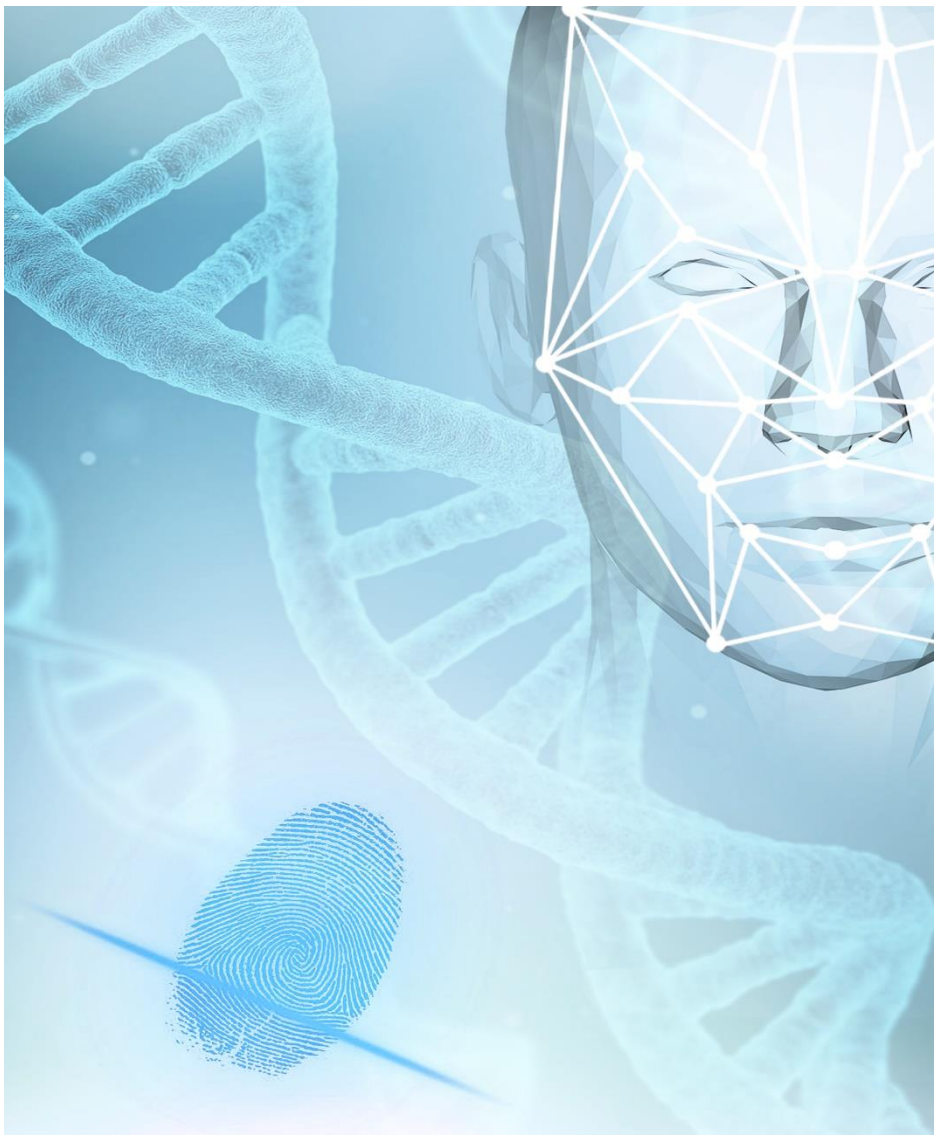

CODE OF PRACTICE

On the acquisition, use, retention and disposal of biometric data for justice and community safety purposes in Scotland.

DRAFT FOR PUBLIC CONSULTATION

Contents

Item	Page
Part 1 – Background, context and purpose of the Code	4
Background	4
Introduction	4
Defining 'biometric data'	5
Purpose of this Code of Practice	5
Bodies to whom this Code applies	5
Adoption by other public bodies on a voluntary basis	6
Private sector/law enforcement interface	6
Part 2 – The Law, Human Rights and Data Protection	7
The Law - Biometrics in the criminal justice process	7
The Law - Public Sector Equality Duty	8
The Law - Human Rights	9
The Law – Data Protection	10
Part 3 – 'General Principles' and ethical considerations	11
General Principles for the use of biometrics	12
Implementation of the 'General Principles'	12
Considerations regarding the collection and processing of biometric data	13
Validation and reliability of techniques	13
Part 4 – Privacy by design	14
Data Protection Impact Assessments (DPIA's)	14
Part 5 – Information to be provided to people	15
Information to be provided in the criminal justice process	15
Biometrics information sheet for prisoners	15

Part 6 – Biometric data review and appeals process 16

Appeal to public body holding data 16

Review requests to Scottish Biometrics Commissioner 16

Part 7 – Children and vulnerable adults and groups 17

Children in the criminal justice system 17

Vulnerable adults and groups in the criminal justice system 18

Part 8 – Compliance with the Code of Practice 18

Oversight of the Code by the Commissioner 19

Breaches of the Code of Practice 19

Glossary of Terms 20

Part 1 – Background, context and purpose of the Code

Background

1. In May 2017, prominent Solicitor Advocate John Scott QC, was asked by the then Cabinet Secretary for Justice, Michael Matheson MSP, to chair an Independent Advisory Group (IAG) to review the retention of custody images by Police Scotland. This followed the publication of a report in 2016 by Her Majesty's Inspectorate of Constabulary in Scotland (HMICS) on the use of facial search technologies, which called for improved legislation and independent oversight of the use of biometric data for policing, law enforcement, and other public protection purposes in Scotland[1]. The Cabinet Secretary for Justice also asked that the Group consider the use and retention of biometric data more generally in policing to seek to establish an ethical and human rights based framework which could be applied to existing, emerging and future biometrics in what is an important and fast moving area of technology.

2. In February 2018, the report of the IAG was delivered to the Cabinet Secretary for Justice. The report made nine recommendations, including proposals to create a Biometrics Commissioner for Scotland and to establish a statutory Code of Practice in relation to the acquisition, retention, use and disposal of biometric data by Police Scotland, the Scottish Police Authority (SPA) and other bodies working in the field of law enforcement.

3. The report of the IAG to the Cabinet Secretary for Justice and the response to that report from the Scottish Government is published on the Scottish Government website: http://www.gov.scot/Publications/2018/03/9437.

Introduction

4. It is a fundamental value of our society that we respect the right of every person to go about their lawful business without unjustified interference from the State. Where the State does interact with any person, that interaction should be governed by a respect by the State for that person, and for that person's freedoms and rights. In all its interactions the State must act with fairness and integrity, and in compliance with the law. Police work is an example of the interaction between the State and the individual, sometimes when the individual is at their most vulnerable. This Code must therefore be read considering that fundamental value.

5. Police work in Scotland is carried out in accordance with the policing principles set out through the Police and Fire Reform (Scotland) Act 2012. These are:

- that the main purpose of policing is to improve the safety and wellbeing of persons, localities and communities in Scotland; and

- that the Police Service (Police Scotland), working in collaboration with others where appropriate, should seek to achieve that main purpose by policing in a way which -
  i. is accessible to, and engaged with, local communities; and
  ii. promotes measures to prevent crime, harm and disorder.

[1] Audit and Assurance Review of the use of the Facial Search functionality within the UK Police National Database (PND) by Police Scotland. HMICS, 2016: https://www.hmics.scot/publications/audit-and-assurance-review-use-facial-search-functionality-within-uk-police-national

These policing principles inform all police work and, by extension, this Code.

Defining 'biometric data'

6. For the purposes of this Code of Practice, we define biometric data as:

> ***'any physical, biological, physiological or behavioural data, derived from human subjects, which have the potential to identify a known individual.'***

7. From this definition it is clear that 'biometric data' is a relatively broad and evolving concept. It encompasses what is often referred to as 'first-generation biometrics' such as fingerprints, DNA and custody photographs which have been commonly used in policing for many years. It also includes biological samples and materials from which such biometric data can be obtained, including materials obtained initially for medical purposes which subsequently come into the possession of the police as part of a criminal investigation. It also includes new and emerging technologies (or 'second-generation biometrics') such as facial recognition software, remote iris recognition, and other behavioural biometrics such as voice pattern analysis. Finally, it includes data collected in other non-policing public sector contexts from citizens engaged in routine activity such as public space CCTV surveillance cameras, road safety enforcement cameras and automatic number plate systems, some of which can capture and store the facial images of citizens. Again, there will be instances when such data subsequently comes into the possession of the police to support their work.

8. It therefore follows from this definition that other forms of data routinely collected by the police and other relevant bodies such as the names, addresses, dates of birth or general physical descriptions of suspects or witnesses does not qualify as 'biometric data' as such information does not render unique or distinct physical, biological, physiological or behavioural data.

Purpose of this Code of Practice

9. This Code of Practice describes the legal framework concerning the acquisition, retention, use and disposal of biometric data for justice and community safety purposes in Scotland. It also contains a set of written rules or 'General Principles' outlining the responsibilities of those to whom this Code applies. Those General Principles embody wider legal, ethical, human rights and data protection considerations as set out in this Code of Practice, including the special considerations to be made for children, vulnerable adults and protected characteristic groups. The contents of this Code will apply to Police Scotland, the SPA and other specified bodies retaining biometric data for criminal justice and community safety purposes within the devolved competence of the Scottish Parliament. The requirement for compliance with the Code of Practice to be promoted by the Scottish Biometrics Commissioner will be set out in statute.

Bodies to whom this Code applies

10. This Code of Practice in relation to the acquisition, retention, use and disposal of biometric data for justice and community safety purposes in Scotland will apply to Police Scotland and the Scottish Police Authority (SPA). The Chief Constable of Police Scotland and the Board of the SPA will ensure that internal systems and processes are in place to ensure compliance with the Code.

11. This Code will also apply to biometric data use for any other policing and law enforcement purpose subject to the competence of the Scottish Parliament. Specifically, it will extend to any other bodies who may collect biometric data whilst exercising powers of arrest for devolved purposes, including the exercise of any of the powers and privileges of a Constable when investigating a matter under the direction of the Crown Office and Procurator Fiscal Service[2]. The Code does not extend to the retention of biometric data for the purposes of UK national security. Responsibility for these matters falls within the statutory remit of the Biometrics Commissioner for England and Wales. Similarly, this Code does not extend to general data protection matters within the statutory remit of UK Information Commissioner.

12. Nothing in this Code of Practice alters or otherwise affects any provision in any statute which makes express provision as to the acquisition, use, retention or disposal of biometric data for justice and community safety purposes in Scotland.

13. Nothing in this Code of Practice alters or otherwise affects any existing rule of law or legal test about the admissibility of evidence with regards to any form of biometric data.

Adoption by other public bodies on a voluntary basis

14. The primary purpose of this Code is to guide the use of biometric data for justice and community safety purposes in Scotland. However, there are also many other public authorities who collect biometric data from citizens engaged in routine activity. This includes, but is not limited to, local authorities and others operating public space CCTV surveillance systems, speed and red-light enforcement cameras funded by the Scottish Safety Camera Programme with data handling by Police Scotland, automatic number plate recognition (ANPR) cameras and average speed cameras (ASC) operated on behalf of Transport Scotland by Traffic Scotland. Many of these systems can capture biometric data in the form of the facial images of citizens, with the potential for some of this data to be used for intelligence or evidential purposes. In addition, biometric data is also collected and retained with consent in various health and educational contexts.

15. The Scottish Government will take forward dialogue with COSLA, the Scottish Safety Camera Programme, Transport Scotland, Traffic Scotland and the health and education sectors with a view to enhancing public confidence and trust in the use of biometric data in other public sector contexts through the wider adoption of the general principles of this Code where appropriate.

Private sector/law enforcement interface – requirement to comply with Code of Practice

16. While not involved in direct regulation of private sector bodies, the Scottish Biometrics Commissioner should have oversight of their work on biometric data where it is done at the request of, or feeds into work by, Police Scotland, the SPA or any other body to whom this Code applies. In such cases, the relevant body (e.g. Police Scotland) should specify a requirement on the part of the private body to comply with relevant legislation and the General Principles of this Code of Practice. Contracts for biometric data handling systems should not be provided to private sector companies who do not agree to comply with this Code of Practice, particularly where private sector biometric identification

[2] In the case of arrests made in Scotland by other bodies such as PIRC or the National Crime Agency, the relevant biometric data capture will be authorised by arresting staff from the relevant body/agency and will thereafter be stored on the relevant Police Scotland and SPA biometric databases.

software uses algorithms that cannot be independently validated due to issues of commercial confidence.

17. More generally, it should be noted that 'Data Controllers' (organisations which decide why and how personal data is processed) are liable for their compliance with data protection legislation and must only appoint 'Data Processors' (third party service providers) who can provide sufficient guarantees that the requirements of such legislation will be met and the rights of people protected. The Information Commissioner's Office guidance on contracts and liabilities between controllers and processors states that in the future, using a processor which adheres to an approved code of conduct or certification scheme (such as this Code of Practice) may help controllers to satisfy this requirement.

18. This requirement may be relevant in areas such as policing, and in other areas such as the Scottish Government's Digital Strategy for Justice in Scotland, where a digital evidence sharing capability is being developed between criminal justice partners. Subject to successful prototyping, testing, and the securing of future funding, this presents opportunities to transform how evidence, including biometric data, is accessed across the justice system, allowing for more efficient sharing of evidence with consequential benefits which may accompany that development.

Part 2 – The Law, Human Rights and Data Protection

The Law - Biometrics in the criminal justice process

19. This Code of Practice will assist in ensuring that the legal framework surrounding the acquisition, retention, use and disposal of biometric data as part of the criminal justice process in Scotland is understood, and that the retention of biometric materials and data by Police Scotland, the SPA and other law enforcement authorities is both necessary and proportionate, and in accordance with the law. This Code of Practice also seeks to establish a framework of standards against which to measure the quality of systems and practices in an area where biometric data is collected from people, often without the usual safeguard of consent. It is proposed that the Scottish Biometrics Commissioner should maintain independent oversight of the retention of biometric data for justice and community safety purposes within the devolved competence of the Scottish Parliament, in part, by promoting compliance with this Code of Practice.

20. The Criminal Procedure (Scotland) Act 1995 ('the 1995 Act') is the primary Scottish legislation allowing the retention of fingerprints and other biometric samples from a person arrested by the police. Sections 18 to 19C stipulate the conditions under which samples may be taken by the police, as well as rules for retention and specification of the purposes of use of samples. It should also be noted that Section 18G permits biometric data to be retained for reserved matters, notably under national security determinations. The existing law may be summarised as follows:

- fingerprint and DNA data from convicted persons can be retained indefinitely. This legal entitlement applies on the basis of a single criminal conviction for any type of offence, regardless of gravity;

- data from children dealt with through the Children's Hearings System may be retained only where the grounds of referral are established (whether through

acceptance by the child at such a hearing or a finding in court) in relation to a prescribed sexual or violent offence. Such data can only be retained for three years unless the police apply for, and are granted, an extension by a Sheriff. For less serious offences, and where grounds are not established, there is no retention in relation to children;

- data from individuals who accept a Fiscal Offer may be retained for three years in relation to a prescribed sexual or violent offence, with the Chief Constable able to apply to the Sheriff Court for further two year extensions (there is no limit on the number of two year extensions that can be granted in respect of a particular person's data); and data may be retained for two years in relation to non-sexual or non-violent offences which are the subject of a Fiscal Offer or fixed penalty notice from the police;

- data from individuals prosecuted for certain sexual and violent offences may be retained for three years (whether or not they are convicted), with the Chief Constable able to apply to the Sheriff Court for further two-year extensions (there is no limit on the number of two-year extensions that can be granted in respect of a person's data); and

- subject to the exception just stated, data from individuals arrested for any offences (and who have no previous convictions) must be destroyed immediately if they are not convicted or if they are given an absolute discharge.

21. Section 83 of the Police, Public Order and Criminal Justice (Scotland) Act 2006 inserted Section 18A into the 1995 Act and contains provisions to allow retention of DNA samples and profiles of persons who have been arrested but not convicted of certain sexual or violent crimes. The list of relevant sexual and violent offences is in section 19A (6) of the Act, and Section 48 of the Crime and Punishment (Scotland) Act 1997.

22. In 2010, the Scottish Government also introduced sections 77 to 82 of the Criminal Justice and Licensing (Scotland) Act 2010 which included provisions to develop the law in relation to the retention and use of DNA, fingerprints and other physical data. This was done by amendment to the 1995 Act.

23. In addition to primary Scottish legislation, the Sexual Offences Act 2003 provides the law to support the registration of sex offenders, and the restrictions and obligations placed on them, including the provision for the capture of biometric data as part of offender management processes. The 2003 Act is supplemented by the Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005.

24. While the Scottish Government will conduct ongoing reviews of relevant primary legislation concerning the retention of biometric data, the foregoing sets out guidance in Scotland for the acquisition, retention, use and disposal of biometric data by Police Scotland, the SPA and other specified bodies.

The Law - Public Sector Equality Duty

25. To ensure compliance with this Code of Practice, Police Scotland, the SPA and other specified bodies should ensure that all standard operating procedures, policies and practices relevant to the acquisition, retention, use and disposal of biometric data have

undergone an Equality Impact Assessment to ensure that such policies and practices do not discriminate unlawfully.

26. Under the Equality Act 2010 (section 149 (Public sector Equality Duty)), police forces must, in carrying out their functions, have due regard to the need to eliminate unlawful discrimination, harassment, victimisation and any other conduct which is prohibited by that Act. This is to advance equality of opportunity between people who share a relevant protected characteristic and people who do not share it, and to foster good relations between those persons. The Equality Act also makes it unlawful for police officers to discriminate against, harass or victimise any person on the grounds of the protected characteristics of age, disability, gender reassignment, race, religion or belief, sex and sexual orientation, marriage and civil partnership, pregnancy and maternity when using their powers.

27. In addition, the Equality Act 2010 (Specific Duties) (Scotland) Regulations 2012 places a responsibility on listed authorities to assess and review all policies and practices to ensure that it complies with the equality duty in the exercise of its functions. The Chief Constable of Police Scotland and the SPA Board are relevant listed authorities.

The Law - Human Rights

28. The Human Rights Act 1998, which incorporates the European Convention on Human Rights (ECHR) into UK law, sets out the fundamental rights and freedoms that everyone in the UK is entitled to, and makes it unlawful for a public authority to act in a way which is incompatible with Convention rights. Consequently, any policy and legal framework for its use must be consistent with the human rights framework, and other guarantees laid down by relevant data protection laws. The use of personal data is sensitive and must be protected from abuse and arbitrariness.

29. Because biometric data retention is an interference with the right to privacy, the obvious approach is to have a presumption in favour of deletion following the expiry of any minimum retention period as prescribed in law. **This Code of Practice therefore establishes a presumption of deletion for biometric data (in circumstances where the subject has no previous convictions) following the expiry of the relevant retention periods as prescribed or permitted in law.** In deleting such data, Police Scotland, the SPA and other specified bodies must ensure that the biometric data records concerned are deleted not only from the primary database on which they are stored, but also from any secondary or tertiary databases onto which the data may have been replicated. This will be monitored by the Scottish Biometrics Commissioner.

30. To comply with this Code of Practice, bodies to whom the Code applies must ensure that the images of people arrested but not subsequently convicted (and who have no previous criminal convictions) are deleted from the National Custody System at the point when fingerprints, DNA and the corresponding Criminal History System (CHS) image are similarly expunged. In relation to custody images held by Police Scotland on legacy force custody systems where there is no automated means of distinguishing between records of convicted and non-convicted persons, it will suffice for the records within those systems to be protected from access in the operational environment until deleted as those systems are shut down. Subject to this caveat on historic images within legacy force systems, it is necessary to ensure that biometric data is completely expunged in circumstances where there are no longer legal grounds for retaining the data in question.

The Law – Data Protection

31. Data Protection legislation in the UK and throughout the wider EU provides a framework for the handling of personal data. In summary, personal data are data which relate to a living individual who can be identified from it directly or with other information which is in the possession of, or is likely to come into the possession of, the data controller (i.e. the organisation using the information). This includes biometric data.

32. The legal framework for all processing of personal data throughout the UK is contained within the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA18). The DPA18 and GDPR should be read side by side as interlinking legislation and form the basis of UK data protection laws.

33. The European data protection regime provides that general processing of personal data must be undertaken in compliance with the GDPR and processing for law enforcement purposes by designated or 'competent' authorities – i.e. named authorities with powers to investigate and/or prosecute crimes and impose sentences, together with certain other organisations – must conform with the Law Enforcement Directive as transposed into UK law via the DPA18.

34. The GDPR extends the data protection regime in several ways. It updates the definition of personal data to reflect scientific and technological advances which have taken place since the passing of Directive 95/46/EC; it provides several enhanced rights for data subjects; and it requires data controllers to strengthen their governance procedures in relation to personal data. Similar changes are seen within the law enforcement provisions of the DPA18.

35. GDPR is framed around several principles that require personal data to be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

36. The data protection regime requires that the controller shall be responsible for, and be able to demonstrate, compliance with the principles. Additionally, the law enforcement provisions of the DPA18 require that logs are kept of processing operations including collection, alteration, consultation, disclosure (including transfers), combination and erasure of personal data records within an automated processing system used for law

enforcement purposes. These logs can only be used to verify the lawfulness of processing, to assist with self-monitoring by the data controller (or processor, where relevant), to ensure the security and integrity of the data and, finally, for the purposes of criminal proceedings.

37. Biometric information is defined as a 'special category' of data within both the GDPR and DPA18. Any processing of biometric information must therefore be undertaken in compliance with either the GDPR or the DPA18 according to whether the processing is general processing or for law enforcement purposes. In this regard, biometric data are defined 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, fingerprints or DNA.

38. The processing of biometric data is only permitted in the GDPR where one of several conditions apply. These include consent, for the vital interests of the data subject where the subject is incapable of giving consent, for the establishment, exercise or defence of legal claims or if courts are acting in their judicial capacity and for reasons of public interest in the area of public health. However, the derogations granted to Member States allow extensions and / or exemptions to these conditions to apply under certain circumstances. Moreover, where a controller is a competent authority as defined in schedule 7 of the DPA18 and is processing for law enforcement purposes (the prevention, investigation, detection or prosecution of criminal offences), there are further restrictions on the conditions for processing which can be used. These are found within the Schedules of the DPA18.

39. To ensure compliance with this Code of Practice, the bodies to whom the Code applies must, in relation to the acquisition, retention, use and disposal of biometric data, comply with the provisions of the DPA18 and the GDPR. This includes a legal requirement to conduct Data Protection Impact Assessments (DPIAs) where the processing is likely to result in a high risk to the rights and freedoms of individuals. If the DPIA reveals high risks, and measures to reduce this risk cannot be taken, the Information Commissioner's Office must be consulted. Processing must not commence until the consultation has been completed.

Part 3 – 'General Principles' and ethical considerations

40. It is important to ensure a proper grasp of ethical, human rights and legal considerations at all stages of the biometric data process – acquisition, use, retention and disposal – given the highly sensitive and personal nature of the data involved. It is equally important to ensure that what is done is informed by considerations of what should be done, as opposed to merely considerations of what can be done. This is best achieved through the design and adoption of a set of overarching 'General Principles' which establish basic rules and procedures to be followed as part of a statutorily approved strategic decision making model.

41. Having some of these rules and procedures in a Code of Practice, which is itself kept under review, allows for the sort of flexibility which may be necessary in an area where advances in the relevant science and technology can occur quickly. It is crucial that such rules and their oversight mechanisms anticipate, or at least keep pace with, technological and other developments.

42. The adoption of high-level guiding principles is also desirable as a means of establishing an agreed framework for what is permissible and desirable in legal, human rights and ethical terms. Such a strategic approach also avoids being over-prescriptive, so as not to unintentionally stifle creativity and innovation in terms of new and emerging biometric technologies.

'General Principles' for the use of biometrics

43. The following 'General Principles' should be adopted to govern the use of biometric technologies and forensic procedures. Specifically, they require that permissible acquisition, use, retention and disposal of biometric data, in addition to being lawful, proportionate, and necessary, should:

- enhance public safety and the public good;
- advance the interests of justice;
- demonstrate respect for the human rights of individuals and groups;
- respect the dignity of all individuals;
- take particular account of the rights of children;
- take particular account of the rights of other vulnerable groups and individuals;
- protect the right to respect for private and family life;
- encourage scientific and technological developments to be harnessed to promote the swift exoneration of the innocent, afford protection and resolution for victims, and assist the criminal justice process; and
- be based on validated evidence.

44. These 'General Principles' form the basis of this Code of Practice and should be used by all bodies to whom the Code applies as part of internal self-assessment processes, procedures and governance mechanisms around the management of biometric and forensic data and their supporting technologies. These 'General Principles' also provide a framework against which compliance may be assessed by the Scottish Biometrics Commissioner.

Implementation of the 'General Principles'

45. The 'General Principles' should be implemented with due regard to the following:

- impartiality – procedures should be applied without bias or discrimination;
- proportionality – balancing individual rights, public safety and community wellbeing;
- effectiveness;
- openness and transparency;
- minimal intrusion needed to achieve outcome;
- the need for systems to be validated to show that they are fit for the specific purpose intended i.e. the results can be relied on irrespective of use (for example, intelligence or evidential purposes);
- the need for assurance in relation to the quality of the system;
- the need for public accountability;
- the need for independent oversight where appropriate;
- the need to provide adequate information and, where appropriate, to obtain consent from those from whom data or samples are sought or retained, or from some other appropriate individual where the individual cannot consent.

46. These important points of guidance in relation to how the 'General Principles' should be implemented are again intended to inform internal self-assessment processes, procedures and governance mechanisms around the management of biometric and forensic data and their supporting technologies. They also provide additional important governance criteria against which compliance may be assessed by the Scottish Biometrics Commissioner.

Considerations regarding the collection and processing of biometric data

47. In relation specifically to the collection and processing of data, the 'General Principles' should be applied as follows:

- data should be collected, stored, used and retained only for specified and lawful purposes;
- data collection, storage, and use must adhere to legal requirements;
- steps should be taken to ensure the accuracy, security and integrity of data collected, stored and used;
- steps should be taken to ensure transparency around error rates and uncertainties inherent in procedures;
- processes should be robust and conform to any relevant standards and be applied by professionally trained staff whose work can be audited;
- intrusion into private lives should be minimised – this may be of particular significance in relation to issues of data linkage;
- account should be taken of the interests of secondary data subjects (i.e. people potentially affected by data collected from others, e.g. family members); and
- policies should be in place around the weeding and disposal of these data, including a presumption in favour of deletion when the legal period for retention has expired or when the data is no longer required in connection with the purposes for which it was collected.

48. These considerations specific to the collection and processing of biometric data are again intended to offer guidance on the internal and external governance mechanisms that are necessary in order to ensure sensitive data is handled lawfully and appropriately by professionally trained staff, and to clear and established data protection, security, quality and audit standards. These considerations provide further governance criteria against which compliance may be assessed by the Scottish Biometrics Commissioner.

Validation and reliability of techniques

49. To comply with the 'General Principles' set out above it is important that the effectiveness and reliability of any biometric technologies is established by those who use them. The key issue is that all technologies should be fit for purpose i.e. capable of achieving the outcome that they are designed to achieve. One means of establishing fitness for purpose is formal validation. This assists with demonstrating the integrity and value of the underlying technology.

50. Validation is the process of providing objective evidence that a method, process or device is fit for the specific purpose intended. It involves demonstrating that a method used for any form of analysis is fit for the specific purpose intended i.e. the results can be relied on.

51. This Code of Practice therefore requires that bodies to whom the Code applies should have internal validation systems, processes and procedures in place in respect of each biometric technology or technique that they operate as part of internal governance regimes. Such validation mechanisms would be kept under review by the Scottish Biometrics Commissioner.

Part 4 – Privacy by design

Data Protection Impact Assessments (DPIA's)

52. A DPIA (previously known as a Privacy Impact Assessment or PIA) is a tool that can help identify the most effective way to comply with data protection obligations whilst meeting individuals' expectations of privacy. An effective DPIA will allow you to identify and fix problems at an early stage, reducing the associated costs and damage to your reputation which might otherwise occur.

53. A DPIA must be undertaken before personal data is processed when the processing is likely to result in a high risk to the rights and freedoms of individuals. Such processing includes (but is not limited to):

- systematic and extensive processing activities, including profiling and where decisions have legal effects, or similarly significant effects, on individuals;
- large scale processing of special categories of data or personal data in relation to criminal convictions or offences; and
- using new technologies (for example surveillance systems).

54. The nature, scope, context and purposes of the processing should be taken into account when deciding whether or not it is likely to result in a high risk to individuals' rights and freedoms.

55. The core principles of DPIA can be applied to any project which involves the use of personal data, or to any other activity which could have an impact on the privacy of individuals. A DPIA is suitable for a variety of situations:

- a new IT system for storing and accessing personal data;
- a data sharing initiative where two or more organisations seek to pool or link sets of personal data;
- a proposal to identify people in a particular group or demographic and initiate a course of action;
- using existing data for a new and unexpected or more intrusive purpose.
- a new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding automatic number plate recognition capabilities to existing CCTV);

- a new database which consolidates information held by separate parts of an organisation; and

- legislation, policy or strategies which will impact on privacy through the collection and use of information, or through surveillance or other monitoring.

56. Bodies to whom the Code applies are likely to be required to conduct DPIAs as part of a privacy by design approach for many of their processing activities as the GDPR and DPA18 require them to be undertaken where the processing is likely to result in a high risk to the rights and freedoms of individuals. As stated in para 39, if the DPIA reveals high risks, and measures to reduce those risks cannot be taken, the ICO must be consulted. Processing must not commence until the consultation has been completed. Such DPIAs will be kept under review on a regular basis by the Scottish Biometrics Commissioner.

Part 5 – Information to be provided to people

57. It is important that the public are provided with clear, jargon free information to help them understand the powers that bodies have, the rights they (the public) have to hold those bodies to account, and how to exercise those rights.

Information to be provided in the criminal justice process

58. As mentioned earlier in this Code of Practice, the Criminal Procedure (Scotland) Act 1995 ('the 1995 Act') is the primary Scottish legislation allowing the retention of fingerprints and other biometric samples from a person arrested by the police. In practice, the most common forms of biometric data captured from adults arrested and charged by the police are fingerprints, photographs and DNA. When a person is arrested by the police, they are informed of their rights whilst in custody and persons who are subsequently charged with qualifying crimes and offences because of their arrest are advised of the legal requirement on them to provide biometric samples as part of the criminal justice process.

59. The GDPR and the DPA18 require individuals to be informed about the collection and use of their personal data. They normally should be provided with details of the purposes for which their personal data is being processed, the retention periods for that personal data, and with whom it will be shared. The information must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language. However, exemptions apply, and the provision of information may be restricted where it is necessary and proportionate to do so, for example, where providing it would prejudice the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties. Any decisions to rely on any restriction must be recorded and provided to the Information Commissioner, if required.

Biometrics information sheet for prisoners

60. In a policing context, the most practical way of ensuring that all the necessary information is properly communicated to persons about to enter the criminal justice process is through the introduction of a 'biometrics information sheet' or leaflet provided to persons who have their biometric data captured because of a custody episode.

61. To ensure compliance with this Code of Practice, bodies to whom the Code applies must introduce a biometrics information sheet, or other means of informing persons whose biometric data is captured as part of the criminal justice process. The sheet should describe the powers that the authorities have in relation to the acquisition, use, retention and disposal of biometric data, including information on how such data might be used and shared, and the powers that members of the public have to appeal against any decision to retain their data.

Part 6 – Biometric data review and appeals process

62. An appeal is the process through which cases are reviewed, where parties request a formal change to an official decision. Appeals therefore function both as a process for error correction and for clarifying practice and interpreting law.

63. In circumstances where biometric data is captured or retained without consent, it is important that there is a clearly understood appeals process. Such an appeals process is required for situations where biometric data has been captured overtly under criminal procedure legislation, and for situations where such data may have been captured less overtly through for example public space CCTV surveillance cameras.

Appeal to public body holding data

64. For these reasons, bodies to whom this Code applies should have a published appeals process concerning the acquisition, use and retention of biometric data. The process should enable individuals to appeal initially for review by the public body holding the data concerned. There should be no fee payable where persons challenge the retention of their personal data, and no fee payable if the body agrees to delete that data.

Review requests to Scottish Biometrics Commissioner

65. If a person is not satisfied with the outcome of such an appeal to the public body concerned then a request can be made to the relevant regulator requesting an independent review of that decision.

66. For the sake of clarity, the role of the Scottish Biometrics Commissioner is not to regulate data protection matters within the remit of the Information Commissioner.

67. In line with its statutory remit, UK Information Commissioner will continue to consider concerns raised by members of the public regarding the accessing or handling of their personal information by Police Scotland, the SPA and those other individuals exercising powers of arrest in Scotland for devolved purposes.

68. Should the Information Commissioner, in the course of considering an individual case, identify the potential for systemic learning and improvement in relation to the use of biometric data for justice and community safety purposes in Scotland, details may be shared with the Scottish Biometrics Commissioner. It would then be open to the Scottish Biometrics Commissioner to consider whether a specific review was required

69. The Scottish Biometrics Commissioner would have a statutory power to require specific information from specified bodies to aid them in undertaking a review. The information would pertain to the taking of biometric data as opposed to the data itself. The Scottish Biometric Commissioner would publish their findings in a manner that protects the identity of any appellant. Whilst there would be no formal recourse in respect of the individual, it would be open to the Scottish Biometric Commissioner to issue an improvement notice should they identify a systemic breach of Codes of Practice.

Part 7 – Children and vulnerable adults and groups

Children in the criminal justice system

70. The numbers of children entering the criminal justice system in Scotland is small by comparison to adults. Scottish Government data shows around 2,200 criminal proceedings being initiated against persons aged between 12 and under 18 in 2017, the vast majority of whom were aged 16 or 17. Consequently, biometric data are rarely captured from younger children, and they are likely to be taken from those in their mid-teenage years only in circumstances where the gravity of their offending or other circumstances are likely to result in criminal proceedings.

71. It is recognised that biometric data are not required in every case involving a child. In some areas of policing, decisions are based on individualised risk assessment and that is what is expected in relation to the acquisition, retention, use and disposal of biometric data as it relates to children. This provides reasonable justification for taking an appropriately distinct approach to the capture of their biometric data.

72. For children under 12 who, under the Age of Criminal Responsibility (Scotland) Bill, will no longer be capable of being held criminally responsible, biometrics will not be obtained except where they are needed for the investigation of a very serious incident. The capture or use of biometrics will have to be authorised by a Sheriff and biometric data taken from children under 12 will have to be destroyed as soon as they are no longer needed for the specific investigation and any ensuing Children's Hearing proceedings. These data will not be placed on the Police Scotland Criminal History System (CHS) or the UK Police National Database (PND).

73. For children aged 12 to 17 years, in each case, consideration should be given by the relevant officer as to whether it is proportionate and necessary to obtain biometric data, with the best interests of the child specifically considered in the decision-making process. In doing this, consideration should also be given to the wider context of the child's offending behaviour, including their previous offences, their likelihood of reoffending and the nature and seriousness of their offending behaviour. Where the decision is to obtain and retain biometric data, the relevant officer should record the reasons. These reasons should be subject to review and scrutiny within a reasonable time frame, both internally by supervising officers and by the Scottish Biometrics Commissioner.

74. This approach is consistent with the Scottish Government's 'Getting it Right for Every Child' approach and the 'Whole System Approach' for young people who offend. This forms the current ethos of Scottish youth justice policy and is therefore similarly advocated by this Code of Practice.

Vulnerable adults and groups in the criminal justice system

Vulnerable adults

75. It is essential that appropriate consideration should be given, and adaptation made, in the treatment of adults with specific vulnerabilities and especially where issues of consent arise. Legislation exists in Scotland to ensure that vulnerable adults are protected from harm. The Adults with Incapacity (Scotland) Act 2000, provides the means to protect those with incapacity through guardianship, while the Mental Health (Care and Treatment) (Scotland) Act 2003 provides powers and duties in relation to people with mental disorder.

76. The bodies to whom this Code applies must ensure that all officers and staff are fully aware of their own individual roles and responsibilities in relation to protecting vulnerable adults, including from discrimination.

Protected characteristic groups

77. As covered in paragraph 26, the Equality Act 2010 (Specific Duties) (Scotland) Regulations 2012 places a responsibility on listed authorities to assess and review all policies and practices to ensure that it complies with the equality duty in the exercise of its functions. This is the mechanism through which listed authorities should ensure that there is no unlawful discrimination and, in terms of this Code of Practice, such authorities must ensure that there is no unlawful discrimination in policies, procedures and practices involving the acquisition, use, retention or disposal of biometric data.

Part 8 – Compliance with the Code of Practice

78. This Code outlines the responsibilities of those to whom this Code will apply and contains a set of 'General Principles' to be followed. Those 'General Principles' embody wider legal, ethical, human rights, and data protection considerations, including special considerations to be made in respect of children, vulnerable adults and protected characteristic groups. The Code also provides an ethical and human rights based framework within which new biometric technologies may safely emerge.

79. This Code of Practice will initially apply to Police Scotland and the SPA. The Chief Constable of Police Scotland and the Board of the SPA will ensure that internal systems and processes are in place to ensure compliance with all aspects of the Code.

80. This Code will also apply to biometric data use for any other policing and law enforcement purpose subject to the competence of the Scottish Parliament. Specifically, this will include any other related public or law enforcement bodies who may collect biometric data whilst exercising powers of arrest for devolved purposes, including the exercise of any of the powers and privileges of a Constable when investigating a matter under the direction of the Crown Office and Procurator Fiscal Service[3]. The Code does not extend to the retention of biometric data for the purposes of UK national security. Responsibility for these matters falls within the statutory remit of the Office of the Biometrics Commissioner for England and Wales. Similarly, this Code does not extend to data protection laws within the statutory remit of the UK Information Commissioner.

[3] In the case of arrests made in Scotland by other bodies such as PIRC or the National Crime Agency, the relevant biometric data capture will be authorised by arresting staff from the relevant body/agency and will thereafter be stored on the relevant Police Scotland and SPA biometric databases.

81. Any other bodies who adopt the Code on a voluntary basis should ensure that the collection of biometric data is lawful, proportionate and necessary and as a minimum, ensure that they comply with the General Principles of this Code of Practice outlined in paragraph 42.

Oversight by the Commissioner

82. For bodies to whom this Code applies, compliance will be promoted by the Scottish Biometrics Commissioner. If necessary, the Scottish Biometrics Commissioner can serve an improvement notice on such a body where a review identifies evidence of a systemic failure to comply. As the Commissioner will report on the outcomes of reviews to the Scottish Parliament, there is an expectation that bodies will act on the advice of the Commissioner.

83. The primary purpose of this Code of Practice is to promote good practice. Nothing in this Code of Practice alters or otherwise affects any statute which makes express provision as to the acquisition, use, retention or disposal of biometric data for justice and community safety purposes in Scotland. Similarly, nothing in this Code of Practice alters or otherwise affects any existing rule of law or legal test about the admissibility of evidence with regards to any form of biometric data.

Breaches of the Code of Practice

84. Breaches of the Code of Practice by bodies to whom this Code applies on a statutory basis do not constitute a civil or criminal offence. Breaches of the Code will not be conclusive for the purposes of legal admissibility but can be considered by the Court in determining admissibility. However, the Scottish Biometrics Commissioner will have the power to serve an improvement notice on any body to whom this Code applies on a statutory basis where there are systemic breaches of the Code, and details of such will be included in the Commissioner's annual report to the Scottish Parliament.

Glossary of Terms

ANPR	Automated Number Plate Recognition
ASC	Average Speed Camera
CCTV	Closed Circuit Television
CHS	Criminal History System (Police Scotland)
COPFS	Crown Office and Procurator Fiscal Service
COSLA	Convention of Scottish Local Authorities
DNA	Deoxyribonucleic Acid
DPA18	Data Protection Act 2018
DPIA	Data Protection Impact Assessment
EIA	Equality Impact Assessment
EU	European Union
GDPR	General Data Protection Regulation
IAG	Independent Advisory Group on Biometric Data in Scotland
ICO	Information Commissioners Office
LED	Law Enforcement Directive
PIA	Privacy Impact Assessment
PND	Police National Database
SOP	Standard Operating Procedure (Police Scotland)
SPA	Scottish Police Authority