Home Office

General Instructions
Immigration Removals, Enforcement and Detention

Data sharing in enforcement cases: standards of operational practice

Version 1.0

Contents

About this guidance

This guidance tells Immigration Enforcement officers about the different aspects of data sharing. It also tells them the standards that cover procedures to support the drive to stop people staying in the UK illegally and to generate the ‘hostile environment’ for persons of interest.

Contacts

If you have any questions about the guidance and your line manager or senior caseworker cannot help you or you think that the guidance has factual errors then email Enforcement Policy.

If you notice any formatting errors in this guidance (broken links, spelling mistakes and so on) or have any comments about the layout or navigability of the guidance then you can email the Guidance Rules and Forms team.

Clearance and publication

Below is information on when this version of the guidance was cleared:

- version 1.0
- published for Home Office staff on 15 July 2016

Changes from last version of this guidance

Have made changes to reflect the Immigration Act 2016

Related content

Contents

Disclosure of enforcement data

This page tells Immigration Enforcement officers about the legislation that specifies when and how personal data may be disclosed or shared. It also tells them about the role of the Interventions and Sanctions Directorate in the use of personal data.

Outline of legal issues

Personal data is defined as 'information that can identify a living individual' and any disclosure of personal data must meet the conditions in the Data Protection Act 1998, the Human Rights Act 1998 and the common law duty of confidentiality. The legal definitions of personal data are also extended to include sensitive personal data, information that requires a higher duty of care.

The Data Protection Act 1998 (DPA)

The Data Protection Act governs the processing of personal data based on 8 data protection principles and ensures that data is processed fairly, lawfully and for a legitimate purpose.

Under the 8 DPA principles, data must be:

- processed fairly and lawfully
- processed for limited, specifically stated purposes
- processed in a way that is adequate, relevant and not excessive
- kept accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the EEA without adequate protection

It also includes the right for an individual to access data about themselves using a subject access request. Subject access requests are usually dealt with by the Subject Access Request Unit (SARU). If, however, a request for personal data is received in writing and can be responded to easily, (eg a request for a letter already sent or a copy of an interview) then the business unit should deal with that request. If the request is more complex or information might need to be redacted, then forward it to SARU without delay.

In accordance with the DPA the Home Office has 40 calendar days to process a request and it is therefore important that the business unit responds to file requests from SARU as quickly as possible. Unnecessary delays can result in the Home Office being in breach of the Data Protection Act.

Human Rights Act 1998 (HRA)

Under the Human Rights Act any sharing of personal data must be **proportionate** to the legitimate aim. Whether a disclosure is proportionate will depend on the circumstances of each case.

For example, if the police/other government departments (OGD) request the personal details of a Home Office subject to further their enquiries, it would not necessarily be proportionate to respond to that request by sending complete copies of all of the Home Office files on the individual concerned. Instead the information provided should reflect the information that is required. The requester is only entitled to be told what they need to know for the purpose of their request.

When information is requested from an OGD or a third party the reason for the request must be ascertained so that you can consider whether disclosure is justified.

Published guidance for Home Office staff on the disclosure of information from OGDs/public bodies and third parties can be found in Disclosure of information. Guidance specific to OGD requests can be found in 01.0 - Introduction and Legal Background.

Freedom of Information Act 2000 (FOI)

Personal data must not be disclosed under the Freedom of Information Act and any FOI requests must be registered with the central FOI team.

See also: Freedom of Information guidance.

Recording the disclosure of data or requests for data

You must always keep a full record of any information you request or are asked to share with other organisations, either with the information itself or in the appropriate casework system. If the case is particularly sensitive, you must refer to senior managers outlining what has been requested and why.

The role of the Interventions and Sanctions Directorate

The Interventions and Sanctions Directorate (ISD) forms part of Immigration Enforcement (IE) within the Home Office. IE's vision is to be a professional and trusted law enforcement organisation that drives cross-system action to reduce immigration abuse and maximise compliance. Inherent in being a trusted organisation is the ability to demonstrate consistent competence in decisions, actions, communications and use of resources.

IE's strategic objectives are:

- **protect:** strengthen our protection from immigration abuse
- **prevent:** stop people staying in the UK illegally or supporting immigration abuse
- **pursue:** taking action against immigration offenders
- **prepare:** improve our ability to reduce immigration crime

ISD contributes to all 4 of IE's strategic objectives, however the primary focus lies in the areas of protect and prevent. ISD do this by removing incentives for people to stay illegally in the UK, increasing compliance with the Immigration Rules and encouraging those who are here unlawfully to regularise their status or to leave. Specifically to:

- work with partners across government, public and private sectors to systematically remove incentives for people to stay illegally in the UK
- make it harder for those who do not have the appropriate status to access benefits and services

Referral to ISD

If you encounter a migrant who claims to be, or is suspected of being, in:

- receipt of free secondary NHS care
- receipt of HMRC or local authority benefits despite having no recourse to public funds (NRPF)
- possession of a driving licence despite having no status

you must refer the case to ISD, for guidance see: The role of the Interventions and Sanctions Directorate (ISD).

The team will then contact the relevant partner to progress the case.

Official – sensitive: start of section

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

Official – sensitive: end of section

Related content
Requests for personal information
Contents

Sharing immigration enforcement data with other government departments

This page tells Immigration Enforcement officers what powers they have to share personal data.

Statutory responsibilities with regard to children

The Home Office is required to engage and share information with other partners to safeguard and promote the welfare of children under statutory guidance. The following links provide comprehensive guidance on identifying and assessing the risk to children:

- Working together to safeguard children (for England and Wales) describes the role of specific agencies and their role in working together to protect children
  - it details the Home Office's statutory safeguarding responsibility and duty to work with and share information with other partners to safeguard and promote the welfare of children. (see chapter 2 section 38 of the guidance)
- Every child matters – change for children, jointly issued by the Department for Schools, Children and Families and Home Office (formerly UK Border Agency) under section 55 of the Borders, Citizenship and Immigration Act 2009, to explicitly encourage the Home Office and other statutory agencies to cooperate and share information in order to safeguard children (see sections 2.32 and 2.33 of the guidance)

Detention and escorting: safeguarding children describes the Home Office's duty to have regard to the need to safeguard and promote the welfare of children while ensuring the return of families with children.

Home Office powers to share immigration data

The Home Office as a Department of State headed by a Minister of the Crown will, in most cases, rely on its **common law power** to share personal data with OGD such as the Department for Work and Pensions (DWP), Driver and Vehicle Licensing Agency (DVLA) and other bodies. However, there are specific legislative gateways that enable certain data sharing to take place.

Section 21 of the Immigration and Asylum Act 1999 provides a statutory gateway for the supply of information, documents and articles by the Secretary of State to:

- the police
- the National Crime Agency
- HM Revenue and Customs (HMRC)

However, disclosures made under these sections must still comply with the Data Protection Act 1998 (DPA), the Human Rights Act (HRA), and where applicable, the common law of confidentiality (see Disclosure of enforcement data).

To note there are separate powers to share personal customs information under the Borders, Citizenship and Immigration Act 2009.

Data sharing: multi-agency public protection arrangements (MAPPA)

The Criminal Justice Act 2003 provides for the establishment of MAPPA (see Multi-agency public protection (MAPPA) cases) in each of the 42 criminal justice areas in England and Wales. These are designed to protect the public, including previous victims of crime, from serious harm by sexual and violent offenders. They require the local criminal justice agencies and other bodies to work together in partnership, including sharing data, in dealing with these offenders. See also: Investigation of criminal offences and assessing harm.

Referring cases for sanctions to be applied

Intervention and Sanctions Directorate (ISD) coordinates the process by which information is shared and sanctions applied where appropriate against those who have no right to remain in the UK. ISD takes action to restrict those who do not have the appropriate status to access benefits and services offered by various departments and agencies including; the National Health Service (NHS), local authorities, the Driver and Vehicle Licensing Agency (DVLA), Department for Work and Pensions (DWP) and HM Revenue and Customs (HMRC).

The process by which sanctions can be considered and applied depends on the correct use of special condition flags that ensures all staff dealing with migrants can quickly and easily identify where sanctions have been, or are being applied. This also enables staff to refer cases for revocation, curtailment or denial of benefits and services to ISD. ISD then tracks the progress of those subject to sanctions, through the immigration system to conclusion.

'Sanctions: refer case to Interventions and Sanctions Directorate' guidance provides information on referral of cases to relevant departments and agencies, including:

- National Health Service (NHS)
- Driver and Vehicle Licensing Agency (DVLA) and Driver and Vehicle Agency Northern Ireland (DVA (NI))
- Transport for London (TfL) Taxi and Private Hire Vehicle Licences
- HM Revenue and Customs (HMRC)
- Department of Work and Pensions (DWP)
- Construction Industry Training Board (CITB) for Construction Skills Certification Scheme (CSCS)
- Civil Penalty Compliance team (CPCT)
- CIFAS (anti-fraud organisation)
- Department for Education (DfE)
- Electoral Registration Office (ERO)
- No Recourse to Public Funds (NRPF) Connect

Related content
Managing information: Data sharing – Horizon
Contents

Requesting information from other organisations

This page tells Immigration Enforcement officers how to request personal data from other organisations.

The supply of information for immigration purposes

Section 55 of the Immigration Act 2016 amended the existing information gateway set out in section 20 of the Immigration and Asylum Act 1999 to enable the supply of information (including documents and articles) held by any public authority or someone acting on behalf of a public authority, other than some named exceptions, to the Home Office for immigration purposes.

It does not apply to information held by, and documents or articles which come into the possession of, the Crown Prosecution Service (CPS) in relation to HM Revenue and Customs (HMRC) information, in order to avoid duplication with the existing information gateway in section 40 of the UK Borders Act 2007.

A ‘public authority’ is defined as a person with functions of a public nature, but it specifically excludes:

- HMRC
- The Houses of Parliament
- The Scottish Parliament
- The National Assembly of Wales
- The Northern Ireland Assembly

or persons exercising functions in connection with those bodies’ proceedings

Definition of ‘immigration purposes’:

- the administration of immigration control under the immigration acts
- the prevention, detection, investigation or prosecution of criminal offences under those acts
- the imposition of penalties or charges under part II
- the provision of support for asylum-seekers and their dependants under part VI
- determining whether to impose, or imposing, penalties under section 15 of the Immigration, Asylum and Nationality Act 2006 (restrictions on employment)
- providing facilities, or arranging for the provision of facilities, for the accommodation of persons under section 4 of the act
- anything else that is done in connection with the exercise of a function under any of the immigration acts

Section S20(6) preserves the ability of the Secretary of State and the Crown to share data under existing common law powers.

Nothing in this section overrides any existing restriction on the disclosure of information however imposed (eg the Data Protection Act 1998, Regulation of Investigatory Powers Act 2000).

Duty to supply information

Section 55 of the Immigration Act 2016 inserted section 20A, into the Immigration and Asylum Act 1999. This imposes a duty on specified bodies to supply nationality documents to the Secretary of State when directed where the document relates to a person who may be liable to removal and that the document may facilitate removal.

Schedule A1 to the Immigration and Asylum Act 1999 (inserted by schedule 9 of the Immigration Act 2016) provides a list of public bodies to whom section 20A applies.

In this context, a nationality document is one that either:

- establishes a person's identity, nationality or citizenship
- indicates the place from which a person has travelled to the UK or to which a person is proposing to go

This duty only relates to a relevant document that is lawfully in the possession of the listed body and must not be used to require documents to be seized from people on behalf of the Home Office or to help locate illegal migrants.

No time limit is given for supplying the document, the legislation only states that this should be done as soon as practical. Where the person holding the document needs it to perform their official functions, they may supply a copy provided that they forward the original as soon as practicable.

Asking for information: how to make a request for information from OGDs and public authorities

All requests for personal data must be specific to the case or individual that is under investigation, and must set out the reasons for the request and what information is required. The more information you provide the more likely it is that a positive response will be received from the other organisation.

To make requesting information easier the Home Office has agreed a number of memoranda of understanding (MoUs) with OGDs. They provide guidance on which powers to use, set out the process for making a request and provide standard forms that must be used.

Making a request

Always give as much information as you can, with enough detail so that the organisation can identify the person. Set out exactly what you need to know and why you need it, so they can be sure that it is lawful to share with you. If you are using a standard template, fill out all required sections on the form. Otherwise, you must clearly set out:

- as much information about the person you are interested in as possible, for example:
  - full name
  - date of birth
  - gender
  - nationality
  - address (if required)
- what specific information you are requesting (you must not just ask what they can tell you about the person)
- what you need the information for
- security marking (which in most cases will be Official)
- deadline for response - this is especially important if you require the information for a court case

Requiring a nationality document

Before requiring a document from a body listed in schedule A1 of the Immigration and Asylum Act 1999, (as inserted by schedule 9 to the Immigration Act 2016), you need to ensure that you have reasonable grounds to believe that the (all apply):

- specific body is in possession of a nationality document
- individual to whom the document relates is a person who may be liable to removal from the UK in accordance with the immigration acts
- document may facilitate their removal

Reasonable grounds to believe means knowledge which is objective, clear and based on specific facts, information or intelligence.

If the document is in hard copy form and the person possesses the original document, it must be supplied unless it is required for the performance of that body's functions (eg a prosecution) in which case a copy must be supplied.

If the listed body says they do not have a nationality document in their possession then there is no further action to take.

Specific organisation requirements

Department of Work and Pensions (DWP), police and Maritime and Coastguard Agency

There are MoUs in place with these organisations that set out the processes that should be followed for requesting information. Further information on approaching other public bodies and supporting MoUs can be found at the section 'Memoranda of understanding with OGDs'.

See: Checking details with DWP.

HM Revenue and Customs (HMRC)

Section 40 of the UK Borders Act 2007 provides a statutory gateway to allow HMRC to share data with the Home Office for immigration and nationality functions as set out in the legislation:

- administering immigration control under the immigration acts
- preventing, detecting, investigating or prosecuting offences under those acts
- determining whether to impose, or imposing, penalties or charges under part 2 of the Immigration and Asylum Act 1999 (c. 33) (carriers' liability)
- determining whether to impose, or imposing, penalties under section 15 of the Immigration, Asylum and Nationality Act 2006 (c. 13) (restrictions on employment)
- providing facilities, or arranging for the provision of facilities, for the accommodation of persons under section 4 of the Immigration and Asylum Act 1999
- providing support for asylum-seekers and their dependants under part 6 of that Act
- determining whether an applicant for naturalisation under the British Nationality Act 1981 (c. 61) is of good character
- determining whether, for the purposes of an application referred to in section 41A of the British Nationality Act 1981, the person for whose registration the application is made is of good character:
  - determining whether, for the purposes of an application under section 1 of the Hong Kong (War Wives and Widows) Act 1996, the woman for whose registration the application is made is of good character
  - determining whether, for the purposes of an application under section 1 of the British Nationality (Hong Kong) Act 1997 for the registration of an adult or a young person within the meaning of subsection (5A) of that section, the person is of good character
- determining whether to make an order in respect of a person under section 40 of the British Nationality Act 1981 (deprivation of citizenship)
- doing anything else in connection with the exercise of immigration and nationality functions.

This gateway provides a legislative basis for the disclosure of personal information but any sharing must still accord with the DPA, HRA and, where appropriate, the common law duty of confidentiality.

There is an MoU with HMRC which sets out the standard process that must be followed for making an information request.

See: Checking details with HMRC.

General Register Office (GRO) sham marriage

From 2 March 2015 Register Offices have a legal requirement to refer notifications of all marriages involving a non-EU national who may gain an immigration advantage by marrying. Reports under section 24 of the Immigration and Asylum Act 1999 are now automatically linked to notices referred by registrars.

In cases where a sham marriage is suspected the Home Office can extend the notice period from 28 days to 70 days so that further investigations can take place. In cases where no further action is required, the referring Register Office is notified that the couple can marry after 28 days. In cases where further action is considered necessary, the notice period will be extended to 70 days to allow for further enquiries to be made.

Official – sensitive: start of section

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

Official – sensitive: end of section

Please note also that Registrars are local authority employees and **do not** work directly for GRO, National Records of Scotland (NRS) or General Register Office Northern Ireland (GRONI).

The duty under section 20A of the Immigration and Asylum Act 1999 to supply nationality documents to the Secretary of State upon request is in addition to the existing duties on registrars to report suspicious marriages and civil partnerships.

Department of Health, NHS trusts and GP surgeries

When using section 20A in seeking to require nationality documents from health bodies listed in schedule A1, this should be a last resort to be used after other means to obtain the relevant documents have been exhausted.

A request for other information can be made under section 20 of the Immigration and Asylum Act 1999 for immigration purposes, or under section 29 of the Data Protection Act 1998 for the investigation, prevention and detection of crime.

Local authorities

In addition to sections 20 and 20A of the Immigration and Asylum Act 1999 (see above), section 129 of the Nationality, Immigration and Asylum Act 2002 provides a legal gateway requiring that local authorities provide certain information for the purpose of locating a person that is reasonably suspected of having lived in the local authority's area, and of having committed one of the following offences under the Immigration Act 1971:

- illegal entry (section 24(1)(a))
- overstaying (sections 24(1)(b)(i) and 24(1)(c))

- failing to observe a condition of leave or temporary admission (including restrictions imposed under schedule 3 of the Immigration Act 1971) (under sections 24(1)(b)(ii) and 24(1)(e)
- disembarking from removal (section 24(1)(f))
- deception (section 24A(1))
- making false representations to an immigration officer (section 26(1)(c))
- creating or possessing false documentation (section 26(1)(d))

For further guidance on the operation of this procedure, see 03.1 - Guidance to local authorities and housing authorities.

All other requests would likely be under section 29 of the Data Protection Act 1998 for the investigation, prevention and detection of crime. There is no central point for obtaining information from local authorities. Approaches may be made to those sections of individual authorities dealing with housing, housing benefit or student awards. Not all authorities will be willing to disclose information to the Home Office and therefore it is very important that the request clearly explains the statutory power and why the information is requested and how it will assist with the investigation.

See: Checking details with local authorities.

Private sector coercive powers

Section 135 of the Nationality, Immigration and Asylum Act 2002 requires a financial institution to supply information about a person if the Secretary of State reasonably suspects that the:

- person has committed an offence under section 105(1)(a), (b) or (c) or section 106(1)(a), (b) or (c) of the Immigration and Asylum Act 1999 (support for asylum-seeker: fraud)
- information is relevant to the offence
- institution has the information

Section 134 Nationality, Immigration and Asylum Act 2002 requires employers to provide information about an employee whom the Secretary of State reasonably suspects of having committed an offence under:

- section 24(1)(a), (b), (c), (e) or (f), section 24A(1) or section 26(1)(c) or (d) of the Immigration Act 1971 (c. 77) (illegal entry, deception etc)
- section 105(1)(a), (b) or (c) of the Immigration and Asylum Act 1999 (support for asylum-seeker: fraud)
- section 106(1)(a), (b) or (c) of the Immigration and Asylum Act 1999 (support for asylum-seeker: fraud)

Under this act a requirement to provide information under section 134 or 135 must be imposed by notice in writing specifying the:

- information required
- manner in which it is to be provided
- period of time within which it is to be provided (minimum 10 working days)

A person on whom a notice is served under this legislation must provide the Secretary of State with the information specified in the notice or face imprisonment or a fine.

Section 139 nationality and Asylum Act 2002 provides that information provided by a person under section 134 or 135 is not admissible in evidence in criminal proceedings against that person.

Related content
Contents

High volume data sharing

This page tells Immigration Enforcement officers about the sharing of high volumes of personal data with Home Office partners.

The purpose of high volume data sharing

The high volume data sharing programme's priority is to embed systematic and large scale data matching arrangements with partners where appropriate so they can make informed decisions on whether to deny, revoke or terminate access to benefits and services. This contributes towards the 'hostile environment' which makes it harder for people to live and remain in the UK illegally.

The programme also works to build awareness and ensure that partners have robust systems and processes in place to protect benefits and services from immigration abuse and increases compliance with the rules.

Additional information may subsequently be received back from partners where there is a confirmed match. This could include new and potentially more up-to-date contact details/addresses for individuals, or identifying potential illegal employers.

Another priority for the programme is to ensure this information is available to Immigration Enforcement and UK Visas and Immigration (UKVI) colleagues to aid case progression, support the civil penalty regime and issue fines against liable employers where appropriate.

Related content

Contents

Documentation: data sharing agreements

This page tells Immigration Enforcement officers what legal, technical and security considerations they must make before sharing large volumes of personal data.

See also: Memorandum of understanding

Data sharing toolkit

When sharing a large amount of protectively marked (including personal) information held by the Home Office with any third party, there are a number of legal, technical and security considerations which must be made. The Corporate Security Directorate designed the data sharing toolkit (toolkit) to elicit information in order that an informed decision at the appropriate level can be made in respect of the proposed data sharing activity.

To complete a toolkit, the key issues that must be addressed are (all apply):

- all parties must be clear on the tangible benefits that are expected from the sharing, who will receive them and how they will be measured
- the purpose of the sharing needs to be linked to one or more of the Department's strategic objectives
- the sharing must be physically and/or technically possible and be compliant with the Data Protection Act 1998, Human Rights Act 1998 and any other legal obligations and requirements

For the purposes of the toolkit, major or large scale data sharing is activity amounting to over 1,000 records either singly or cumulatively over a 12 month period. As a general rule of thumb, anything above this threshold requires the senior information risk owners (SIRO) approval, whilst anything below can be authorised by the information asset owner (IAO).

However, there will be circumstances when the number threshold is not met, but SIRO sign-off would still be appropriate, such as:

- issues relating to national security
- a particularly sensitive or high profile or risk recipient, or case where direct access to the department's IT systems is requested

In these cases the toolkit will need referral to the Home Office SIRO. IAOs may also choose to seek SIRO approval where they deem the sharing activity though small, to be sufficiently noteworthy because either:

- it stands to reap an extraordinary amount of benefit or enhancement of the department's reputation
- where the IAO is unsure of the level of risk

Privacy impact assessment

A privacy impact assessment (PIA) is a process which helps assess privacy risks to individuals through the collection, use and disclosure of information. The PIA forms part of the wider assessment (along with the data sharing toolkit and adequacy assessment where applicable) in deciding whether to proceed with any data sharing activity.

The PIA will set out how a memorandum of understanding (MoU) can be expected to relate to the privacy of the individuals, whose information is exchanged, including the overall adequacy of the data protection arrangements.

In most instances of large scale data sharing a PIA will not be required in addition to a data sharing toolkit as the majority of the privacy aspects of data sharing will be contained with the toolkit. However, as part of the toolkit process consideration must be given as to whether or not the exchange warrants a PIA in addition to a toolkit. That decision will be made in consultation with the data sharing and protocols team who own the data sharing toolkit process.

Adequacy assessment

An adequacy assessment is only used when sharing data outside of the European Union (EU).

The eighth principle of the Data Protection Act states that:

> ‘Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.’

The EEA includes Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom.

This principle prevents the transfer of personal data outside of the EEA unless either the:

- receiving country ensures an ‘adequate level of protection’ for the rights and freedoms of data subjects in relation to the data processing
- eighth data protection principle does not apply, by virtue of one of the conditions in schedule 4 of the Data Protection Act being met

One of the conditions in schedule 4 of the DPA is where the transfer of data is necessary for reasons of substantial public interest, such as to prevent and detect crime. However, as a matter of policy, an adequacy assessment must be completed as the final instrument, to determine if any data sharing activity can proceed.

The European Commission has decided that certain countries have an adequate level of protection for the transfer of personal data. Currently, the following countries are considered as having adequate protection: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. An adequacy assessment is not needed for these countries, **except** in the case of Canada as the European Commission's adequacy finding is for personal data in the private sector only.

In the US, although the European Commission has approved the Safe Harbor scheme it is not currently in operation. The scheme is designed to allow the free flow of personal data from EEA data controllers to US organisations which have joined the scheme, it does not apply to Government departments. Any data sharing with the US requires an adequacy assessment.

Related content
Contents

Memorandum of understanding

This page tells Immigration Enforcement officers about the memorandum of understanding (MoU) and how to create one.

MoU is the Home Office preferred term for a ‘data sharing agreement’ although other parties may use the phrases such as information sharing agreement (ISA). They are non-legally binding documents that record ‘commitments’ between 2 or more participants. MoUs are the most common data sharing agreement when the exchange is likely to occur on **multiple** or **regular** occasions.

All systematic and large scale data sharing activity must be supported by formal written agreements between those parties engaged in the activity. These agreements are referred to as MoU or (within HM Revenue and Customs (HRMC)) data usage agreement (DUA).

When entering into regular data sharing activities with other government departments (OGDs), an umbrella MoU must be drafted which is a high level formal, non binding agreement and sets out the high level data sharing principles governing the exchange of information between the 2 departments.

Umbrella MoUs must contain the following information as a minimum:

- description of the parties involved
- purpose of agreement
- details of security and legal assurances
- financial consideration
- Freedom of Information Act 2000 (FOIA), Data Protection Act 1998 (DPA) and Human Rights Act 1998 (HRA) obligations
- conditions of termination or review

Process or supplementary MoUs

Any new information exchange specific (‘process level’) agreements will require separate process or supplementary MoUs and must reference the umbrella MoU as the basis for the exchange and as a minimum include:

- details of the legal basis under which the exchanges are taking place
- any restrictions on the use of that information (such as whether it can only be used for specific purposes or restrictions on onward disclosure)
- details of the physical data transfer method
- details of exactly what data is being transferred between parties
- the purpose for which the data is being transferred
- relevant contact points within each party’s organisation

For more information see: Requests for personal information (data protection).

Memoranda of understanding with OGDs

To facilitate data sharing the Home Office has agreed various memoranda of understanding regarding data exchange with many OGDs and agencies including:

- HM Revenue and Customs (HMRC)
- Department of Work and Pensions (DWP)
- Gangmasters Licensing Authority
- National Police Chiefs' Council (NPCC) (previously Association of Chief Police Officers (ACPO)), concerning criminal record requests
- NHS Protect, concerning NHS fraud
- multi-agency public protection arrangements (MAPPA)

These agreements contain agreed procedures and constraints for the exchange of data, the circumstances in which data may be shared and points of contact within the respective bodies where requests can be made.

You must consult Share information or respond to requests for information and the appropriate MoU, where applicable, on disclosure before responding to a request for the information from a third party.

Extensive information concerning how and when to request or share data with other government departments can be found in Data sharing. The webpage links to guidance on requesting information from HMRC and DWP. It also provides advice on accessing and using Experian (Guidance on Experian charges and licence application) and details of current agreements with other organisations.

If you have questions on these MoUs then email Data Sharing team.

Creating a memorandum of understanding

The MoU must include the following sections.

Introduction

This section helps the reader to understand the agreement content. In particular, this section will:

- fully identify all the participants
- briefly state the background of and the rationale for pursuing the arrangement
- reference any existing relevant agreements between participants

Purpose and scope

This section explains the intention of the new or proposed capability that makes the MoU necessary. It explains how the participants will use the new capability and under what circumstances. In particular, this section will:

- outline why information needs to be shared
- describe the work to be accomplished
- specify the extent of the MoU

Benefits of the data share to the parties to the MoU (optional)

This section lists the benefits of the exchange to all parties involved and where appropriate, the wider general public or central government.

Procedures for the exchange of information
This section describes circumstances under which the capability can be used. In particular, this section will:

- outline how the participants will request information, ie in writing, and include any exceptional circumstances
- ensure the receiving participant justifies a request for information disclosure
- state whether a participant may spontaneously disclose information to the other participant or participants
- define roles of officials and points of contact

Information which may be exchanged
This section will:

- list the information to be exchanged in relation to a person, goods, service or other
- state the conditions and restrictions of the information exchange
- highlight any restrictions on information sharing

Limitations of use
This section limits the scope of any further disclosure.

Security and safeguards
This section assigns responsibility to the participants to ensure standard operating procedures for the capability are followed. In particular, this section will:

- fully establish the obligations of participants to control, safeguard and protect sensitive information and assets, including physical transfer of information
  - it also explains what must happen if any 'failures' occur
- describe provisions and use of sensitive information, the use of other than official government to government channels, and procedures in case of disclosure of sensitive information and/or assets

Consultation
This section describes the conditions for a consultation to occur. In particular, this section will:

- clarify how and under what circumstances a consultation takes place
- establish that the participants need to notify each other of any changes which could affect the MoU

Performance management reporting, reviews and audits
This section describes how compliance is carried out. In particular, this section will:

- agree to review, on an on-going basis, the usefulness of the MoU and report on the volume of exchanges of information

- establish a review period
- establish a provision to be audited

Financial arrangements
This section outlines:

- training arrangements
- funding arrangements
- auditing arrangements

It is recommended to state if there are no specific financial implications.

Legal disclaimer
This section clarifies that the MoU is not a legally binding agreement.

Amendment and dispute resolution
This section describes how updates are made to the MoU and how disputes are resolved. In particular, this section will:

- set forth the procedure for amending the MOU and/or its supplements which requires mutual consent
- address the means of resolving disputes between the participants

Retention and destruction schedule
This section describes how the data will be stored, protected and accessed by the receiving body and that it is consistent with the information's government security classification (GSC).

As a rule, personal data processed for any purpose should not be kept for longer than is necessary for that purpose. If there are to be different retention periods for different data sets these should be detailed.

This section also describes how the data will be destroyed when no longer in use. When data is no longer needed, it is the responsibility of the unit to ensure the data is destroyed securely. This is usually in accordance with each department's retention and destruction policies. Details should be included within each MoU.

Duration, withdrawal and termination
This section confirms any expiry date and describes the conditions for withdrawing and terminating the MoU. In particular, this section will:

- specify the duration of the MoU
- provide for the participants' termination of the MoU by unanimous consent
- provide for the conditions under which the participant may withdraw
- state which sections of the MoU (if any) remain in force when a participant withdraws, or termination or expiration

Effective date and signature
This section will:

- establish the date on which the MoU will come into effect for each participant
- specify whether the MoU will come into effect only after all of the participants have signed or as soon as a specified number of the participants have signed
- specify the titles of the individuals who are authorised to sign the MoU, ensuring the appropriateness and comparable ranking of the participants
- specify the languages used in the MoU

Annexes
This section includes, but is not limited to:

- definitions of terms used in the MoU
- document review control
- escalation points and business contacts

Data usage agreement

A data usage agreement (DUA) is a non-legally binding document which records ‘commitments’ between 2 or more participants. DUAs are normally prepared when the data sharing exchange is likely to occur on **one occasion** with **HMRC** only. This is the most common data sharing agreement in place for proof of concept (PoC) exercises.

A DUA will contain most of the information required within an MoU, except it will usually give specifics around the volume of the exchange rather than the duration of the agreement.

Related content
Contents

Enforcement data sharing and storage

This page tells Immigration Officers where and how they must record personal data. It also tells them the standards to meet when sharing data.

All data shared with others must be done using a secure route (such as over the government secure intranet (GSI)), both to and from the Home Office as there are significant volumes of personal and sensitive information involved. Information received back as a result of sharing, needs to be stored securely and must not be retained for longer than is necessary for the purpose it was obtained.

Data storage locations

The location of the storage will be dependant upon each agreement, but options include CID, data sharing hub (DASH) and shared folders on the shared drive (not personal drives).

CID

CID is an official government database to which access is only given to members of staff who have appropriate security clearance and need to use the system to carry out their job.

The Home Office stores personal (and sometimes sensitive) information on CID about individuals. It is a database used across all in-country case working to manage and process applications made by foreign nationals. It holds details of all applications currently being processed, as well as completed applications.

The data held on CID can be requested through a subject access request or the Freedom of Information Act. As a result, the database is monitored constantly and all actions on there can be traced.

CID is a case centric system. An individual can have multiple cases on CID but there should only be one person record for each individual. Every person is given a unique identifier, known as the CID ‘per ID’.

All activity on a case must be recorded onto CID. Activity undertaken by Interventions and Sanctions Directorate (ISD) is usually recorded in the special conditions screen. Flags include:

- ISD DVLA Match
- ISD HMRC Match
- ISD HMRC B&C Revoked
- NHS Treatment Case
- ISD NHS Debtor
- NRPF Supported
- I & S D interest

DASH

ISD utilises a data hub called DASH (data sharing hub), which was developed, and is maintained by, Managing Integrated Data Application Solutions (MIDAS) to assist with the monthly data exchanges with other government departments and mitigate the risks that are associated which may lead to data protection act (DPA) or memorandum of understanding (MoU) breaches.

DASH was designed to control the flow of data that is shared on a monthly basis. It also records results that are received back so that the information can be shared with the rest of the business, ie caseworkers can use the information to support robust decisions.

Due to the personal data held in DASH, access is limited to those that work in the Bulk Sharing team and members of ISD who are required to produce an extract for our partners. Currently 7 members of ISD have access to DASH and one member of MIDAS, who receives data and leads on development of the system.

DART

DART (data retrieval tool) is a look up tool provided for Home Office internal partners (casework areas) as a way to view the data held on DASH. Caseworkers need the CID ‘per ID’ of an individual whose data has been shared to access the relevant data. Cases in DASH can be identified using a special condition flag on CID (for confirmed matches only) which refers caseworkers to DART to check if the data may help them progress their case. DART also provides an audit function which allows ISD to audit users and those undertaking random searches.

Data sharing with partners: standards

All exchanges of data must be managed and co-ordinated as a project. This ensures all parties understand what the objectives, requirements, responsibilities and timescales are.

Identification of a project

What this standard means:
In the interests of ensuring consistency and high quality, the bulk data sharing programme must have oversight of all proposed data sharing projects. This will ensure that involvement is sought from an early stage from key teams, especially MIDAS and the Data Sharing and Protocols team.

How to apply the standard:

1. When a new idea or project is identified, the ISD member of staff leading must email ISD data sharing request inbox or enter the details onto the ‘data sharing request spreadsheet’ held on the shared drive. The information required will be:

    - details of the partner/other government department
    - what data is going to be shared
    - what the primary purpose/benefit will be
    - which strategic objectives it supports

- proposed timescales

2. The Bulk Data Sharing team will discuss the concept with MIDAS and the Data Sharing and Protocols team as appropriate and confirm whether it meets business requirements, is justified under the relevant legislation (including Data Protection Act 1998 (DPA) and Human Rights Act 1998 (HRA)) and is proportionate. Historical records will be consulted to ascertain whether an agreement already exists.
3. The group will consider and recognise other potential bodies that may need to be consulted prior to any form of bulk sharing, eg anything WI related would require explicit WISDO board agreement.
4. If agreed, the bulk data sharing team will provide support and/or lead (whichever is applicable) the project, providing a central point of contact for MIDAS and the Data Sharing and Protocols team. An assessment will be done to ascertain if a privacy impact assessment (PIA) and/or adequacy assessment (AA) is also required. If rejected, a full reason will be provided as to why.

How to measure the standard:

Every data sharing project will:

- be known about and documented as an agreed project by the bulk data sharing team or work planning committee
- adhere to the data sharing protocols for the Home Office
- be fully documented with a full, cleared toolkit and signed MoU
- contribute towards ISD and Immigration Enforcement strategic objectives
- does not duplicate other agreements or facilities

Proof of concept

What this standard requires

When exploring new projects or new ways of working or data sharing with other government departments (OGDs), or private companies, a proof of concept exercise must be completed to test whether the data exchange will meet the objectives required for all participants, is proportionate and delivers value.

How to apply the standard:

1. Once the principle has been agreed with the bulk data sharing team, a toolkit, DUA/MoU and project plan must be produced.
2. Timescales must be agreed with all parties involved, particular consideration will need to be given to the time and resource required by all teams involved where data needs to be collated, extracted or ‘washed’ against Home Office databases.
3. Regular meetings must be held with all participants to ensure effective communication and keep the project on track. Any alterations required to the project plan must be made following this consultation.
4. Communication plans must be prepared by the project lead (whether that be the data sharing team or another nominated individual in ISD) to ensure the relevant business areas are aware of the exercise and can assist with the

analysis. Depending on the exercise aims, the business areas may also be involved in identifying the data to be exchanged (eg priority cases).
5. Once the data has been shared and analysed, a full evaluation report should be produced to consider whether the objectives were met and if the exchange is worth doing on a regular basis.

How to measure the standard:

Every proof of concept exercise will:

- be fully documented so that it is clear what the objectives are, how they will be achieved and when
- be supported by detailed, authorised and signed data sharing agreements as required (dependant on size, method and data involved)
- be delivered on time
- deliver clear, tangible results for the business
- have a documented evaluation to justify decisions on whether to introduce into business as usual or not

Regular exchanges

What this standard requires:

When establishing a regular exchange, the main objectives will have been identified and key relationships built through the initial proof of concept. However, as well as ensuring the exchange is fully documented, the project will also need to consider the full impact on the business and how results will be communicated as business as usual.

How to apply the standard:

1. Once the proof of concept has been completed and proposals to incorporate a regular exchange has been authorised, a new toolkit, MoU (process or supplementary depending on what else is already in place) and project plan must be produced.
2. Timescales must be agreed with all parties involved, particular consideration will need to be given to the time and resource required by all teams involved where data needs to be collated, extracted or ‘washed’ against Home Office databases.
3. The project lead must produce process maps in collaboration with partners to document how the exchange will be managed and who will be involved at each step.
4. The project lead must prepare communication plans to ensure the relevant business areas are aware of the exchange and will be prepared to utilise any useful information received to progress cases. Any new instructions or guidance required should be drafted in consultation with the relevant business areas.
5. The project lead or board must give consideration as to how the business is notified of any matches made or new information. Should this require changes

to CID (eg new outcomes or flags), change requests must be submitted as early as possible to prevent unnecessary delays.

6. Once implementation has occurred, the project and ISD senior management team (SMT) must give consideration on how to report results and include these details on the weekly dashboard.

How to measure the standard:

Every regular data exchange will:

- be supported by a full audit trail to demonstrate testing, evaluation and justification for the regular exchange
- be fully documented so that it is clear what the objectives are, how they will be achieved and when
- be supported by detailed, authorised and signed data sharing agreements as required (dependant on size, method and data involved)
- be delivered on time
- deliver clear, tangible results which aids case progression and contributes towards the hostile environment
- be reported on in the weekly dashboard

Related content
Contents