## Annex F: Legislation summaries

The information that follows is taken from a high level analysis of current legislation and policy in relation to biometric data for immigration and law enforcement purposes, focussing upon the use and retention of data.

In Scope

- Analysis of UK legislation and accompanying guidelines

Out of Scope

- Analysis of potential upcoming policy changes
- Analysis of local practices
- Analysis of technical standards and guidance, e.g. ISO, ANSI/NIST

The analysis was first completed in April 2016 and has been reviewed for any changes in August 2017

## Data Legislation

**HOB made a commitment under the Data Protection Act 1998 to undertake a programme PIA, consisting of a suite of individual PIAs for each project as well as an overarching programme level PIA. The documents published on GOV.UK are those that have been completed and approved under the DPA 1998.**

**Now that the Data Protection Act 2018 has come into force, the HOB Programme PIA and existing project PIAs will be reviewed on a rolling schedule against the new data protection principles. Any new developments and projects will be assessed using the DPIA template.**

**This Annex currently only includes a section on DPA 1998 to cover the published PIA documents. It will be updated and republished with a DPA 2018 section.**

**Data Protection Act 1998**[1]

This act defines personal data as data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

The act identifies eight principles of data protection which cover areas such as requiring that personal data be obtained for specified purposes and not kept longer than necessary.

- Principle 1: Fair and lawful processing of personal data
- Principle 2: Personal data obtained is for limited purposes and not further processed for incompatible purposes
- Principle 3: Personal data shall be adequate, relevant and not excessive for the purpose
- Principle 4: Personal data shall be accurate and kept up to date
- Principle 5: Personal data shall not be kept for longer than necessary
- Principle 6: Personal data is processed in line with rights under the DPA
- Principle 7: Measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
- Principle 8: Personal data is not transferred to countries without adequate protection for the rights and freedoms of data subjects in relation to the processing of personal data

In addition, the act gives individuals rights of access to personal data (upon submitting a written request) which includes: an entitlement to being informed if the data is processed; provided with description of the data; and provided with both the

[1] The current PIAs have been completed within the principles of the Data Protection 1998 and using the Home Office template that covers this legislation. Under the new data protection regime HOB will be completing a DPIA for its projects, refreshing any existing PIAs against the new legislation

data and information about its source. There are wide exemptions for national security and lesser exemptions for fighting crime.

### Freedom of Information Act 2000

This act covers some of the same ground as the Data Protection Act in that it describes the right of individuals to request and be informed of any information held about them by public authorities. It lists several organisations that are exempt, including the security services and SOCA. It also lists a few situations where exemptions apply such as law enforcement and investigations.

## Immigration

### Immigration Act 1971

The Immigration Act 1971 is the earliest legislation setting out the power to take fingerprints for immigration purposes.

Paragraph 18(2) and (2A) of Schedule 2 establishes the power for any immigration officer, constable, prison officer or any other person authorised by the Secretary of State to take all such steps as may be reasonably necessary for photographing, measuring or otherwise identifying a detained person who is liable to examination or removal (defined in section 16). This identification may be required for the purpose of ascertaining the person's citizenship or nationality or making arrangements for their admission to another country or territory other than the UK.

This includes the power to take fingerprints. This is a verification power only, and hence, once the person has been identified, the fingerprints must be destroyed.

Section 1(1) exempts persons who have the right of abode in the UK from immigration control including the taking of biometrics, providing they can prove they

have the right of abode. This means that they do not need to obtain the permission of an immigration officer to enter the UK, and may live and work without restriction.

Hence fingerprints cannot lawfully be taken under this power if a valid passport proving right of abode is presented. If identification is presented after the taking of fingerprints, the fingerprints must be destroyed. The right of abode is defined in section 2 (1) as those with British or Commonwealth citizenship.

Under paragraph 4(5) of Schedule 2, an immigration officer examining a person who presents a biometric passport or document may require the person being examined to provide information about their external physical characteristics, which may include fingerprints or features of the iris. This is not a free-ranging power to take biometrics and may only be used to ascertain whether the passport/document relates to the person being examined (including British/EEA citizens), if the validity is in question. Biometrics may be checked against the IABS database but this does not mean that provision of biometric information is a requirement for entering the UK. This is a verification power only, and hence, once the person has been identified, the fingerprints must be destroyed.

**Immigration and Asylum Act 1999**

Section 141 of the Immigration and Asylum Act 1999, which came into force on 11 December 2000, gives power to Immigration officers (IOs) at ports, officials in the Asylum Screening Units (ASUs) and at Application Registration Card (ARC) Event Centres, police constables, prison officers and persons employed by removal centre contractors to take fingerprints in immigration cases under certain circumstances:

- Any person who fails to produce a valid passport with photograph or some other document, satisfactorily establishing their identity and nationality and citizenship, when required to do so by a Border Force officer, on their arrival in the UK
- Any person who has been refused leave to enter the UK but granted temporary admission under paragraph 21 of Schedule 2 to the Immigration Act 1971, if a Border Force officer reasonably suspects they might break any

condition imposed on them relating to residence as to reporting to the police or a Border Force officer

- Any person in respect of whom a relevant immigration decision has been made. Information on what constitutes a 'relevant immigration decision' can be found in section 82(2) of the Nationality, Immigration and Asylum Act 2002 and chapter 24 of the enforcement instructions and guidance
- An individual who has been arrested under paragraph 17 of Schedule 2 to the Immigration Act 1971
- An individual who has made a claim for asylum. Note that all asylum applicants can be required to have their fingerprints taken, from the point of claim until the applicant (if refused) has exhausted all rights of appeal or has abandoned the claim. There may be other circumstances in which the fingerprints can be taken after this time (depending on how the applicant entered the UK). For practical reasons fingerprints should be taken as early in the process as possible
- An individual who is the dependant of someone who falls into one of the above categories. Note that children (defined as under sixteen years of age) must be fingerprinted in the presence of a responsible adult, who cannot be a person authorised to take fingerprints. Children under five years of age do not need to be fingerprinted

The expectation is that fingerprints should be taken from all those in the above categories. Section 146 (1) allows an immigration officer to use reasonable force to take fingerprints from persons in the above categories. If a claimant or dependent continues to obstruct the taking of their fingerprints, this should be taken into account in the reasons for refusal letter. An asylum claimant should not be issued with an ARC or SAL. Section 142 (3) provide powers of arrest without warrant for a person who is required to provide their fingerprints and fails to do so.

Section 143 (1) (amended by the Anti-Terrorism, Crime and Security Act 2001) establishes the retention periods for fingerprints taken under section 141. The

Secretary of State may specify a retention period; if no period is specified, then it defaults to 10 years from the day on which fingerprints were taken. At that point all fingerprints stored on the IABS system will be automatically deleted. Physical and electronic fingerprints must be securely destroyed after the 10 year period.

However, if the individual proves to be an EEA/British/Commonwealth citizen with right of abode, the fingerprints must be destroyed as soon as reasonably possible.

Under the Data Protection Act 1998[2], claimants can obtain copies of their fingerprints by making a subject access request under section 7 of the Act. All subject access requests should be referred to the Subject Access Bureau. Claimants may request confirmation that computer data which relates to their fingerprints has been destroyed, erased or blocked as required under section 143 of the 1999 Act. When such a request is received, a certificate must be issued within 3 months of the request date.

**Asylum and Immigration (Treatment of Claimants, etc.) Act 2004**

Section 35 establishes the power for the Secretary of State to require a person to provide their fingerprints if they are subject to a deportation or removal decision or if the action may enable a travel document to be obtained by or for the person, which would facilitate the person's removal from the UK, in order to enable determination of an application.

An Application Registration Card (ARC) or a Standard Acknowledgement Letter (SAL) will not be issued if a claimant refuses to be fingerprinted or fails to attend for fingerprinting. If a claimant refuses to be fingerprinted this may also be taken into account in the reasons for refusal letter as a credibility issue. There is a general requirement under section 8 (1) of the Asylum and Immigration (Treatment of Claimants, etc) Act 2004 for the Home Office to take into account as damaging to the

[2] Now replaced by the Data Protection Act 2018

claimant's credibility any behaviour that is designed or likely to conceal information or obstruct or delay the handling or resolution of the claim. However, claims must not be refused solely on the basis that the applicant refused or failed to attend for fingerprinting; the claimant's substantive claim should also be considered.

Note that this does not include the power to use reasonable force to take a person's biometrics.

**Nationality, Immigration and Asylum Act 2002**

Section 126 of the Nationality, Immigration and Asylum Act 2002 (the 2002 Act) establishes the power for the Secretary of State to make regulations requiring a person making an application for entry clearance, leave to enter or remain in the UK or variation of leave to enter or remain in the UK to provide their biometrics. For the purpose of this legislation, biometrics is defined as 'information about a person's external physical characteristics', in particular, fingerprints and features of the iris and other parts of the eye. However, no data regarding features of the eye is currently collected.

The secondary legislation established under this Act is the Immigration (Provision of Physical Data) Regulations 2006, as amended, which enable authorised persons to require an individual to provide fingerprints and a photograph of their face. If required, the individual must attend a particular location to have their fingerprints and photo taken.

Safeguards remain in place for children under sixteen (under section 141 of the 1999 Act), who must be fingerprinted in the presence of a responsible adult, who is not a person authorised to take fingerprints.

Fingerprints obtained under Regulations made under 2002 Act may normally only be retained for up to ten years, except where specified (regardless of the outcome of the application). Where a person is considered to be a risk of high-harm to the UK or where the person has unclasped permanent status in the UK, their fingerprints can be retained for longer. If the person who provided fingerprints proves to be a

British/EEA/Commonwealth citizen with right of abode, then their fingerprints should be destroyed as soon as reasonably practicable. Facial images obtained under these powers may be retained until the person becomes a British citizen and obtains a British passport.

Section 126 (4) (g) has been superseded by Section 8 of the UK Borders Act 2007, which provides powers to make regulations about use and retention of biometric information. Provision was made in 2015 in the Immigration (Provision of Physical Data) (Amendment) Regulations 2015.

Section 127 of the Nationality, Immigration and Asylum Act 2002 allows the Secretary of State to operate a voluntary scheme under which an individual may provide their biometrics to be used wholly or partially in connection with entry to the UK. Individuals may be charged for participation in this scheme but would benefit from faster entry into the UK. The Secretary of State may require an authorised person to use information supplied under such a scheme, and make provision about the collection, use and retention of information supplied under such a scheme (eg. that authorised persons must comply with a code of practice).

**The Immigration (Provision of Physical Data Regulations) 2006**

The Immigration (Provision of Physical Data) (Amendment) Regulations 2015 is secondary legislation made under the Nationality, Immigration and Asylum Act 2002. It amends the Immigration (Provision of Physical Data Regulations) 2006, which introduced a requirement for persons who are required to apply for entry clearance prior to coming to the UK, to provide their biometric information. This is applicable for persons who have applied for entry clearance or where a person seeking leave to enter presents a Convention travel document endorsed with an entry clearance.

The 2015 regulations add the requirement for persons applying for transit visas and for non-EEA family members of EEA nationals applying for family permits or residence cards under the section 2 (2) of the European Communities Act 1972.

Biometric information provided in accordance with these Regulations may be retained only if the Secretary of State thinks that it is necessary to retain it for use in connection with:

- The exercise of a function by virtue of the Immigration Acts
- The exercise of a function in relation to nationality
- In connection with the prevention, investigation or prosecution of an offence
- For a purpose which appears to the Secretary of State to be required in order to protect national security
- In connection with identifying persons who have died, or are suffering from illness or injury
- For the purpose of ascertaining whether a person has acted unlawfully, or has obtained or sought anything to which the person is not legally entitled
- In connection with the exercise of a function concerning the entitlement of a person who is not a national of an EEA state or Switzerland to enter or remain in the United Kingdom by virtue of an enforceable EU right or of any provision made under section 2(2) of the European Communities Act 1972

Retention of biometric data obtained under these regulations is as set out under the 2002 Act, as amended.

**UK Borders Act 2007**

Sections 5 to 15 of the UK Borders Act 2007 establish the power to collect biometric information including fingerprints and facial images from foreign nationals subject to immigration control, who are required to apply for biometric immigration documents. This is relevant for both persons who apply for leave to remain in the country (the card provides written confirmation as required by section 4 of the Immigration Act 1971), and for those who have already been granted leave to remain (they will in time be required to upgrade their current immigration status documents to the secure biometric immigration documents). Holders of biometric immigration documents are required to produce the document when they make an application for leave to remain

and when examined by immigration officers either during the course of their journey to the UK, or at port. Note that this is not a freestanding power to take biometrics, which may only be taken when the person applies for an immigration product.

It establishes the framework for issuing secure biometric immigration documents and provides the Secretary of State with the power to make regulations to create the scheme for issuing the biometric document.

The 2007 Act also establishes the power to create a sanctions scheme for those failing to comply with a requirement of the regulations, for example, a failure to apply for the secure biometric card or to provide their biometrics. Sanctions may include refusal of application for leave, curtailment or cancellation of leave, or the imposition of a civil penalty.

Biometric information on documents may be used for specified immigration purposes, in connection with specified immigration procedures, or in specified circumstances, where a question arises about a person's status in relation to nationality or immigration. The act also states that regulations must be established to further set out how information may permissibly be used, which may include use for non-immigration purposes, for example, the prevention, investigation and prosecution of crime. Regulations may also require a person to produce a card in certain specific circumstances or to provide information to verify that they are the rightful holder. If the holder is asked to provide fingerprints or a photograph to verify that these match those provided upon application, the information can be checked against the card and the IABS database, but must not be retained.

Regulations must also be established to set out a framework for the destruction of biometric information in certain circumstances. The powers to retain and use biometrics are the same as section 126(8A) of the 2002 Act. If an individual is found to have right of abode, their biometric information must be destroyed as soon as reasonably practical. There regulations are set out in the Immigration (Biometric Registration) Regulations 2008 as amended, which sets out specific circumstances for retaining biometric information and establishes the framework for sanctions including civil penalties via the Immigration (Biometric Registration) (Civil Penalty Code of Practice) Order 2008, as amended.

**The Immigration (Biometric Registration) Regulations 2008, as amended**

The Immigration (Biometric Registration) Regulations 2008 is secondary legislation made under the powers established by the UK Borders Act 2007, and requires anyone who is subject to immigration control and applying for leave exceeding 6 months to apply for a biometric immigration document, which is commonly known as a biometric residence permit (BRP). This includes those applying for leave to enter or remain in the UK, those making claims for asylum, and those applying for replacement immigration documents. It also includes those applying for limited leave to remain in the UK under certain categories, including as a student, prospective student, student nurse, sabbatical officer or the spouse, civil partner, unmarried or same sex partner of a person present and settled in the UK. During the process of application for a biometric residence permit, an authorised person may require the applicant to provide a record of their fingerprints or photograph of their face.

The regulations allow the Secretary of State to:

- Define the process including taking of biometrics
- Set out how children aged under 16 should be treated
- Set out when a BRP is to be surrendered or cancelled
- Set out obligations on the holder of the BRP to notify the SoS in specified circumstances
- Set out when the biometric information may be used and retained by the SoS
- Require biometrics to be destroyed when a person becomes a British citizen
- Set out when the holder of the BRP must produce it and submit to a biometric check against the card
- Set out consequences for non-compliance with the regulations

The regulations also cover sanctions for non-compliance with the regulations. These may include:

- Refusal to issue a BRP
- Imposition of a civil penalty of up to £1,000
- Refusal or rejection of an application for leave

- Alteration or cancellation of existing leave

Regulation 7 establishes safeguards for children under sixteen (as per section 141 of the 1999 Act), who must be fingerprinted in the presence of a responsible adult, who is not a member of the Home Office (Borders and Immigration) or a person authorised to take fingerprints.

Regulation 9 provides that the Secretary of State may use a record of a person's fingerprints or a photograph of a person's face in accordance with the following purposes:

- In connection with the exercise of a function by virtue of the Immigration Acts
- In connection with the control of the United Kingdom's borders
- In connection with the exercise of a function related to nationality
- In connection with the prevention, investigation, or prosecution of an offence
- For a purpose which appears to the Secretary of State to be required in order to protect national security
- In connection with identifying victims of an event or situation which has caused loss of human life or human illness or injury
- For the purpose of ascertaining whether any person has failed to comply with the law or has gained, or sought to gain, a benefit or service, or has asserted an entitlement, to which he is not by law entitled

Fingerprints and photographs may be retained if the Secretary of State believes that they are required for the purposes above; otherwise they should be destroyed as soon as possible. There is no blanket timeframe for destruction of biometric data.

If biometric data is to be destroyed, the Secretary of State must take all reasonably practicable steps to ensure that data held in an electronic form which relate to any record of fingerprints or photograph which is due to be destroyed are either destroyed, erased or inaccessible. The person to whom the data relate is entitled, on written request, to a certificate issued by the Secretary of State confirming that this is the case, and this must be issued within three months of the request being received.

**The Immigration (Biometric Registration) (Civil Penalty Code of Practice) Order 2008, as amended**

The Immigration (Biometric Registration) (Civil Penalty Code of Practice) Order 2008 is a code of practice made under the powers established by the UK Border Act 2007 and establishes sanctions for non-compliance with the biometric registration regulations.

These include:

- A refusal to issue a Biometric Immigration Document (BID)
- An immigration sanction, that is:
    - The refusal or rejection as invalid of a person's application for leave to enter or remain in the UK
    - The cancellation or variation by curtailment of a person's existing leave to enter or remain in the UK
- A financial sanction in the form of a civil penalty notice

**Immigration, Asylum and Nationality Act 2006**

The Immigration, Asylum and Nationality Act 2006 enhanced existing fingerprint provisions under paragraph 16 of Schedule 2 to the 1971 Immigration and Nationality Act (covered in section on the 1971 Act).

If claimants and/or their dependents are required to attend a specified place to be fingerprinted, they must be given at least 3 days' notice. This notice period does not apply when a claim for asylum is made, and those authorised to do so take the claimant's fingerprints on the day.

**Borders, Citizenship and Immigration Act 2009**

Section 51 of the Borders, Citizenship and Immigration Act 2009 amended section 141 of the Immigration and Asylum Act 1999 to allow fingerprints to be taken from a

person who is a foreign criminal within the meaning of section 32 of the UK Borders Act 2007 and in respect of whom a decision is taken that the automatic deportation provisions in that act apply.

Section 146(1) allows the use of reasonable force in the exercise of these powers and powers to require a person to attend to provide their fingerprints. Section 142 (3) establishes powers of arrest if a person is required to attend but fails to do so.

Section 143(1) establishes retention periods for fingerprint data, which must be destroyed before the end of period specified by the Secretary of State, beginning with the day on which they were taken. If no period is specified by the Secretary of State, the retention period defaults to 10 years from the day on which they were taken.

**Immigration Act 2014**

This Act was partly intended to enable the Secretary of State to update and align the powers to use and retain biometric taken for immigration purposes.

Sections 8 to 14 of the Act cover biometric information, expanding powers to collect biometric information and increasing the scope of embarkation checks. Prior to the Immigration Act 2014, immigration officers were only able to take the fingerprints of persons suspected of being removable from the UK if they had been arrested, or provided consent. The act enables immigration officers to conduct biometric checks on suspected immigration offenders without consent. Fingerprints taken under this power are used for verification purposes only and may not be retained if the person proves to be lawfully resident in the UK.

Section 8 amends section 126 of the Nationality, Immigration and Asylum Act 2002 to require foreign nationals to provide biometrics when applying for transit visas. This also applies to non-EEA family members of EEA nationals applying for family permits or residence cards.

Section 9 amends paragraph 18(2) of Schedule 2 to the Immigration Act 1971, allowing immigration officers to take the fingerprints of persons who are suspected of being immigration offenders and hence liable to be detained.

Section 10 amends Section 41 of the British Nationality Act 1981 to require persons applying to become British citizens to provide biometric information as part of their application, in order to verify that they are the same person who was previously granted leave to remain. If British citizenship is granted, the fingerprint record should be deleted, and the photograph should be deleted once a British passport has been issued.

Section 13 updates the safeguards for children, ensuring that children under 16 are not required to provide biometric information unless authorisation is obtained from a Chief Immigration Officer and a parent/guardian is present when information is provided

Section 14 enables the Secretary of State to update and align the provisions about the use and retention of biometric information provided, which must state that biometric information is only retained if necessary to retain it for immigration nationality purposes, and for specific non-immigration purposes including the prevention of crime and the protection of national security. The regulations must include provision for the destruction of biometric information where it is no longer necessary to retain the information, and allow an individual whose biometric information has been destroyed to request confirmation of this.

## Summary of retention periods and permitted uses

| Situation | Legislation | Modes | Retention Period | Permitted Uses |
|---|---|---|---|---|
| Persons who have made claim for asylum, failed to produce valid travel documents, persons for whom a relevant immigration decision has been made, persons arrested under Schedule 2 of the Immigration Act 1971 | S143 (1) of the Immigration and Asylum Act 1999, amended by the Anti-Terrorism, Crime and Security Act 2001 | Fingerprints | A period specified by the Secretary of State, or ten years if no period specified. If the person proves to have right of abode in the UK, the fingerprints should be destroyed as soon as reasonably practicable | Purpose unspecified but the intention is to take and keep prints of certain categories of people who present a high risk to immigration control; searches may be performed to identify if an individual is already known to immigration control |
| Persons subject to a deportation or removal decision or if the action may enable a travel document to be obtained for the person, which would facilitate the person's removal | S35, Asylum and Immigration (Treatment of Claimants, etc.) Act 2004 | Fingerprints and photographs | No specified period | Should only be used for the specific purpose of identifying someone who is subject to a removal decision |
| A person making an application for entry clearance, leave to enter or remain in the UK or variation of leave to enter or remain in the UK to provide their biometrics | S126 of the Nationality, Immigration and Asylum Act 2002 | Fingerprints and photographs | Normally 10 years, unless the person is a risk of high harm or has unelapsed settled status in the UK<br>Photos retained until person obtains a British passport | As specified under regulations made under s8 of the UK Borders Act 2007 |

| | | | | |
|---|---|---|---|---|
| Foreign nationals subject to immigration control, who are required to apply for biometric cards | Sections 5 to 15 of the UK Borders Act 2007 | Fingerprints and photographs | Normally 10 years, unless the person is a risk of high harm or has unelapsed settled status in the UK<br>Photos retained until person obtains a British passport | As specified under regulations made under s8 of the UK Borders Act 2007 |

| **Situation** | **Legislation** | **Modes** | **Retention Period** | **Permitted Uses** |
|---|---|---|---|---|
| A person who is a foreign criminal within the meaning of s32 of the UKBA 2007 and is subject to automatic deportation provisions | S51 of the Borders, Citizenship and Immigration Act 2009 | Fingerprints | A period specified by the Secretary of State, or ten years if no period specified | NA |
| Foreign nationals applying for transit visas | S126 of the Nationality, Immigration and Asylum Act 2002, amended by S8 IA 2014 | Fingerprints, photographs | Ten years | For identification purposes for high-risk categories of persons to immigration control |
| Persons applying to become British citizens | S41 of the British Nationality Act 1981, amended by s10 IA 2014 | Fingerprints and photographs | Fingerprints must be deleted when citizenship granted. Photographs must be deleted when passport issued. | To verify that they are the same person who was granted leave to remain |
| Persons who are suspected of being immigration offenders and hence liable to be detained | P18(2) of Schedule 2 Immigration Act 1971, amended by s9 IA 2014 | Fingerprints | None – verification power only | In line with police powers for suspected offenders |

| | | | | |
|---|---|---|---|---|
| A person who is subject to a Terrorism Prevention and Investigation Measure | Schedule 6, Terrorism Prevention and Investigation Measures Act 2011 | Fingerprints and DNA profiles | Six months for an individual with no previous convictions (or one exempt) conviction<br>Indefinite if the individual has been convicted of a recordable offence | Purposes of terrorism prevention and national security |

**EC Council Regulation 2725/2000: EU Eurodac Regulations**

The UK is signed up to data sharing via the Eurodac central database where European member states store and verify three key categories of fingerprint records:

1. All asylum applicants over 14 years of age have their fingerprints taken, verified and stored (for ten years, with certain exceptions) to ensure that when they apply for asylum in one member country, they do not already have an ongoing application in another country
2. Persons over 14 years of age found illegally attempting to cross the external border have their fingerprints checked and then stored for 18 months (since July 2015, previously this was two years)
3. Persons found illegally present within a member state; on a discretionary basis, a state may request to search against Eurodac stored asylum records. Their data may not be stored as this is a verification power only

Since 20th July 2015, there have been some changes to allow law enforcement authorities to make a search into Eurodac for the purpose of prevention and detection of a serious crime or terrorism (previously this was only allowed for border control purposes). This is a fairly limited power, as there is a stringent verification procedure to prevent law enforcement from making ad-hoc searches into Eurodac. In particular, countries requesting a search into Eurodac for law enforcement purposes must demonstrate that they have searched all national databases and interrogated systems using Prüm; only then they are allowed to launch law enforcement searches

into Eurodac. Hence the UK, which has not yet implemented Prüm, is not able to launch law enforcement searches.

In addition, countries have agreed more stringent deadlines for data exchange. For asylum applicants (category 1), data must be transmitted within 72 hours of the asylum application being lodged. For those caught crossing the external border illegally (category 2), data must also be transmitted within 72 hours. The exception is for people who are detained, where time periods are dependent upon national laws.

**Council Regulation (EC) No 1030/2002 as amended: Uniform format for residence permits for non-EU country nationals**

This regulation establishes a uniform format for residence permits, and the information they must contain, for non-EU nationals living legally in the EU.

Regulation (EC) No 380/2008 amends Regulation (EC) No 1030/2002 regarding the integration of biometric identifiers into the uniform format for residence permits:

- Biometric identifiers are used to verify the permit's authenticity and the holder's identity. These consist of an applicant's recent photo and two digital flat fingerprints to be stored within a secure chip on a standalone card
- The procedure for taking these identifiers must respect national legislation and the safeguards contained in the UN human rights and child conventions
- The data from the biometric identifiers must be stored and secured so that their integrity, authenticity and confidentiality are guaranteed

**Prüm**

On 8th December 2015, the House of Commons voted to endorse opting into Prüm, which includes reciprocal searching of EU Member States' databases for DNA

profiles, fingerprints and vehicle registration information. The UK then applied to re-join Prüm and the application was duly accepted in May 2016.

The Prüm Treaty was an agreement signed by seven EU member States in May 2005 to encourage cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal immigration, in part by granting reciprocal access to national databases containing DNA profiles, fingerprints and vehicle registration data.

On 23 June 2008, significant elements of the Treaty were transposed into EU law in Council Decisions. The main elements are automated search and comparison of DNA, fingerprint and vehicle registration data (Chapter 2 of the Council Decision 2008/615/JHA and Chapters 2-6 of the Council Decision 2008/616/JHA), automated exchange for the prevention of offences in the context of major events (including terrorism) with a cross-border dimension (Chapter 3 and 4 of the Council Decision 2008/615/JHA), police cooperation (Chapter 5 of the Council Decision 2008/615/JHA and Chapter 6 of the Council Decision 2008/616/JHA) and data protection rules (Chapter 6 of Council Decision 2008/615/JHA).

In addition, a further decision was passed: Council Framework Decision 2009/905/JHA(Annex C) on the accreditation of forensic service providers carrying out laboratory activities. This Framework Decision requires forensic service providers (for both fingerprints and DNA) to be accredited to ISO standard 17025 and also requires Member States to treat forensic results from ISO 17025 accredited laboratories in Member States as they would a domestic ISO 17025 accredited laboratory.

These council decisions are together known as the Prüm Decisions.

While prior legislation already allows for the international sharing of this data, opting into Prüm allows for faster access with greater automation. Implementing Prüm

would partially automate the process for sharing DNA and fingerprint data and wholly automate it for vehicle enquiries. The Home Office has published a comprehensive business and implementation case regarding the impact of an opt-in to Prüm, which is publically available online.

## Law Enforcement

### Types of Offences

Powers to take and retain biometric records for law enforcement purposes depend upon the type of offence for which a person is charged, arrested or convicted.

A **recordable** offence is one for which the police are required to keep a record, usually on the Police National Computer (PNC). Generally speaking, these are imprisonable offences; however, they also include a number of non-imprisonable offences, such as begging and taxi touting. The police are not able to take or retain the DNA or fingerprints of an individual who is arrested for an offence which is not recordable. The full definition of a recordable offence is defined in the Schedule to the National Police Records (Recordable Offences) Regulations 2000, SI 2000/1139.

A **qualifying** offence is one listed under section 65A of the Police and Criminal Evidence Act 1984; this includes sexual, violent, terrorism and burglary offences.

A **minor** offence is a recordable offence that is not a qualifying offence.

An **excluded** offence is a minor offence that was committed when the individual was under 18, for which they received a sentence of fewer than 5 years imprisonment and is the only recordable offence for which the person has been convicted.

### Police and Criminal Evidence Act 1984

The Police and Criminal Evidence Act (PACE) is the key legislation governing the powers of police officers (and anyone else involved in investigating crime or charging offenders) in England and Wales. This is a wide-ranging piece of legislation that includes powers to arrest, detain, interrogate, and enter and search premises. These powers include the taking of biometric samples.

In general, under PACE, police may not take fingerprints or a non-intimate sample from a person without their consent. Exceptions to this include when a person has been arrested for, charged with or convicted of a recordable offence. Under these circumstances, police can take fingerprints or non-intimate samples without consent. 'Non-intimate samples' include DNA samples taken by means of a cheek swab.

**Section 64 of PACE** sets out the former legal framework on retaining fingerprints and DNA data. This did not specify time limits for retention nor any procedure by which data should be removed from police records; hence police were effectively able to retain fingerprint and DNA data taken from individuals arrested for a recordable offence for an indefinite period of time.

**Section 64 has now been repealed by the Protection of Freedoms Act 2012.**

**PACE Codes of Practice**

The Codes of Practice establish more specific practices associated with police powers to search persons and premises, to detain, investigate and arrest individuals, and to deal with the detention of terrorism suspects.

**Code A** (revised in Mar 2015) deals with a police officer's powers to stop and search a person or a vehicle prior to making any request, as well as the requirements to record these encounters.

**Code B** (revised in Oct 2013) establishes a code of practice for searches of premises, and covers seizure and retention of property.

**Code C** (revised in Feb 2017) establishes the requirements and procedures for the detention and questioning of persons by police officers. The statutory provisions in section 65(I) of PACE requiring appropriate consent refer to persons who have not attained (or where there is no clear evidence that they have attained) the age of 17, where consent is required by that person and their parent or guardian. This applies

to taking of fingerprints, samples, footwear impressions, photographs, searches and examinations.

**Code D** (revised in Feb 2017) is the main code concerning biometrics and is covered in the next section.

**Code E** (revised in Jan 2016) governs audio recording of interviews carried out at police stations. Interviews that fall under the following scenarios must be audio taped:

- All interviews with a suspect who is cautioned in relation to a criminal offence
- Any extra questions put to a suspect after they have been charged with a criminal offence
- All discussions with a person, who has been charged with a criminal offence, regarding any other written statement or interview with another person

**Code F** (revised in Oct 2013) governs visual recording with sound of an interview, which may occur in all the scenarios outlined under Code E, and in addition:

- In the presence of a deaf/blind or speech impaired person who uses sign language to communicate
- In the presence of a minor or anyone else who requires an appropriate adult
- Where a visually recorded interview is requested by the suspect or their representative

**Code G** (revised in Jul 2012) concerns statutory powers of arrest by police officers. Where mobile fingerprinting is available and the suspect's name cannot be ascertained or is uncertain, the officer should consider using the power under section 61(6A) of PACE (see Code D paragraph 4.3(e)) to take and check the fingerprints of a suspect as this may avoid the need to arrest solely to enable their name to be ascertained.

**Code H** (revised in Jun 2014) establishes the requirements for the detention of suspects arrested under the Terrorism Act 2000 and how they should be treated and

questioned whilst in custody. This code ceases to apply once a suspect is either charged with an offence, released without charge or transferred to a prison.

**PACE Code of Practice D: The Identification of Persons by Police Officers**

Code D establishes the code of practice for the identification of persons by police officers. 'Identification by fingerprints' applies when a person's fingerprints are taken to compare with fingerprints found at the scene of the crime, to check and prove convictions, and to help ascertain a person's identity.

'Identification by body samples and impressions' applies when samples such as blood or hair are taken to generate a DNA profile for comparison with material obtained from the scene of a crime, or a victim. Code D states that fingerprints, samples, impressions and photographs may be taken, used and retained, and identification procedures carried out, only when justified and necessary for preventing, detecting or investigating crime.

Code D clarifies that 'fingerprints' refer to any record, produced by any method, of the skin pattern and other physical characteristics or features of a person's fingers or palms. **A person's fingerprints may be taken in connection with the investigation of an offence with their consent (in writing if at a police station) or (under PACE section 61), without consent, provided that they are aged over ten years and:**

- Have been detained at a police station in consequences of being arrested for a recordable offence, **and** if they have not had fingerprints previously taken **or** if previously taken fingerprints are not a complete set or not of sufficient quality ***(section 61(3))***
- Have been detained at a police station and charged with a recordable offence or informed that they will be reported for such an offence, **and** if they have not had fingerprints previously taken **or** if previously taken fingerprints are not a complete set or not of sufficient quality ***(section 61(4))***
- Have answered to bail for a person whose fingerprints were taken previously, and there are reasonable grounds for believing they are not the same person

**or** they have claimed to be a different person **and** the court or an officer of inspector rank or above authorises the fingerprints to be taken at the court or police station ***(section 61(4A))***

- Have been arrested for a recordable offence and released on bail **and** if they have not had fingerprints previously taken **or** if previously taken fingerprints are not a complete set or not of sufficient quality ***(section 61(5A))***
- Have been charged with a recordable offence or informed they will be reported for such an offence (but not detained at a police station) **and** if they have not had fingerprints previously taken **or** if previously taken fingerprints are not a complete set or not of sufficient quality ***(section 61(5B))***
- Have been convicted of a recordable offence **or** given a caution in respect of a recordable offence which, at the time of caution, the person admitted to; **and**, if since their conviction, they have not had fingerprints taken **or** if previously taken fingerprints are not a complete set or not of sufficient quality; **and** if an officer of inspector rank or above is satisfied that taking the fingerprints is necessary to assist in the prevention or detection of crime and hence authorises the taking ***(section 61(6))***
- Are subject to reasonable suspicion of committing or attempting to commit, **or** have committed or attempted to commit any offence; **and** if either the person's name is unknown and cannot be readily ascertained by the constable **or** if the constable has reasonable grounds for doubting whether a name given by the person is their real name ***(section 61(6A))***. Fingerprints taken under this power are not regarded as having been taken in the course of the investigation of an offence
- Have been previously convicted outside of England and Wales for an offence, which, if committed in England and Wales, would be a qualifying offence as defined by PACE, section 65A; **and** if they have not had fingerprints previously taken **or** if previously taken fingerprints are not a complete set or not of sufficient quality ***(section 6(6D))***; **and** if a police officer of inspector rank or above is satisfied that taking fingerprints is necessary to assist in the prevention or detection of crime and authorises them to be taken

**PACE section 63A(4) and Schedule 2A provide powers to require a person to attend a police station to have their fingerprints taken** in the exercise of certain powers enumerated above, when the power applies at the time the fingerprints are taken. Persons who fail to comply with the requirement may be arrested without warrant. These powers apply to individuals who have been:

- Arrested for a recordable offence and released, if the requirement is made less than six months from the day the investigating officer was informed that the fingerprints previously taken were incomplete or not of sufficient quality ***(section 61(5A))***
- Charged with a recordable offence, if the requirement is made less than six months from the day the person was charged or reported if fingerprints have not been taken since then **or** from the day the investigating officer was informed that the fingerprints previously taken were incomplete or not of sufficient quality ***(section 61(5B))***
- Convicted, cautioned, warned or reprimanded for a recordable offence in England and Wales. If the offence was a qualifying offence, there is no time limit for the exercise of this power. Where the offence is for a recordable offence which is not a qualifying offence, the requirement must be made less than two years from the day the person was convicted, cautioned, warned or reprimanded, if fingerprints have not been taken since then or from the day the investigating officer was informed that the fingerprints previously taken were incomplete or not of sufficient quality ***(section 61(6))***
- Persons convicted of a qualifying offence outside England and Wales ***(section 61(6D))***

Reasonable force may be used, if necessary, to take a person's fingerprints without their consent under the powers enumerated above. Before fingerprints are taken without consent, the person must be informed of the reason their fingerprints are to be taken, the power under which they are to be taken, and the fact that the relevant authority has been given, where applicable.

If fingerprints are taken, the person must be informed that their fingerprints may be the subject of a speculative search against other fingerprints, and that their

fingerprints may be retained in accordance with Annex F (no longer up to date following POFA). A record must be made as soon as practicable after the fingerprints are taken, and should be included in the person's custody record if they are detained at a police station when the fingerprints are taken.

Fingerprints, footwear impressions and samples taken from a person suspected of committing a recordable offence but not arrested, charged or informed they will be reported for it, may be subject to a speculative search only if the person consents in writing. Fingerprints of a suspect who has not been arrested may be taken in connection with any offence using a mobile device and then checked on the street against the database containing the national fingerprint collection, but may not be retained.

**Part II (Powers of entry, search and seizure) of the Police and Criminal Evidence Act 1984 (as amended)** apply to the recovery and retention of latent marks:

- **s.8** provides for a warrant to be issued by a justice of the peace if; there are reasonable grounds for believing that an indictable offence has been committed and it is believed that a premises contains evidence of substantial value to an investigation that is likely to be relevant and admissible
- **s.19** confers the powers to a constable, when lawfully on a premises (i.e. without a warrant), to seize any evidence from the premises where there are reasonable grounds for believing that it can be used in the investigation of the offence being investigated or any other offence
- **s.22** outlines the retention periods for items seized under s19

**Protection of Freedoms Act 2012**

Part 1 of the Protection of Freedoms Act 2012 (POFA) sets out the regime for the retention and destruction of fingerprints, DNA profiles and DNA samples. Note that a 'DNA profile' refers to the alphanumeric string derived from a DNA sample, which can be loaded onto an electronic database. It contains relatively limited information

about a person's genetic information but is sufficient to identity a person. References in later sections to 'data' relate to fingerprints and DNA profiles and not to any other type of data.

A 'DNA sample', in contrast, refers to the 'wet sample' taken, for example, from a swab from inside of the cheek. This contains the entirety of a person's genetic information. DNA samples must be destroyed as soon as a DNA profile has been created from the sample or, if a DNA profile has not been created from the sample, within six months. However, there is an exception to this if the sample may be required for disclosure to the defence. Section 146 of the Anti-Social Behaviour, Crime and Security Act amends section 63U of PACE so that a sample which falls within the terms of the Criminal Procedure and Investigations Act (CPIA) and its associated Code of Practice may be retained for longer than six months. It must be destroyed once CPIA ceases to apply.

Fingerprints and DNA profiles must be destroyed if the taking of the data was unlawful, the data was taken in connection with an unlawful arrest, or the data was taken in connection with an arrest due to mistaken identity.

For fingerprints and DNA profiles taken lawfully under PACE or with the individual's consent, there is a presumption that this data must be destroyed unless one or more exceptions applies. Under section 63P of PACE as added by section 12 of POFA, if fingerprints or DNA profiles are taken when one exception applies, and that exception ceases to apply but another one comes into effect, the material can continue to be retained.

Exceptions are as follows:

**Individual under investigation**

Section 63E of PACE, inserted by section 2 of POFA, allows retention of a DNA profile and fingerprints as long as the person from whom the material was taken remains under investigation or the subject of criminal proceedings.

**Individuals arrested for or charged with a qualifying offence**

Section 63F of PACE, inserted by section 3 of POFA, deals with those arrested for or charged with (but not convicted of) qualifying offences.

If the individual who has been arrested or charged has a previous conviction for a recordable offence, then the police can retain their data indefinitely.

If the individual has no previous convictions and:

- They have been charged with a qualifying offence, then the police can retain their data for three years
- They have been arrested but not charged for a qualifying offence, **and** the police have first obtained the consent of the Independent Commissioner for the Retention and Use of Biometric Material (appointed under section 20 of the 2012 Act), then the police can retain their data for three years. Moreover, that 3 year period may be extended for a further 2 years if, following an application by the relevant Chief Officer under section 63F(7), a District Judge so orders.

**Individuals arrested for or charged with a minor offence**

Section 63H of PACE, inserted by section 4 of POFA, deals with those who are arrested for or charged with, but not convicted of, a minor offence. Data taken from such people must be destroyed, unless they have previously been convicted of a recordable offence (other than an excluded offence) in which case the material can be retained indefinitely.

**Adults convicted of a recordable offence**

Section 63I of PACE, inserted by section 5 of POFA, states that data from an adult convicted of a recordable offence can be retained indefinitely. 'Convicted' for these purposes includes being cautioned, being found not guilty by reason of insanity, or being found to be under a disability (i.e. unfit to plead) and to have committed the act they have been charged with.

**Persons under 18 convicted of an offence**

Data from those convicted of a qualifying offence committed when aged under 18 can be retained indefinitely. Similar provision is made for the indefinite retention of data taken from those convicted of a minor offence (other than a first minor offence) committed when aged under 18. 'Convicted' includes being reprimanded or warned,

being found not guilty by reason of insanity, or being found to be under a disability (i.e. unfit to plead) and to have committed the act they have been charged with.

Section 63K of PACE, inserted by section 7 of POFA, states that data from those convicted of a first minor offence committed when aged under 18 can be retained for the following periods:

- Where the individual is given a custodial sentence of less than five years in respect of the offence, the data can be retained until the end of the period consisting of the term of the sentence plus five years
- Where the individual is given a custodial sentence of five years or more, the data may be retained indefinitely
- Where the individual is given a sentence other than a custodial sentence, the data may be retained for five years

If the offender commits a further recordable offence during any of these retention periods then their data may be retained indefinitely.

**Persons given a penalty notice**

Section 63L of PACE, inserted by section 7 of POFA, states that data from a person who is given a penalty notice under section 2 of the Criminal Justice and Police Act 2001 and in respect of whom no proceedings are brought for the offence to which the notice relates, may be retained for a period of two years.

**Summary of retention periods under POFA (see pages 63-67)**

**Retention for reasons of national security**

Section 63K of PACE, inserted by section 9 of POFA, makes provision for the retention of material for the purposes of national security. Where a person's data would otherwise have to be destroyed, the police may retain it for up to two years where the responsible chief officer of police determines that it is necessary to do so for the purposes of national security under a 'national security determination'. National security determinations can be renewed for up to two years at a time; there

is no limit on the number of times that a national security determination can be renewed.

The Independent Commissioner for the Retention and Use of Biometric Material (appointed under section 20 of POFA) is responsible for keeping every national security determination made by the police under review. The police must send the Commissioner a copy of every determination they make or renew, together with the reasons for making or renewing it, within 28 days of making or renewing it. They must also provide the Commissioner with such documents and information as he may require for the purpose of reviewing national security determinations.

If, on reviewing a national security determination, the Commissioner concludes that it is not necessary to retain the data that the determination relates to, then they may order the destruction of the material (provided that it is not otherwise capable of being lawfully retained).

Section 22 of POFA requires the Secretary of State to issue statutory guidance on the making and renewal of national security determinations. The guidance was issued by the Home Office in June 2013: Protection of Freedoms Act 2012: Guidance on the making or renewing of national security determinations allowing the retention of biometric data.

**Retention of material given with consent**

Section 63N of PACE, inserted by section 10 of POFA states that fingerprints and DNA profiles taken voluntarily may be retained until they have fulfilled the purpose for which they were taken or derived.

Material taken from a person who is convicted of a recordable offence or has previously been convicted of a recordable offence may be retained indefinitely.

If material is retained with consent, then consent must be given in writing and can be withdrawn at any time.

**Destruction of DNA samples**

Section 63R of PACE, inserted by section 14 of POFA states that ‘wet’ samples must be destroyed as soon as a DNA profile has been created from the sample or, if a

DNA profile has not created from the sample, within six months (subject to the 'CPIA exception' described above).

**Purposes for which DNA samples, DNA profiles and fingerprints taken by the police can be used**

Section 63T of PACE, inserted by section 16 of POFA, states that DNA samples, DNA profiles and fingerprints taken by the police under PACE powers or with consent can be used only for the following purposes:

a) In the interests of national security
b) For the purposes of a terrorist investigation
c) For purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution
d) For purposes related to the identification of a deceased person or of the person to whom the material relates

So, for example, the courts have held that DNA taken from a person arrested for a recordable offence cannot be used to determine whether that person is the father of a child and therefore liable to make child support payments for that child, as that is not a crime or security issue.

**Deletion of data taken and retained before the 2012 Act's provisions came into force**

Before the relevant sections of POFA were brought into force, DNA and fingerprints that had previously been taken and were being stored, which would not meet the requirements of the Act, were deleted from the relevant databases. Secondary legislation was issued by the Secretary of State under section 25 of POFA which set out the framework for the destruction of such data.

The Protection of Freedoms Act 2012 (Destruction, Retention and Use of Biometric Data) (Transitional, Transitory and Saving Provisions) (Amendment) Order 2015 came into force on 31st October 2015 and extends the transitional period in which material taken under PACE prior to POFA may be considered as to whether it

qualifies for extended retention for reasons of national security for an additional year, to 31st October 2016.

**Early deletion and the record deletion process**

In certain circumstances individuals may apply to a chief officer to have their biometric information deleted before the end of the retention period set out in legislation.

The National Police Chiefs' Council has issued guidance to chief officers, the stated purpose of which is to ensure that a consistent approach is taken in relation to dealing with applications for the deletion of records from national police systems: Deletion of Records from National Police Systems (PNC/NDNAD/IDENT1).

In certain circumstances individuals may apply to have their lawfully retained biometric information deleted from national police systems (NDNAD and IDENT1) earlier than the periods specified under PACE (as amended), if:

- They have no previous convictions and their biometric information is held as a result of being arrested and charged with a Qualifying Offence but not subsequently convicted: or,
- They have no previous convictions and their biometric information is held due to a PND [a Penalty Notice for Disorder.

Individuals who are clearly not linked to any crime must 'evidence' their grounds for making an application.

**NDNAD Strategy Board (now the Forensic Information Databases (FIND) Strategy Board)**

Section 63AB of PACE, inserted by section 24 of POFA, sets out the statutory basis for a National DNA Database Strategy Board to oversee the operation of the national DNA database. The Strategy Board has operated on this basis since 31st October 2013 (it existed previously but operated on a non-statutory basis), and defines the permitted uses of samples and associated data in The NDNAD Strategy Board Policy for Access and Use of DNA Samples, Profiles and Associated Data.

The Board has also issued guidance on the deletion of DNA profiles and publishes an annual report.

**Anti-Social Behaviour, Crime and Policing Act 2014**

The Anti-Social Behaviour, Crime and Policing Act (section 144) amends Section 61 of PACE, creating a power to take further fingerprints or non-intimate samples if fingerprints have already been taken but an investigation was discontinued and subsequently resumed, and if before resumption of the investigation, fingerprints or DNA profiles were destroyed.

Section 145 amends Section 63P of PACE, creating a power to retain fingerprints or DNA profiles in connection with a different offence; if fingerprints or DNA were taken under section 63D from a person in connection with the investigation of an offence, and the person is subsequently arrested for or charged with a different offence, or convicted of or given a penalty notice for a different offence.

Sections 63E to 63O and sections 63Q and 63T relate to material taken or derived from a sample taken:

a) in connection with the investigation of the offence

b) on the date on which the person was arrested for that offence (or charged with it or given a penalty notice for it, if the person was not arrested)

**Criminal Procedure and Investigations Act 1996 & Codes of Practice**

The Criminal Procedure and Investigations Act 1996 (CPIA) regulates the investigation and prosecution of criminal offences, and governs preservation of evidence, including allowing retention of biometric data, if samples may be required for use in an ongoing case; this includes court proceedings and any possible appeal.

Section 64 amends section 63A of PACE, allowing retention of fingerprint and DNA data if a person has been arrested on suspicion of being involved in a recordable offence or has been charged with such an offence or has been informed that he will be reported for such an offence. Under these circumstances biometric data may be checked against other fingerprints or samples are held by or on behalf of a police force (or police forces) in England, Wales, Scotland, the Royal Ulster Constabulary, the States of Jersey, the Island of Guernsey or the Isle of Man.

As stated above, section 146 of the Anti-Social Behaviour, Crime and Security Act amends section 63U of PACE so that a DNA sample which falls within the terms of CPIA and its associated Code of Practice may be retained for longer than six months. It must be destroyed once CPIA ceases to apply.

**Crime and Security Act 2010**

Section 7 inserts section 65A into PACE providing a list of qualifying offences; this includes murder, manslaughter, false imprisonment, kidnapping, sexual, violent, terrorism and burglary offences.

Following ***R v Chief Constable of South Yorkshire ex parte S and Marper***, S and Marper lodged an application with the European Court of Human Rights (European Court of Human Rights Ruling - S. & Marper v. UK - 30562/04 [2008] ECHR 1581). The Grand Chamber's judgment was handed down on 4 December 2008.

The Court accepted that the retention of fingerprint and DNA information pursued a legitimate purpose, namely the detection and prevention of crime, but held unanimously that the retention and storage of the applicants' fingerprints and DNA samples was disproportionate and not "necessary" in a democratic society. Article 8 of the European Convention on Human Rights had therefore been violated.

**Criminal Justice and Public Order Act 1994**

Section 58 amends the definition of an intimate sample to mean:

(a) A sample of blood, semen or any other tissue fluid, urine or pubic hair

(b) A dental impression

(c) A swab taken from a person's body orifice other than the mouth

A non-intimate sample refers to:

(a) a sample of hair other than pubic hair

(b) a sample taken from a nail or from under a nail

(c) a swab taken from any part of a person's body including the mouth but not any other body orifice

(d) saliva

(e) a footprint or a similar impression of any part of a person's body other than a part of his hand

**International Criminal Court Act 2001**

Schedule 4 allows that a nominated court may order the taking of a person's fingerprints or non-intimate DNA sample by a police constable, if the Secretary of State receives a request from the ICC for assistance in obtaining evidence as to the identity of a person.

The nominated court may require the person to attend a police station, subject to at least seven days' notice, and if the person fails to comply with the requirement, the court may issue a warrant for their arrest or detain the person for a period as required to enable the identification to be taken.

The evidence may be taken with consent given in writing, or without consent if authorised by an officer of the rank of superintendent or above. Records must be taken as soon as reasonably practical and a copy sent to the Secretary of State.

The fingerprints, samples or information may be used only for the purpose of an investigation into a relevant offence. A check may not be made against them under section 63A(1) of the Police and Criminal Evidence Act 1984 (c. 60) (checking of fingerprints and samples), or Article 63A(1) of the Police and Criminal Evidence (Northern Ireland) Order 1989 (S.I. 1989/1341 (N.I. 12)) (checking of fingerprints and samples), except for the purpose of an investigation into a relevant offence (an ICC crime or an offence defined in part 5 of this act).