Immigration and Nationality Division of the Guernsey Border Agency

Fair Processing Notice

The Immigration and Nationality Division of the Guernsey Border Agency is responsible for managing foreign and Commonwealth immigration and nationality policy throughout the Bailiwick of Guernsey. The Division regulates the entry and stay of those people subject to immigration control under the various Immigration Acts, takes deportation action against those non-British citizens who are considered non conducive to the public good and provides, on behalf of the Committee for Home Affairs, a work permit system for non-European Economic Area citizens to meet the economic and high skill requirements of the Bailiwick.

The Division also deals with nationality matters such as the acquisition of British citizenship and the operation of the Bailiwick of Guernsey's passport office acting under the authority of the Lieutenant Governor who exercises the Royal Prerogative on behalf of the Sovereign.

The data controller with responsibility for delivering these services is the Guernsey Border Agency. The information that we request and collect is necessary in order to process and make decisions regarding the services that the Division is responsible for.

1. The Data Protection Law

The Guernsey Border Agency (GBA) acknowledges its obligations as per the Data Protection (Bailiwick of Guernsey) Law 2017, ('the Law'), which provides a number of requirements in terms of processing activities involving personal data. The controller further acknowledges the general principles of processing as well as the rights of a data subject and more information in relation to these provisions are provided within this fair processing notice.

2. The Principles of Processing

a. Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and in a transparent manner.

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.

We are only allowed to use, gather and share personal information where we have an appropriate legal basis to do so under the Data Protection (Bailiwick of Guernsey) Law 2017.

All personal data is collected and processed in a lawful manner in accordance with the Law. Schedule 2 (Conditions for Processing to be Lawful) of the Law provides a number of conditions to ensure that the processing of personal data by a controller is lawful.

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

- You make an application for a passport
- You corroborate an applicant’s identity on a passport application
- We require further information from you or a third party to support your application for a passport
- We seek to verify your information, documents or identity
- You supply a biometric (for example, fingerprints or a facial biometric)
- 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
- You make an application (online, on paper or in person)
- You enter the UK by crossing the UK border e.g. an airport or ferry port
- You travel to and from the UK
- Seeking to verify documents, information, or identity in relation to your application. This may include private and public authorities in other countries
- Seeking to verify information supplied by other States Of Guernsey departments such as Revenue Service, Social Security, Population Management and Law Enforcement

The type of information we require from you will depend on the application you are making but may include:

Personal details about you including general contact information, identity data, financial information, occupational data, your reasons for applying for visas, your travel history, where you intend to reside and details of the property (as necessary).

Details about your spouse/partner, parents, any dependent children you may have and information regarding your Sponsor and Countersignatory (as necessary).

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 settlement scheme status, extensions, renewals or transfers of conditions, etc.	• To verify your information, documents and identify • 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 offences • To support enforcement operations • To support enforcement with employment regulations • For safeguarding purposes • To support review process
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 • For safeguarding purposes • To support review process 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 Bailiwick of Guernsey border and borders of the Common Travel Area	• To control entry of people subject to immigration controls • To protect against threats to public security • To detect and prevent offences • To develop risk and fraud profiles
To enforce the Bailiwick of Guernsey Immigration Law, protect public security and prevent offences	• To prevent voluntary return • To support removals and deportation • Plan and undertake enforcement operations • To prevent, detect and investigate offences • To develop risk and fraud profiles • For detention purposes • For safeguarding purposes
To safeguard and promote 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 passport applications	• To verify your identity and nationality in order to make a decision on your passport application and assist in its delivery • For safeguarding purposes

We rely on two different lawful bases for processing personal data. Dependent on which application you are making. The two bases we use (and where you can find them within the Data Protection Law) are as follows:

Schedule 2, Part 2, 8: The processing is necessary for the controller to exercise any right or power, or perform or comply with any duty, conferred or imposed on the controller by an enactment.
Schedule 2, Part 2, 13(b): The processing is necessary for the exercise of any function of the Crown, a Law Officer of the Crown, the States or a public committee.

For an in-depth description of the exact data we require for each application, the lawful basis we rely on and the specific retention periods, please see Appendix 1 at the end of this document.

b. Purpose limitation

Personal data must not be collected except for a specific, explicit and legitimate purpose and, once collected, must not be further processed in a manner incompatible with the purpose for which it was collected.

The Guernsey Border Agency acknowledges its responsibility with regards to this data protection principle and therefore the controller maintains that it will not further process that personal data in a way which is incompatible to its original reason for processing as specified in section 2a, unless the controller is required to do so by law.

c. Minimisation

Personal data processed must be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed.

The controller maintains that it will only process the personal data which is detailed in section 2a, and will not process any further personal data that is not necessary in relation to the original reason for processing personal data as specified in section 2a, unless the controller is required to do so by law.

d. Accuracy

Personal data processed must be accurate, kept up-to-date (where applicable) and reasonable steps must be taken to ensure that personal data is inaccurate is erased or corrected without delay.

The controller will ensure that all personal data that it holds is accurate and kept up-to-date, and any personal data that is inaccurate will be erased or corrected without delay.

e. Storage limitation

Personal data must not be kept in a form that permits identification of a data subject for any longer than is necessary for the purpose for which it is processed.

The personal data will be retained in hard copy and electronic format for the following periods;

Application Type	Retention Periods
Passport application in paper form with any documents given in support	Adults: 11 years from date of determination Children: 6 years from date of determination
Electronic passport records held on Passport System Main Index	80 years from date of issue of passport
Failed/withdrawn passport applications	1 year

Lost or stolen British passport notification	GBA: 1 year Her Majesty's Passport Office: 80 years
Recovered passports sent to the Bailiwick of Guernsey Passport Office	If passport contains no evidence of fraud, it is cancelled on the passport system then securely destroyed unless the passport is handed in by a safe third party, when attempt to contact the holder will be made and the passport kept for 3 months. If not reclaimed, securely destroy If passport contains evidence of fraud, it is retained for duration of any subsequent criminal investigation
Failed or withdrawn passport applications	1 year
Naturalisation, Registration and EU/EEA/SWISS Settlement Scheme applications	Paper records -25 years from date granted Electronic records - Indefinitely
Indefinite leave to remain (ILR) applications	Paper records - 25 years from date leave granted or 6 months after naturalisation as British Citizen (if applied for) Electronic records - Indefinitely
Further Limited Leave to Remain; Work permits; Family Settlement Visa Applications; and Visa applications for work, study, dependents and youth mobility	5 years and 6 months from date leave granted
Visit visa applications	1 year
Deportation information	Paper records -20 years Electronic records – Indefinitely
Visa refusals	Paper records – 5 years 6 months from date refused Electronic records - Indefinitely

f. Integrity and confidentiality

Personal data must be processed in a manner that ensures its appropriate security, including protecting it against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The personal data will be held in hard copy and electronic format. Both formats will only be accessible by authorised personnel within the Guernsey Border Agency and security is in place to protect that data from unauthorized or unlawful processing and against accidental loss, destruction or damage.

g. **Accountability**

The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles. The controller and data protection officer contact details are provided below.

3. Contact Details

The contact details of the controller are as follows:

The Committee for Home Affairs

Tel: 01481 221420

Email: immigration@gba.gov.gg

The contact details for the Data Protection Officer of Home Affairs is as follows:

Data Protection Officer, the Committee for Home Affairs

Tel: 01481 220012

Email: data.protection@gov.gg

4. Data Subject Rights

a. Right of access

A data subject has the right to be advised as to whether a controller is processing personal data relating to them and, if so, that individual is entitled to one free copy of their personal data (with further copies available at a fee prescribed by the controller). This is known as a Subject Access Request (SAR). Upon receipt of an SAR, the controller has a period of one month to adhere to the request (an extension of two further months can be sought by the controller depending upon the complexity and number of requests submitted by the data subject).

b. Right to data portability

A data subject has the right to data portability, this means that an individual is able to arrange for the transfer of their personal data from one controller to another without hindrance from the first controller. This right can only be utilized where the processing is based on consent or for the performance of a contract. This right cannot be used for processing by a public authority.

Where a data subject invokes the right to data portability, the data subject has the right to be given their personal data in a structure, commonly used and machine-readable format suitable for transmission from one controller to another. Upon the request of a data subject, the controller must transmit their personal data directly to another controller unless it is technically unfeasible to do so.

c. Exception to right of portability or access involving disclosure of another individual's personal data

A controller is not obliged to comply with a data subject's request under the right of access or right to data portability where the controller cannot comply with the request without disclosing information relation to another individual who is identified or identifiable from that information.

d. Right to object to processing

A data subject has the right to object to a controller's activities relating to the processing of personal data for direct marketing purposes, on grounds of public interest and for historical or scientific purposes.

e. Right to rectification

A data subject has the right to require a controller to complete any incomplete personal data and to rectify or change any inaccurate personal data.

f. Right to erasure

A data subject has the right to submit a written request to a controller regarding the erasure of the data subject's personal data in certain circumstances. These include where:

- The personal data is no longer required in relation to its original purpose for collection by the controller;
- The lawfulness of processing is based on consent and the data subject has withdrawn their consent;
- The data subject objects to the processing and the controller is required to cease the processing activity;
- The personal data has been unlawfully processed;
- The personal data must be erased in order to comply with any duty imposed by law; or
- The personal data was collected in the context of an offer from an information society service directly to a child under the age of 13 years of age.

g. Right to restriction of processing

A data subject has the right to request, in writing, the restriction of processing activities which relate to the data subject's personal data. This right can be exercised where:

- The accuracy or completeness of the personal data is disputed by the data subject who wishes to obtain restriction of processing for a period in order for the controller to verify the accuracy or completeness;
- The processing is unlawful but the data subject wishes to obtain restriction of processing as opposed to erasure;
- The controller no longer requires the personal data, however the data subject requires the personal data in connection with any legal proceedings; or
- The data subject has objected to processing but the controller has not ceased processing operations pending determination as to whether public interest outweighs the significant interests of the data subject.

h. Right to be notified of rectification, erasure and restrictions

Where any rectification, erasure or restriction of personal data has been carried out, the data subject has a right to ensure that the controller notifies any other person to which the personal data has been disclosed about the rectification, erasure or restriction of processing. The controller must also notify the data subject of the identity and contact details of the other person if the data subject requests this information.

i. Right not to be subject to decisions based on automated processing

A data subject has the right not to be subjected to automated decision making without human intervention.

To exercise these data subject rights, please contact either the data protection officer or the controller (as per the contact details provided in 2g).

j. Right to make a complaint

An individual may make a complaint in writing to the supervisory authority (the Office of the Data Protection Commissioner) if the individual considers that a controller or processor has breached, or is likely to breach, an operative provision of the data protection law, and the breach involves affects or is likely to affect any personal data relating to the individual or any data subject right of the individual (as listed above).

k. Complainant may appeal failure to investigate or progress and may appeal determinations

An individual may appeal to the Court where:

- The Supervisory Authority has failed to give the complainant written notice that the complaint is being investigated or not within two months of receiving the complaint;
- The Supervisory Authority has failed to provide written notice of the progress and, where applicable, the outcome of the investigation at least once within three months of providing notice of the beginning of an investigation; or
- Where the individual seeks to appeal against a determination of the Supervisory Authority.