

Chapter 24 – Fingerprinting/taking fingerprints/powers

24	Introduction
24.1	EURODAC
24.2	Use of Morpho RapID units
24.3	Notification form IS 86
24.3.1	Fingerprint record – (form IFB)
24.4	Persons authorised to take fingerprints
24.5	Fingerprinting juveniles and dependants
24.6	Attendance for fingerprinting
24.7	Destruction of fingerprints
24.8	Procedures for fingerprinting
24.9	Taking fingerprints for identification purposes only
24.10	Requesting checks with other agencies
24.11	Use of force when taking fingerprints
24.12	Requests for expert statements for prosecution of fraudulent applicants
24.13	Fingerprints for documentation purposes
24.14	Fingerprinting of corpses

24 Introduction

Section 141 of the 1999 Act, which came into force on 11 December 2000, gives power to take fingerprints in immigration cases from the following specified categories:

- Any person who, on being required to do so by an immigration officer (IO) on his arrival in the UK, fails to produce a valid passport with a photograph or some other document satisfactorily establishing his identity and nationality and citizenship [group A].
- Any person who has been refused leave to enter the UK but granted temporary admission under paragraph 21 of schedule 2 to the 1971 Act if an IO reasonably suspects he might break any condition imposed on him relating to residence as to reporting to the police or an IO [group B].
- Any person in respect of whom a relevant immigration decision has been made. 'Relevant immigration decision' means a decision of the kind mentioned in section 82(2) (g), (h), (l), (j), (k) of the Nationality, Immigration and Asylum Act 2002 [group C]. Fingerprints may be taken from the time C is given notice of the decision until the time the decision ceases to have effect (or, in the case of a deportation order, it is revoked or otherwise ceases to

have effect). This was amended by section 15 of the Asylum and Immigration (Treatment of Claimants, etc.) Act 2004.

- Where an individual is detained under paragraph 16 or has been arrested under paragraph 17 of schedule 2 to the Immigration Act 1971 [group D].
- Where an individual has made a claim for asylum [group E].
- Where an individual is a dependant of someone who falls into one of the above categories [group F].

[Back to Top](#)

24.1 EURODAC

The EURODAC Regulation was adopted on 11 December 2000 to establish a computerised central database of fingerprint images, as well as the electronic means for European Union (EU) member states to transmit and store fingerprint images and to receive results from the central unit database based in Luxembourg. EURODAC enables the fingerprints of asylum applicants and certain other third country nationals over the age of 14, principally those apprehended in connection with crossing the external frontier of the EU, to be compared solely in order to support the application of the Dublin Convention. The system commenced on 15 January 2003.

EURODAC identifies:

- Those over the age of 14 who have applied for asylum in a member state after 15 January 2003.
- Certain categories of those who enter illegally or are found on the EU territory unlawfully after 15 January 2003. These are included because they may also be subject to the provisions of Dublin if they later claim asylum.

Comprehensive checks and quick responses from EURODAC (maximum 24 hours) will result in a greater proportion of UK applicants being identified and returned to other EU states under the provisions of the Dublin Convention. The possible match or 'hit' identified by the EURODAC central unit will be transmitted automatically to

the Immigration Fingerprinting Bureau (IFB), who will manually verify that it is a match. The results of the EURODAC searches are then automatically transmitted via email to the location code where the fingerprints were taken and to third country unit (TCU). It will be TCU's responsibility to inform the office where the application was made, obtain the file and take appropriate action under the Dublin mechanisms leading to the applicant's transfer. Refer to the asylum instruction (AI) on [third country cases](#) for further information.

Should IFB be required to scan on any sets of fingerprints, form IFB1 should be fully completed with the individual's correct demographic data, reason for fingerprinting and correct EURODAC category code (should a EURODAC search be required).

The appropriate UK EURODAC category **must** be clearly marked on the fingerprint form (IFB1) as follows:

UK EURODAC Category	UK Definition
Category 1 (mandatory)	Asylum (main app. and deps) 14+ years old
Category 2 (mandatory)	Apprehended in connection with irregular crossing of UK border from outside EU territory. Non-asylum 14+ years old
Category 3 (discretionary)	Encountered illegally present in UK. Non-asylum 14+ years old

EURODAC categories 2 and 3 apply even when fingerprints are taken from someone who has not claimed asylum.

Note. EURODAC data cannot be used for prosecution action against an applicant who is a EURODAC match. The data can only be used for the sole purpose of supporting the application of the Dublin convention and its I successor, Dublin II.

Under no circumstances should IOs carry out checks against EURODAC on behalf of the police.

[Back to Top](#)

24.2 Use of Morpho Rapid units

Establishing identity is a key objective on enforcement operations, and the Morpho RapID device allows for biometric checks to be completed enhancing the quality of investigations. Biometric information allows officers to make more accurate and informed decisions about a person's identity and immigration status.

It is possible, with consent, to check the fingerprints of any person encountered on an enforcement operation using the Morpho RapID units.

When an individual is encountered on an enforcement operation, initial enquiries should be made to establish key details such as name, nationality and their current immigration status. At this stage and if the officer believes that the person is still of interest or suspected of any breach of immigration legislation, regardless of any documentation or the verbal credentials presented by the individual, the investigating officer must attempt to use the Morpho RapID device with the consent of the individual being questioned.

This will allow the individual an opportunity to quickly eliminate themselves from further enquiries, and give officers certainty as to the identity of the individual being questioned.

If consent is given, the officer should record this clearly in their personal notebook. This fact will also need to be recorded on the port and HO files, together with the name of the officer who took the fingerprints, the RapID result, including the unique identification number and/or IFB barcode number.

Where consent is refused, or where there is no match on the Morpho RapID device, officers may continue with their investigations to confirm identity and immigration status, and may later have the power to obtain fingerprints under section 141 of the 1999 Act, or paragraph 18(2) of schedule 2 to the 1971 Act.

Officers must attempt to make full use of the Morpho RapID device with all individuals suspected of immigration offences encountered on enforcement operations, in line with the legal powers.

MorphoRapID units do not capture and record fingerprints. Templates of fingerprints are transmitted to the immigration and asylum biometrics system (IABS) database and a search is made against existing records. A response is transmitted back to the unit indicating whether or not a possible match has been found. A fingerprint expert does not verify the results of these searches. All checks must be recorded in the officer's pocket notebook with the related transmission identifier. Reference should also be made as to which power the fingerprint check was conducted under.

Security and safe storage of units

Units are encrypted for security purposes and all transmissions are automatically deleted from the units once the results have been viewed and the units are switched off. The units also include a camera facility to enable photographs to be compared against any possible match.

Morpho RapID units may only be used by an officer who has completed the mandatory training. A written record of this should be held by both the officer and the officer's line manager and will be required before an officer can be assigned to a unit. For these purposes, the term 'officer' also includes legacy customs officers who have been designated as immigration officers and seconded police officers.

Storage of units must be in line with the generic physical security guidance at:

[Physical and environmental security-full security guidance](#)

In addition, there are several security points that are specific to the RapID units:

- Devices must be located in a secure area/office when not in use.
- Every team must have a list recording all the units held by the team.
- Each team should have a designated officer responsible for the equipment and updating of the log.
- The log should be checked at the end of every shift so that all units are accounted for.
- The log should detail the movement of each device on operations, noting the officer responsible on the day.

- Passwords must not be visible under any circumstances. This includes not sticking passwords to units and not leaving them under workstation keyboards.
- The devices should not be taken in situations where theft or risk to personal safety is increased.
- The devices should not be visible in any vehicle or unattended in public places.

[Back to Top](#)

24.3 Notification form IS 86

Every individual to be fingerprinted under section 141 of the 1999 Act should be served with form IS86 notifying the individual that he is to be fingerprinted, explaining why he is to be fingerprinted and also explaining when the fingerprints will be destroyed.

[Back to Top](#)

24.3.1 Fingerprint record – (form IFB1)

All sections of the IFB1 form must be fully completed when a set of fingerprints are taken. If the set is captured electronically on a 'livescan' workstation, all demographic details should be fully completed before electronically transmitting to the IFB. If the set of fingerprints are taken by the ink and the paper method, they should be transmitted via a 'cardscan' workstation where available, again ensuring all demographic details have been fully completed. The original set of fingerprints (IFB1) should be sent immediately or at the latest within 24 hours to the IFB. Copies must not be kept on file. If cardscan is not available, IFB will scan the fingerprint form into IABS.

[Back to Top](#)

24.4 Persons authorised to take fingerprints

Under section 141(5) of the 1999 Act those authorised to take fingerprints are:

- a police constable
- an immigration officer
- a prison officer
- an officer of the Secretary of State authorised for the purpose
- a person who is employed by detention centre contractors.

[Back to Top](#)

24.5 Fingerprinting juveniles and dependants

Fingerprints may not be taken from a person between the ages of five and 16 unless in the presence of an adult (18 years or older) who is the child's parent, guardian or person who, for the time being, takes responsibility for the child (section 141(3) of the 1999 Act refers). In the latter case the adult may not be an officer of the Secretary of State, that is, a Home Office employee, a police officer, prison officer, a person employed under a detention centre contract or a person authorised by the Secretary of State to take fingerprints. The decision to do so must be confirmed by a chief immigration officer (CIO) (or other suitably designated person depending on the type of 'authorised person') (section 141 (12) of the 1999 Act). CIOs should only refuse to authorise the taking of fingerprints in exceptional circumstances, identified below, and should refer to an Inspector grade or above if refusing authority:

- where there is a serious health risk to either the child or a member of staff
- if the child is distressed.

Where a deferral of fingerprinting is made, arrangements should be made to fingerprint the child as soon as possible thereafter.

In accordance with section 141(13), where it is reasonably believed that a person is over 16, they should be treated accordingly and there is nothing to prevent

fingerprints being taken if they fall into one of the categories specified in section 141(7) of the 1999 Act.

Section 141(14) of the 1999 Act [group F] defines a person as a dependant of another if:

- they are that person's spouse or child under the age of 18
- they do not have a right of abode, indefinite leave to enter or remain in the United Kingdom

[Back to Top](#)

24.6 Attendance for fingerprinting

Normally, those subject to fingerprinting should be fingerprinted immediately so that fingerprint results are known when considering service of papers and detention. However, under section 142 of the 1999 Act, they may be required to attend at a specified place for fingerprinting. (Note also that the person must be given a period of at least seven days in which to attend). Where this is necessary, form IS 96 (or equivalent) should be used. Those who fail to comply may be arrested without warrant by a police constable or IO (unless the requirement has ceased to have effect). Before such a person is released, they may be moved to a place where their fingerprints can be taken.

Note. In family cases with a child under the age of five years, a note should be placed on the appropriate Restricted content- to remind the reporting centre officer that once the child has reached five years of age, they should be fingerprinted as soon as possible. In these circumstances, officers should bear in mind our policy on children and reporting. If it is possible for members of the local family team to fingerprint the child during an invited family returns process meeting or a welfare visit, using a mobile fingerprinting kit, this is to be preferred to the setting up of a required one-off reporting event. Should the family be reported

and confirmed as missing at a later stage, our fingerprint records will be the best means of identification for the Missing Persons Bureau, who will lead the investigation to trace the family.

[Back to Top](#)

24.7 Destruction of fingerprints

Section 143 of the 1999 Act (as amended) requires that if they have not already been destroyed (see below), fingerprints must be destroyed before the end of 10 years beginning with the day on which they were taken.

If it is proved that an individual is a British citizen or a Commonwealth citizen who has the right of abode in the UK as a result of section 2(1)(b) of the 1971 Act, fingerprints must be destroyed as soon as reasonably practicable.

Fingerprints taken from a dependant must be destroyed when fingerprints taken from the person whose dependant he is, have to be destroyed.

It is the responsibility of IFB to destroy fingerprint records within the specified time period or upon notification.

[Back to Top](#)

24.8 Procedures for fingerprinting

Take fingerprints as soon as possible after it is established that a person and any dependants is/are liable to be fingerprinted.

Fingerprints may be taken in enforcement offices, which have the correct facilities, or in a police station (this has been agreed with the police). IOs must not take fingerprints for immigration purposes on police live-scan units as this process does not record results on the IABS database. Its use is solely for the searching or

verification of those fingerprints on IABS. A separate set of fingerprints will need to be taken on an IFB1 for immigration purposes and processed as detailed below:

- tell the applicant that they are to be fingerprinted and explain that it is normal procedure
- where prints are being taken under section 141 of the 1999 Act, give them form IS86 which explains their liability to be fingerprinted
- fully complete the written details on form IFB1 (do not use any other form) including the reason for taking fingerprints and if they are required for a EURODAC search and the EURODAC category
- check fingerprint quality and that form IFB1 has been completed correctly. If fingerprint quality is inadequate destroy and take another set
- do not make or keep copies of the IFB1
- transmit the set of fingerprints to the IFB via a 'cardscan' workstation if available and send the IFB1 to the IFB as soon as practically possible. If there is no access to a 'cardscan' workstation send the form by internal post or 1st class recorded delivery immediately, or at the latest, within 24 hours to:

The Immigration Fingerprint Bureau (IFB),
5th Floor, Lunar House,
40, Wellesley Road,
Croydon, CR9 2BY

Restricted – do not disclose – start of section

The information in this page has been removed as it is restricted for internal Home Office use only.

Restricted – do not disclose – end of section

[Back to Top](#)

24.9 Taking fingerprints for identification purposes only

Where a person is detained under paragraph 16 of schedule 2 to the 1971 Act*, fingerprints can be taken under paragraph 18(2) of schedule 2 to the 1971 Act. This power should only be exercised where it is necessary to positively identify the offender. Fingerprints taken using this power will be checked against existing records, not to create a new record. Fingerprints should be taken on either form IFB1 or a Morpho RapID unit. Local files should be minuted to the effect that a search has taken place and the result.

IFB1s should be sent to IFB for searching with a clear indication that they have been taken under paragraph 18(2) of schedule 2 to the 1971 Act so that they can be processed appropriately and deleted when necessary.

Paragraph 2(4) of schedule 3 to the 1971 Act states: 'In relation to detention under sub-paragraph (2) or (3)... paragraphs 17 and 18 of schedule 2 to this Act shall apply as they apply in relation to detention under paragraph 16 of that schedule.'

*Paragraph 16(2) of schedule 2 to the 1971 Act (as amended), states that if there are reasonable grounds for suspecting that a person is someone in respect of whom directions may be given under paragraphs 8 to 10 or 12 to 14 of schedule 2 to the 1971 Act, they may be detained pending:

- a decision whether or not to give such directions
- their removal in pursuance of such directions.

Where a person is fingerprinted under either the powers in the 1971 Act or the powers in the 1999 Act, you are required to comply with the relevant parts of the PACE Codes of Practice provisions on fingerprinting as modified by the Immigration (PACE Codes of Practice No 2 and Amendment) Direction 2000.

[Back to Top](#)

24.10 Requesting checks with other agencies

Section 20 of the Immigration and Asylum act 1999 allows for information held by the police to be supplied to the Secretary of State for the purposes of immigration control. Fingerprints of foreign nationals routinely taken for enforcement purposes should therefore be searched through IDENT 1 where one of the following criteria are met:

- anyone who has made an asylum claim in their own right
- a dependant, aged at least 6 years of age, of a person who has made an asylum claim
- anyone who has had an enforcement decision served on them (for example, service of IS151A part 2 or IS151B)
- anyone who is refused leave to enter at port
- anyone who is taken to police custody
- anyone who has consented to their fingerprints being checked

Officers with access to Cardscan/Livescan can request that fingerprints are also searched against the police database (IDENT1) via that system. Note that all asylum seekers over the age of 16 are routinely searched against IDENT1, although the check requires this to be manually verified on the livescan/cardscan at enrolment. If the search results in a positive match against the police database, an automatic email response will be returned to the requesting officer's or team's mailbox. On receipt of a PNC200 request form, the PNC report will be emailed out by the IFB to a PNC authorised officer on a specific email box. You will be automatically emailed any 'no match' results. Any other request, such as a search via Interpol or a foreign immigration service, must be authorised by a CIO and made through the IFB in the first instance.

[Back to Top](#)

24.11 Use of force when taking fingerprints

Section 146 of the 1999 Act states that an IO exercising any power conferred on him by either the 1971 Act or the 1999 Act may, if necessary, use reasonable force. However, IOs must not exercise their power to use reasonable force unless they have been trained in its use. Only those IOs designated to exercise the existing power of arrest and the powers of entry, search and seizure are suitably trained. Non-designated IOs must rely on the police to take fingerprints where the use of force is necessary to take fingerprints or where it has been assessed that there is a realistic threat of violent behaviour, but only with the authority of a police inspector.

In line with guidance at [chapter 45.15](#) force may only be used on a pregnant woman, child or young person to prevent harm to themselves or another person. Force must not be used to take their fingerprints.

[Back to Top](#)

24.12 Requests for expert statements for prosecution of fraudulent applicants

Fingerprint experts will prepare and forward to the relevant crime intelligence team expert witness statements for all prosecution cases. The request should be made direct to IFB by email to the [IFB Mail box](#) (poise) giving full details of both identities used by the applicant.

Note. Fingerprint experts will only prepare statements if they have hard copies of the IFB1 form for both identities. It is therefore imperative that all IFB1 forms are sent to IFB as soon as possible. In the case of an urgent request for a statement where the IFB1 form is still at the port/enforcement office, please courier the form to IFB.

[Back to Top](#)

24.13 Fingerprints for documentation purposes

The process for the taking of fingerprints for documentation purposes can be

found under modernised guidance at [fingerprints for documentation purposes](#).

[Back to Top](#)

24.14 Fingerprinting of corpses

For health and safety reasons, under **no** circumstances should officers agree to fingerprint corpses using the Morpho RapID equipment, or lend the equipment for police officers to use themselves.

Police officers who require post mortem prints to be checked against the IABS database should take them themselves, using ink and card or a police digital unit, and submit them to the IFB. They must contact IFB before they submit the fingerprints.

Any queries regarding fingerprinting should be made to the IFB:

Restricted – do not disclose – start of section

The information in this page has been removed as it is restricted for internal Home Office use only.

Restricted – do not disclose – end of section

[Back to Top](#)

Revision history

Date change published	Officer/Unit	Specifics of change	Authorised by;	Version number after change
		OEM revision		24 v1
1-4-2008		Amendment to section – removal of reference to IS 86A	Julia Dolby	V2.0
30-6-08		Update from previous OEM Nov 07	Judith Craig	v3.0
		Update following new equipment; RapID		V4.0
29-7-2010	PSE	Review of v4, plus removal of Asylum guidance (24.16-24.18) & Hyper linking		V5.0
23-4-2013	EROP	Updating of RapID instructions	Sonia Dower, Director OPRU	V6.0
27-11-2013	EROP	Review of restricted material. Restrictions apply at: 24.6; 24.8; 24.14	Kristian Armstrong, Director, IBPD	V7.0