle:** personal data must be adequate, relevant and not excessive in relation to the purpose for which it is processed.
  - **The fourth principle:** personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay.
  - **The fifth principle:** personal data must be kept for no longer than is necessary for the purpose for which it is processed. 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.
  - **The sixth principle:** personal data must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.
- 3.5 Any organisation processing personal data for law enforcement purposes is 'responsible for, and must be able to demonstrate, compliance with' the above principles, which in practice means, being able to evidence compliance.

## 4. Part 1 of the Justice Bill - Biometric data

### Biometric data and data protection law

- 4.1 Biometric data is defined under section 205(1) of the DPA 2018 as “personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images or dactyloscopic data”.
- 4.2 The use of biometric data to uniquely identify an individual is regarded as ‘sensitive processing’<sup>1</sup> under section 35(8) of the DPA 2018. This is because it carries greater risk and may have a greater impact on individuals’ rights. As such, this type of processing requires organisations to ensure that higher levels of protection and safeguards are in place for those individuals.
- 4.3 Where sensitive processing is taking place, the organisation responsible for processing the data (known under data protection law as the ‘controller’<sup>2</sup>) must be able to demonstrate that processing for a law enforcement purpose is either based on consent or alternatively, is ‘strictly necessary’ and must satisfy additional legislative conditions. Strictly necessary imposes a more exacting standard than ‘necessary’, and in practice calls for a more rigorous justification for why such information is being processed, including why it is being retained<sup>3</sup>.

### Replacing indefinite biometric retention

- 4.4 The ICO recognises that Part 1 of the Justice Bill and the proposed changes to biometric retention aim to ensure compliance with judgments of the European Court of Human Rights and the UK Supreme Court (S & Marper v UK (2008) and Gaughran v UK (2020)).
- 4.5 Our office responded to the DoJ’s 2020 public consultation on the proposals to amend the legislation governing the retention of DNA and fingerprints in Northern Ireland and welcomed the move away from indefinite retention of such material to a more nuanced regime.
- 4.6 We welcome the proposal contained in clause 1 of the Justice Bill to introduce a basic rule that biometric material must be destroyed, unless it can be retained under the rules set out in**

---

<sup>1</sup> [Principles | ICO](#)

<sup>2</sup> [Scope and key definitions | ICO](#)

<sup>3</sup> [Principles | ICO](#)

**Article 63D to 63U. It is our view that this proposal goes some way to ensuring compliance with the fifth principle set out above, when compared with the indefinite retention of biometric material.**

## Retention limitations

- 4.7 We welcome the proposal to replace the indefinite retention of biometric material with maximum retention periods, based on age of the offender, severity of the offence, and the outcome of the case.
- 4.8 As a principles-based piece of legislation, the DPA 2018 does not set out specific or defined retention periods. Instead, it requires that data be kept no longer than is necessary, and it is up to each organisation to determine what is necessary in their circumstances, based on the type of personal data being processed and the nature of the processing.
- 4.9 The DoJ must therefore be able to justify and evidence how the proposed retention periods set out within Article 63 are reasonable, particularly with respect to the proportionality and strict necessity of the proposed time frames. Given the extended periods for which data would be retained under the longest retention periods, which in practice are likely to result in this material being retained for the whole, or majority of, an individual's life time, we would expect to see consideration of both the risks to the individuals' whose data is being retained, and the reasons why this level of retention is necessary. This may include evidence such as reoffending patterns and the value of retaining data in the detection and prevention of other crimes.
- 4.10 We would recommend that the Committee seek evidence and assurances from the DoJ that the retention periods proposed within the Justice Bill are justified based on the age of the offender, severity of the offence, and disposal/sentence, and that they meet the requirements of strict necessity and proportionality<sup>4</sup> set out within the DPA 2018.**
- 4.11 The DoJ must also be able to justify how the proposed review period of every five years, which is set out under Article 63T, is reasonable and proportionate with respect to fingerprint and DNA material retained pending investigation of offences.
- 4.12 We would recommend that the Committee seek evidence and assurances from the DoJ that the review period of every five years proposed within Article 63T for biometric material retained**

---

<sup>4</sup> [ICO guidance on 'strictly necessary'](#)

**pending investigation of offences is justified, strictly necessary and proportionate.**

## Review of long term retained biometric material

- 4.13 We note the provisions within the Justice Bill pertaining to the proposed biometric review mechanism for long-term retained material, as set out under Article 63U. Article 63U notes that the DoJ must make regulations that require the Chief Constable of the Police Service of Northern Ireland (PSNI) to conduct reviews of the continued retention of long-term retained material, where material is held for 25 years and over.
- 4.14 As set out in section 3.4, the compliance requirements regarding the fifth data protection principle are twofold, as it requires that personal data is retained for no longer than is necessary, but also that appropriate time limits are established for the periodic review of the continued retention of personal data for criminal law enforcement purposes.
- 4.15 Given that Article 63U proposes to introduce a requirement on the DoJ to make regulations on conducting reviews of long term retained material, it is currently not possible to assess whether the proposals will fully comply with the fifth principle until further details on the review mechanism are available. For this reason, it would have been more helpful for the details of the review mechanism to be built into the primary legislation instead of via secondary regulations.
- 4.16 We would recommend that Article 63U should set out the appropriate time limits for the periodic reviews of biometric material.**
- 4.17 In the event that Article 63U is not amended as per recommendation 4.16 above, we would recommend that clarification be sought by the Committee on the interim position between the enactment of the Justice Bill and the making of regulations regarding the review mechanism, and how PSNI will ensure full compliance with the fifth data protection principle during this time.**

## Convictions outside of the UK

- 4.18 We note the proposals contained within Article 63N of the Justice Bill providing for the retention of biometric material where an individual is convicted of an offence outside Northern Ireland.

4.19 If the application of this article requires the PSNI to implement any international transfers of biometric data for law enforcement purposes, PSNI will need to ensure compliance with Part 3, Chapter 5 of the DPA 2018 which sets out the requirements for transferring such personal data to, what is referred to as, a ‘third country’<sup>5</sup>. This is a complex area of data protection law and we would be happy to advise the DoJ and/or PSNI further on the relevant requirements.

**4.20 The Committee should seek assurances from the DoJ that consideration has been given to the potential international transfer requirements concerning the proposals within Article 63N.**

**The Northern Ireland Commissioner for the Retention of Biometric Material (‘the Biometrics Commissioner’)**

4.21 Data protection law is an important part of the legal framework governing the use of biometric data. It helps to ensure transparency and accountability in the use of biometric data, as well as new technology, and to empower people by giving them rights in relation to their data.

4.22 Data protection is a necessarily broad, principles-based regulatory framework. The provisions contained within the Justice Bill must comply with the six principles of data protection outlined in section 3.4 above.

4.23 We welcome the additional oversight that the role of a Biometrics Commissioner would bring, which will provide clarity and regulatory certainty to organisations, and in turn, trust to citizens. It is important to ensure that regulatory activity is undertaken in a way which enables individuals, organisations and other stakeholders to be clear about how the responsibilities of the Information Commissioner and the Biometrics Commissioner are discharged individually, and collectively.

4.24 The ICO’s role also extends to the regulation of biometric material and there appears to be the potential for some overlap between the proposed functions of the Biometrics Commissioner and those already exercisable by our office.

4.25 We note the proposed functions of the Biometrics Commissioner are to “keep under review”, and issue guidance about, the acquisition, retention and use of biometric material, as well as to “keep under review the use and development of existing and new biometric technologies used by, or

---

<sup>5</sup> [International transfers | ICO](#)

capable of being used by, law enforcement authorities for the prevention and detection of crime”.

**4.26 We would ask the Committee to seek additional information from the DoJ as to what is meant by “keep under review” in the context of the Biometrics Commissioner’s proposed functions.**

4.27 We would seek to work in partnership with the Biometrics Commissioner, once appointed, as we do with similar Commissioners in Scotland, England and Wales, in the conduct of our respective statutory duties. We would be keen to explore the development of a memorandum of understanding (‘MoU’) with the Biometrics Commissioner to help manage any overlap between our respective roles and provide clarity and certainty to the regulated organisations.

## **5. General data protection implications regarding the biometric proposals**

### Transparency and the right to be informed

- 5.1 The first data protection principle for law enforcement processing requires the processing to be both lawful and fair<sup>6</sup>. ‘Fairness’ means organisations must not process personal data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned. It also requires organisations to be clear and open with individuals about how their information is used, in keeping with their reasonable expectations.
- 5.2 Under Part 3, Chapter 3, section 44 of the DPA 2018, individuals have the right to be informed<sup>7</sup> when their information is being processed for law enforcement purposes. They should be provided with this information in a concise, intelligible and easily accessible way, using clear and plain language, which if necessary is adapted to the needs of vulnerable people.
- 5.3 It will be important for PSNI to inform individuals in advance as to how their biometric material is going to be processed by the service, including the period of time for which it will be retained and the reasons for this. Providing this information to individuals is crucial in order to ensure compliance with the first principle and in the interests of fairness, openness, transparency and building trust.

---

<sup>6</sup> [Principles | ICO](#)

<sup>7</sup> [The right to be informed | ICO](#)

- 5.4 **The Committee should seek assurances from the DoJ that the proposals contained within the Bill will comply with the transparency obligations and right to be informed requirements set out in the DPA 2018. We recommend that the relevant PACE Codes of Practice are updated to reflect these requirements.**

### Individuals' rights under the Justice Bill proposals and DPA 2018

- 5.5 Under Article 63U of the Justice Bill, the DoJ may make provisions within regulations enabling an individual to request that a review be conducted into the continued retention of their long-term retained biometric material and may also confer a right of appeal against a determination made.
- 5.6 The DPA 2018 provides individuals with data protection rights<sup>8</sup>, such as the right to request the erasure<sup>9</sup> of personal data. It also provides a procedure for individuals raising their complaint with the ICO when they have concerns about how an organisation is processing their personal data, as well as the possibility of seeking redress before the courts.
- 5.7 We do not foresee that there will be a conflict between existing data protection rights and the proposed rights for individuals set out within the Justice Bill.
- 5.8 The rights under data protection law are not absolute, particularly the right to request deletion or removal of personal data. Organisations must erase personal data without undue delay where processing the data will infringe the data protection principles; where the organisation does not meet safeguards for archiving and processing of sensitive personal data; or where there is a legal obligation to erase the data.
- 5.9 In practice, if PSNI have reviewed the retention of an individual's data in accordance with the proposed provisions of the Justice Bill and decided that it was necessary and proportionate to retain the data, it is likely that their conclusion to refuse a request for deletion would be well founded and they would not be in breach of data protection.
- 5.10 The rights afforded to individuals under the Justice Bill proposals to request a review into long-term retained material and those under Part 3 of the DPA 2018, are separate, as are the secondary appeal processes to the Biometrics Commissioner proposed under the Justice Bill, and the ICO under the DPA 2018. We would recommend that consideration is given to how the rights and appeal rights of an individual will be clearly

---

<sup>8</sup> [Individual rights | ICO](#)

<sup>9</sup> [The right to erasure and the right to restriction | ICO](#)

communicated to them in relation to their biometric material from the outset.

**5.11 We advise the Committee to seek clarification from the DoJ in relation to how an individual will be made aware of their rights and appeal options, both in respect of the long-term retention of their biometric material proposed under Article 63U and the right to erasure under Part 3 of the DPA 2018.**

### Children's biometric data

5.12 The obligations to ensure transparency and the right to be informed require additional measures for children, with the legislation requiring organisations to provide transparency information in a way in which the individual will understand, ensuring that it is adapted to the needs of vulnerable persons, such as children<sup>10</sup>. Given the sensitive nature of biometric data, the fairness requirements mentioned in section 5.1 above may also require these additional measures to ensure fair outcomes for children.

**5.13 The Committee should also seek clarification from the DoJ on what efforts have been made to ensure that children will be appropriately informed to ensure the required transparency around the retention of their information.**

### IT systems and security

5.14 It is important that the DoJ takes into consideration the IT systems and software which will be required to implement the changes to biometric retention and the proposed review dates generated under the review of long-term retained biometric material.

5.15 Before the changes are implemented, PSNI must have the appropriate systems in place to administer the changes and to handle and store the data securely, as required under the sixth data protection principle. This requires organisations to have technical and organisational measures in place to ensure that personal data is protected with an appropriate level of security.

5.16 It is also likely that biometric data may be shared across different law enforcement databases in the UK, and this could include data being held on national databases across England, Wales and Scotland, such as the UK Police National Database. It is important that DoJ considers the

---

<sup>10</sup> [The right to be informed | ICO](#)

possible variation in retention periods across the different UK jurisdictions following the proposed changes to the legislation in Northern Ireland.

**5.17 We would advise the Committee to seek assurances from the DoJ and PSNI that the required IT systems and capabilities will be in place to support the implementation of the proposed biometric framework in line with the requirements set out in the DPA 2018.**

**5.18 We would advise the Committee to seek information from the DoJ on whether they have considered how the PSNI will be able to securely manage and implement varying retention periods when biometric data is shared across different UK databases and ensure individuals are appropriately informed of this.**

### Automated decision making

5.19 The DoJ must also give consideration as to whether there will be meaningful human involvement in the processing relating to the calculation of retention periods and decisions to retain or delete, or whether these decisions will be automated.

5.20 Part 3 of the DPA 2018 provides safeguards for individuals against the risk that a potentially damaging decision is taken by solely automated means, i.e. without human intervention. It is important that the DoJ consider whether any automated decision making in relation to the retention of an individual's biometric data, will likely have a legal or similarly significant effect.

**5.21 We would recommend that the Committee seek clarification as to whether there will be any automated decision making in the retention of an individual's biometric data and, if so, how the requirements under Part 3 of the DPA 2018 will be satisfied in respect of such decisions.**

### Implications of photographs

5.22 While fingerprint and DNA profiles are undoubtedly considered to be biometric data, the position is not so clear in relation to custodial photographs.

5.23 Our view is that while someone's physical characteristics may be shown in a photo, this isn't enough to make that photo biometric data. It's only when something else happens to that photo, such as a discrete processing operation or set of operations that result in something that allows or confirms someone's unique identification, that the result becomes biometric data. For example, if specific techniques are applied to

the photo to extract someone's facial features, then the photo has been "processed through a specific technical means" that allows the person to be uniquely identified.

**5.24 We would recommend that the Committee seek clarification as to whether further technical processing of custody photos is taking place to render them biometric material as per section 5.23 above. We would welcome further engagement with the DoJ as they progress their thinking in this area.**

## **6. Part 3 of the Justice Bill – Use of live links**

- 6.1 We note the proposals within Part 3 of the Justice Bill to enable video-conferencing technology (referred to as 'live links') to be used by police for a number of custody functions. We note the Bill also seeks to introduce amendments for the use of live links by courts and tribunals.
- 6.2 We consider there to be a number of data protection implications concerning the use of such live link technology. The relevant organisation(s) deploying such technology will need to be satisfied that there are proper safeguards in place to protect vulnerable individuals, including children, when using live links. This includes providing them with appropriate transparency information to ensure they understand how their information is being used. They will need to ensure that appropriate security measures are in place for the live link technology, including access controls so that only relevant staff have access to the software. Consideration must also be given as to whether any recordings of the live link will take place, and if so, that the technology can satisfy any requests for access to such footage from individuals captured within it.
- 6.3 We would recommend that the Committee seeks clarification from the DoJ as to the data protection considerations that have been applied to the live link technology, such as those outlined above.**

**Should you have any queries on this submission, please do not hesitate to contact our office by emailing [ni@ico.org.uk](mailto:ni@ico.org.uk)**