Home Office

International and Immigration Policy Group (IIPG)
2 Marsham Street
London SW1P 4DF

020 7035 4848 (switchboard)

www.gov.uk/home-office

Amit Hidri
request-222368-7d85f956@whatdotheyknow.com

13 January 2015

Dear Mr Hidri

FOI Request 32457

Thank you for your further request for information regarding all guidance held by the Home Office relating to biometric data – in particular, we have interpreted your request to mean how biometrics are collected, and the measures taken to ensure that it is securely stored and maintained and then destroyed in line with data protection obligations. Your full request can be viewed at **Annex A**. This response covers biometric guidance held centrally within the Home Office including those used by the police and those used for immigration and nationality purposes.

It is possible that some additional biometric guidance is held locally, but I wish to inform you that it may exceed the cost limit under section 12 of the Freedom of Information Act (FOIA) 2000 for us to identify and retrieve any such guidance. Your request was not entirely clear about what you required. Any requests for checks made by the Office of the Information Commissioner should be made direct to the Information Commissioner's Office.

You also may be interested to note that additional information relating to biometrics including fingerprints and DNA can be found via the publications link on the gov.uk website

You may recall that we wrote to you in our letter dated 29 August in which we explained that we needed additional time to consider your request under the exemption at section 35 of the FOIA. After further consideration it was decided that there were no grounds to withhold any information within scope of your request under this exemption, but that there are grounds to withhold some information under the exemption at section 31 – Law enforcement. Further explanation of this exemption can be found below.

There is published guidance available on Gov.uk and legislation.gov.uk that sets out how biometric information should be taken, used and retained. The various pieces of legislation set out how and

when biometric information may be used. The published guidance which is available online reflects the legislation and is used by staff and members of the public.

The legislation and guidance about taking, retaining and using biometric information varies depending on whether that are required for immigration and nationality purposes, or in relation to the prevention, detection or investigation of a crime.

Biometrics taken by police purposes

In respect of biometrics taken by police services, the main piece of legislation governing the retention of biometrics by the police is the Protection of Freedoms Act 2012 (specifically sections 1-25). When a person is arrested, a sample of their DNA and their fingerprints are taken. Where they are convicted of an offence, and under certain other circumstances, these are retained on the fingerprint database (IDENT1) and the National DNA Database (NDNAD).

Protection of Freedoms Act 2012 also establishes the post of the Commissioner for the Retention and Use of Biometric Material ('the Biometrics Commissioner') who, upon receipt of an application by the police, has the power to allow the retention of DNA and fingerprints taken by the police where a person has been arrested for but not charged with a qualifying offence where these would normally fall to be destroyed. Overall governance of policy on DNA is provided by the National DNA Database Strategy Board which was put on a statutory basis by section 24 of Protection of Freedoms Act 2012.

Because the scope of your request is very wide, we have limited our response to a search of emails and personal and corporate filing belonging to the Police, Science and Technology Unit. The trawl has revealed a number of items which I am able to disclose. These are as follows:

- Flowchart showing the application procedure to the 'Biometrics Commissioner' for retention of DNA and fingerprints and for applications to (Annex A)
- Guidance showing the application procedure to magistrates' and Crown Courts to extend retention for a further 2 years beyond the period granted by the Biometrics Commissioner (Annex B)
- Flowchart and questions and answers for police forces in relation to the implementation of sections 1-25 of Protection of Freedoms Act 2012 (Annexes C & D)
- Flowcharts showing the fingerprint retention process (Annexes E & F)

There is correspondence between Ministers and the Information Commissioner's Office about the Protection of Freedoms Act 2012, however we are not prepared to disclose this information as it relates to policy development.

There are also a number of documents which are already in the public domain which we believe answer the questions that you have posed. These are as follows:

- The Protection of Freedoms Act 2012
- Access and use of DNA samples profiles and associated data
- Protection of Freedoms Act 2012: DNA and Fingerprint provisions which explains the provisions of the Act
- Information for police forces on making an application to the Biometrics Commissioner to retain a person's DNA and fingerprints
- Annual Reports produced by the National DNA Database Strategy Board which provide details on the storage and destruction of DNA profiles
- Minutes of the proceedings of the National DNA Database Strategy Board some of which cover the issues you have asked about
- Reports published by the National DNA Database Ethics Group which consider any ethical issues arising from the sampling and retention of DNA

- Guidance on access and use of DNA profiles, samples and associated data
- Police and Criminal Evidence Act 1984 Code of Practice D, issued under the Act, which provides guidance to police officers on the identification of individuals and includes information on the taking, searching against existing records and destruction of DNA and fingerprints

Section 21 of the Freedom of Information Act 2000 exempts the Home Office from having to provide you with this information, because it is already accessible to you by other means (already in the public domain).

Arguments in favour of disclosure:

Disclosure of the documents in question would enable you to understand the exact processes that a police officer needs to take to ensue that a record held on the Police National Computer complies with the retention regime established under Protection of Freedoms Act or ensure that biometrics taken for immigration or nationality purposes are properly retained and used.

The police guidance would also enable you to have a better understanding of "Operation Nutmeg"; a police operation that was carried out to take DNA samples from a number of individuals who had been convicted of sexual offences but who had not had been sampled at the time. Disclosure would demonstrate our commitment to transparency around police processes.

Arguments against disclosure:

The documents under consideration contain information that, were it to be released into the public domain, risks allowing an individual to undermine the police investigation of a suspect, including any subsequent prosecution. Releasing information on a police operation risks providing criminals with intelligence that could allow them undermining of subsequent police operations.

Immigration and nationality biometrics

Turning to biometrics provided for immigration and nationality purposes, these are governed by different legislation, which the Acts which are still current in relation to biometric powers are set out below.

- The Immigration Act 1971
- The Immigration and Asylum Act 1999
- The Nationality, Immigration and Asylum Act 2002
- Asylum and Immigration (Treatment of Claimants, etc.) Act 2004
- Immigration, Asylum and Nationality Act 2006
- UK Borders Act 2007
- Borders, Citizenship and Immigration Act 2009
- Immigration Act 2014

There are statutory instruments and orders made under these various pieces of legislation which can be found on legislation.gov.uk, that set out the powers to take, use and retain biometric information for immigration and nationality purposes.

Guidance to British citizens and foreign nationals about providing biometrics can be found on Gov.uk, and is linked to guidance about applying for passports, immigration and nationality products. I have not listed them here as there are many types of applications where the provision of biometric information is a requirement.

However, I have attached the links to our staff guidance about taking biometrics which is online:

- Modernised guidance for how UK Visas and Immigration manages an applicant's biometric information.
- Immigration Enforcement - Chapter 24 – Fingerprinting/taking fingerprints/powers
- Fingerprinting foreign national offenders (FNOs)
- Photographing
- UK Visas and Immigration guidance for refusing applications because of unfavourable biometric hits
- Criminal casework - Biometric data sharing - fingerprint matching
- Biometric passports and passport readers
- Biometric Residence Permits
- Non-compliance with the biometric registration regulations

Section 21 of the Freedom of Information Act 2000 exempts the Home Office from having to provide you with this information, because it too is already accessible to you by other means (already in the public domain).

I can confirm we engage regularly with the Information Commissioner's Office when developing guidance and policy. I can confirm there is correspondence between the Home Office and the Office of the Information Commissioner about biometrics taken for immigration and nationality purposes, however as it relates to public policy development arising from the Immigration Act 2014 we are not prepared to release it. The items immigration documents we are prepared to show are as follows:

- Extract of the Immigration and Asylum Biometric System (IABS) Security Operating Procedures (SyOPS) IFB Users (Annex G)

Access to the biometric data is protected by unique access so that only those entitled to access such information are able to do so.

I can confirm that the Home Office holds additional guidance relating to biometric data. This covers how biometric information is processed on databases. However, following the consideration outlined below we consider that these items should be exempted under sections 31(1)(a), (b) and (e) of the Freedom of Information Act 2000. These provide that information can be withheld where disclosure would or would be likely to prejudice:

(a) the prevention or detection of crime,
(b) the apprehension or prosecution of offenders; and
(e) the operation of the immigration controls.

The FOI Act provides a right of access to information, and such information should be released wherever possible; however, it would clearly not be appropriate for all information to be made public. This is recognised by "exemptions" in the FOI Act. Some of the exemptions in the FOI Act are 'absolute', meaning that information can be withheld without considering any public interest in disclosure.

However the majority of the exemptions in the FOI Act are 'qualified' and subject to a public interest test (PIT).

This PIT is used to assess the balance of the public interest in disclosure against the public interest in favour of withholding the information; or the considerations for and against the requirement to say whether the information requested is held or not. The 'public interest' is not the same as what interests the public. In carrying out a PIT we consider the greater good or benefit to the community as a whole.

The ‘right to know’ must be balanced against the need to enable effective government and to serve the best interest of the public. The Act is ‘applicant blind’. This means that we cannot, and do not, ask about the motives of anyone who asks for information.

In providing a response to one person, we are expressing a willingness to provide the same response to anyone, including those who might represent a threat to an individual or to the UK.

Arguments in favour of disclosure:

The immigration guidance would enable you to understand the exact processes an officer of the Immigration Fingerprint Bureau follows to process biometric information provided for immigration and nationality purposes.

Disclosing the whole of the IABS Security Operating Procedures (SyOPS) IFB Users would show you the safeguards for keeping biometric information safe.

Arguments against disclosure:

Disclosing all of the immigration fingerprint guidance may risk our ability to control our border and prevent immigration abuses and expose how we use biometrics taken for immigration and nationality purposes to prevent, detect and prosecute crime.

Disclosing all of the Immigration and Asylum Biometric System (IABS) Security Operating Procedures (SyOPS) IFB Users may undermine our security procedures for keeping the biometric data safe.

Some of the information you have requested contains personal details, such as names, which are exempt from disclosure under section 40(2) of the Freedom of Information Act 2000

Section 40 of the Freedom of Information Act 2000 exempts personal data from disclosure if its release would breach any of the ‘data protection principles’ of the Data Protection Act 1998.

Conclusion

Therefore, after careful consideration of both sides of the argument, we consider that the public interest is against releasing these documents to you.

If you are dissatisfied with this response you may request an independent internal review of our handling of your request by submitting a complaint within two months to the address below, **quoting reference 32457**. If you ask for an internal review, it would be helpful if you could say why you are dissatisfied with the response.

Information Access Team
Home Office
Ground Floor, Seacole Building
2 Marsham Street
London SW1P 4DF
e-mail: info.access@homeoffice.gsi.gov.uk

As part of any internal review the Department's handling of your information request will be reassessed by staff who were not involved in providing you with this response. If you remain dissatisfied after this internal review, you would have a right of complaint to the Information Commissioner as established by section 50 of the Freedom of Information Act.

Yours sincerely

J Allen
International and Immigration Policy Group (IIPG)