How your personal information is used within the borders, immigration and citizenship system

Last updated 25 May 2018.

Contents

Introduction 2
How we protect your personal information 2
How we gather and use your personal information 2
Which other organisations have access to your personal information 6
Automated decision-making and profiling 7
Data transfers outside of the European Economic Area 7
Contacting you using your personal information 7
How long we keep your personal information for 7
How to get a copy of your personal information 8
How to complain 8

Introduction

Personal information supplied or collected for the purposes of entering or leaving the UK, securing the border, making an application for a visa, leave, settlement, citizenship or other immigration service, claiming asylum or other form of protection, or gathered as part of the process of securing the border or enforcing immigration laws will be held and processed by The Home Office, which is based at 2 Marsham Street, London SW1P 4DF. The Home Office is the controller for this information. This includes when the information is collected or processed by third parties on our behalf.

Data protection law in the UK changed on 25 May 2018. This notice reflects your rights under the new laws and lets you know how we will look after and use your personal information. This includes what you tell us about yourself, what we learn about you as you engage with the borders, immigration and citizenship system, and what others share with us to fulfil their legal obligations or help prevent abuse of the immigration system and/or prevent and detect crime. It also covers what information we may share with other organisations.

The Home Office has appointed a data protection officer (DPO) to help ensure that we fulfil our legal obligations when processing personal information. The DPO can be contacted by emailing DPO@homeoffice.gsi.gov.uk.

How we protect your personal information

We have a duty to safeguard and ensure the security of your personal information. We do that by having systems and policies in place to limit access to your information and prevent unauthorised disclosure. Staff who access personal information must have appropriate security clearance and a business need for accessing the information, and their activity is subject to audit and review.

How we gather and use your personal information

We are only allowed to use, gather and share personal information where we have an appropriate legal basis to do so under the General Data Protection Regulations (GDPR) or the Data Protection Act 2018. The Home Office collects and processes personal information to fulfil its legal and official functions.

The legal basis for the processing of your data will, in most cases, be Article 6(1)(e) of the (GDPR) – that is, that the processing is necessary for the

performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

At points, for example in considering asylum claims and verifying your identity, we also process special categories of personal data on the basis of Article 9(2)(g) of the GDPR where the processing is necessary for reasons of substantial public interest. This may include information about political beliefs, sexual orientation, religious beliefs and biometrics.

We may also process personal data under Part 3 (law enforcement processing) of the Data Protection Act 2018.

Examples of ways in which we may gather your personal information include when:

- you travel to and from the UK
- you enter the UK by crossing the UK border, for example, an airport
- you make an application or claim (online, on paper or in person)
- you attend an interview
- we seek to verify your information, documents or identity
- you supply a biometric (for example, fingerprints or a facial biometric)
- we receive information from a sponsor or other third party in relation to your application
- we receive allegations or intelligence from law enforcement agencies and others involved in preventing crime and fraud
- we are notified of a relevant criminal conviction

We may also request information from third parties. For example, this might be for the purposes of verifying information you supplied in support of an application, obtaining information needed for a safeguarding purpose, obtaining new address details of people we are trying to trace, or undertaking other enforcement actions. This may involve, for example:

- contacting your sponsor or linked applicant
- obtaining information from other government departments – these may include HM Revenue & Customs (HMRC), Department for Work and Pensions (DWP), Department for Education(DfE), Driver and Vehicle Licensing Agency (DVLA), and Driver and Vehicle Standards Agency (DVSA)
- obtaining information from credit reference agencies, fraud prevention agencies (for example, Cifas) or banks, and local authorities

- seeking to verify documents, information, or identity in relation to your application – this may include private and public authorities in other countries
- local authority services (for example, social services)

The main ways we process personal information are given in the table below:

What we process and hold personal information for	**Examples of how we may use your data**
To process applications. These may include applications for visas, leave, settlement, citizenship, EU residence permits, extensions, renewals or transfers of conditions, and so on	• to verify your information, documents and identity • to engage with your sponsors, or other relevant individuals including dependants and responsible adults • to keep in contact with you • we may notify you when your period of leave is due to come to an end • to detect and prevent crime • to support enforcement operations • to ensure compliance with employment regulations • for safeguarding purposes • to support appeals and review processes
To decide claims for asylum and other forms of protection	• to confirm your identity and details of claims • to keep in contact with you while we process your application • to provide accommodation and financial support • for safeguarding purposes • to detect and prevent crime • for unaccompanied asylum seeking children, we may make family tracing checks provided this will not put you at any risk • to check with other countries to determine if your claim should be processed elsewhere • to support appeals processes

	Please note: we will not share any of your information with authorities in your country of origin if this would put you or your family at risk
To secure the UK border	• to control entry of people and goods subject to immigration and customs controls • to protect against threats to public security • to detect and prevent crime • to refuse carriers authority to carry individuals who are within the scope of the Authority to Carry Scheme 2015 • to develop risk and fraud profiles
To enforce UK immigration law, protect public security and prevent crime	• to promote voluntary return • to support removals and deportation • to plan and undertake enforcement operations • to prevent, detect and investigate crime • to enforce right to work legislation • to maintain the compliant environment • to develop risk and fraud profiles • for detention purposes • for safeguarding purposes
To safeguard and promote the welfare of children and adults	• to ensure that relevant authorities and services are able to provide support to vulnerable individuals and families • to support decisions on vulnerable people • to identify people at risk
To process your application to join a premium service such as the Registered Traveller Service or Electronic Visa Waiver, or to support applications to join Global Entry	• to decide your application • to keep in contact with you • to improve the service • we may notify you when your membership period is due to come to an end in order you may consider renewing

Which other organisations have access to your personal information

A number of organisations from the private, public and charity sectors are either contracted by, or subject to agreement with, the Home Office to provide functions in relation to the borders, immigration and citizenship system. To do this they may process personal data on our behalf and under our direction. Examples of these functions where we use other organisations in this way include:

- to support the visa process – we may use contractors to take payments, take biometrics on our behalf, to operate visa centres overseas, and print biometric residence permits
- to conduct customer experience research and operate customer contact centres
- to help provide services in relation to vulnerable people and those seeking protection – this extends from support for the processing of resettlement cases overseas, support for unaccompanied asylum seeking children, and the provision of helplines
- the operation of detention centres and holding facilities, and associated health services
- escorting services
- border processing

Which other organisations we share data with

We will also share data for law enforcement purposes and to prevent fraud and to assist other organisations in delivering their statutory functions. These include, for example:

- law enforcement agencies to support the prevention of crime, or for national security purposes – this may include international agencies, for example, Interpol, and national authorities
- organisations involved in the prevention of fraud – for example Cifas and credit reference agencies
- local authorities and charity organisations to assist them in delivering their statutory duties in particular protecting children and other vulnerable individuals in the community
- HMRC, DWP, and the NHS in relation to rights to access public services
- other government departments and agencies as necessary for them to deliver their statutory duties and public functions
- HM Courts and Tribunals Service in relation to appeals
- banks in accordance with the 2014 and 2016 Immigration Act provisions

Automated decision-making and profiling

Article 22 of the GDPR provides the right not to be subject to a decision made solely on the basis of automated processing which produces legal or other significant effects. Parts of our processing may involve degrees of automation, but complex or adverse decisions will always be taken by a trained officer or caseworker.

We may use personal information, for example from previous applicants, to develop tools that allow us to assess and then process applications in a particular way. This helps us to target our resources and ensure our processing is efficient, allowing us to minimise costs while protecting the public effectively. However, a case officer would still decide these cases. Any profiling must comply with our wider obligations under equality legislation.

Data transfers outside of the European Economic Area

We may transfer personal information to authorities or organisations in countries outside the European Economic Area. When we do, this will be for specific purposes. These may include, for example, validating aspects of your application, preventing or detecting of crime, including fraud, supporting returns or helping to identify or prevent those who may seek to enter or remain in the UK who may not comply with the conditions attached to their entry or leave to remain. When we do this, we seek to take appropriate steps to safeguard your information, for example by agreeing memoranda of understanding. We may rely on the derogation in Article 49(1)(d) of the GDPR where necessary.

Contacting you using your personal information

Beyond the normal processing of your application, we may use your personal information (for example, email address and mobile number) to send you prompts. For example, to remind you when your period of leave is coming to an end or to issue a renewal reminder in advance of the expiry of your membership of any premium passenger service, such as the Registered Traveller Service, to facilitate your renewal. In addition, we may use your details to seek feedback on the handling of your application to help us improve our services.

How long we keep your personal information for

We will keep your personal information for as long as it is necessary for permitted purposes. In the borders, immigration and citizenship system, we maintain a long-term record of immigration history and immigration offending

to support future decision-making and enforce penalties. Personal data will be typically retained for 25 years after a decision to grant settlement or naturalisation and for 15 years after the last action in other cases. Information on foreign national offenders may be retained until the death of the data subject. At the border, passenger name records data is retained for 5 years. Advance passenger information may be retained for 10 years. Arrest and detention records may be held for 6 years. We continue to keep retention periods under review to ensure they meet our role of securing the UK border and ensuring we can support those who are seeking to enter or remain in the UK.

However, it should be noted that the Jay Inquiry, which commenced in February 2015, has placed a moratorium on the disposal of all records throughout the Home Office, including all operational records and case files. This is currently in force and will remain so until further notice. It does not apply where there is a statutory requirement to delete data.

How to get a copy of your personal information

You can request your personal information.

Under the GDPR you also have the right to object to and ask to restrict our use of your personal information, and to ask us to rectify or delete your personal information. However, there may be a number of legal or other official reasons why we need to continue to keep or use your data. If you want to exercise these rights please write to us at the following address:

SARU
Home Office
40 Wellesley Road
Croydon
CR9 2BY

Or email us at: SubjectAccessRequest@homeoffice.gsi.gov.uk

How to complain

You also have the right to complain to the Information Commissioner's Office about the way we handle your information or respond to your requests for access to your personal information or the exercise of your other rights under the GDPR or the Data Protection Act 2018. Their contact details are as follows:

The Office of the Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Website: www.ico.org.uk