

**Policy Document**

How the British Indian Ocean Territory administration (“BIOTA”) protects *special category* *data* and *criminal offence data*: appropriate policy document.

Created 15 October 2024

The British Indian Ocean Territory has its own domestic laws, but these laws do not include any specific provisions which relate to data processing and data protection. As such, the BIOTA seek to apply, as far as possible in the unique circumstances of the territory, the spirit of the applicable laws in force in England and Wales. These are the UK General Data Protection Regulation and the Data Protection Act 2018, which require that data controllers provide information to people whose personal information they process. This includes having an Appropriate Policy Document to record their policies for processing *special category data* and *criminal offence data*. Processing information means how it is collected, used, stored, shared and destroyed.

This Appropriate Policy Document includes:

a. Who we are

b. What we mean by *special category data* and *criminal offence data*

c. What information we process

d. Which conditions we rely on

e. How we comply with the data protection principles

f. How long we keep your data for

g. How to contact us

h. How to make a complaint

a. Who we are

The British Indian Ocean Territory (“BIOT”) is a British Overseas Territory. It comprises over fifty uninhabited islands (the Chagos Archipelago) and is one of the most remote island groups in the world. Diego Garcia is the largest island of the Chagos Archipelago, which hosts a Joint UK/US military facility, pursuant to an agreement constituted by an exchange of diplomatic notes between the Governments of the United States of America (US) and the UK. It is a sensitive Joint UK/US military facility of significant strategic importance to both the UK and the US.

There is no permanent population on Diego Garcia and no right of abode in the territory. Ordinarily, the only persons present on BIOT are military personnel from the US and UK, public officers of the BIOTA, support staff for the defence facilities and occasionally visiting scientists. In effectively carrying out its administrative functions in relation to civilians who are present in the territory, BIOTA must collect, use, store and share *special category data* and *criminal offence data*.

b. What we mean by *special category data* and *criminal offence* *data*

*Special category* *data* is any personal information that can reveal your:

* racial or ethnic origin
* political opinions
* religious or philosophical beliefs
* trade union membership
* genetics
* biometrics
* health
* sex life
* sexual orientation

*Criminal offence data* is any information about a person’s criminal convictions, offences or related security measures. This can include suspicions and allegations of criminal offences or confirmation that they have not been committed. Security measures are penalties, conditions and restrictions imposed through the criminal justice system. They can also include civil measures that carry a criminal penalty for non-compliance.

c. What information we process

As an employer, we process *special category data* and *criminal offence data* about our staff and job applicants. This can include:

* information about race or ethnicity, religious beliefs, sexual orientation and political opinions
* trade union membership
* information about health, including medical conditions, health and sickness records
* genetic information and biometric data
* information on past criminal convictions

We also process *special category data* and *criminal offence data* in order to carry out the administrative duties required in relation to civilians who have arrived in the territory with or without prior permission and properly considering any claims made by such persons. This can include:

* health information
* your racial or ethnic origin
* information on your sex life or sexual orientation
* your political, religious or philosophical beliefs
* criminal offence data

Other instances where we may process *special category data* and *criminal offence data* include:

* health information you may provide when applying for a permit to visit the territory, for example accessibility and dietary requirements
* *criminal offence data* we may collect when conducting a central assurance or due diligence assessment

d. Which conditions we rely on

We aim to follow (UK) data protection law by documenting certain conditions we rely on to process *special category data* and *criminal offence data*. In doing so, we rely on the following conditions that require documentation in Schedule 1 of the Data Protection Act 2018:

* employment, social security and social protection
* statutory etc. and government purposes
* equality of opportunity or treatment
* racial and ethnic diversity at senior levels of organisations
* preventing or detecting unlawful acts
* protecting the public against dishonesty etc.
* regulatory requirements relating to unlawful acts and dishonesty etc.
* preventing fraud
* suspicion of terrorist financing or money laundering
* safeguarding of children and of individuals at risk

e. How we aim to comply with the (UK) data protection principles

The UK General Data Protection Regulation sets out seven principles to follow when processing personal data. We aim to comply with these principles in several ways when processing *special category data* and *criminal offence data*.

We aim to comply with the lawfulness, fairness and transparency principle by:

* ensuring that personal data is only processed where a lawful basis applies and where processing is otherwise lawful
* processing personal data fairly and ensuring that data subjects are not misled about the purposes of any processing
* ensuring that data subjects receive full privacy information so that any processing of personal data is transparent

We aim to comply with the purpose limitation principle by:

* only collecting personal data for specified, explicit and legitimate purposes and informing data subjects what those purposes are in a privacy notice
* only using personal data for purposes that are compatible with the purposes for which it was collected and informing data subjects if we use it for a new purpose

We aim to comply with the data minimisation principle by:

* only collecting the minimum personal data that we need for the purpose for which it is collected
* ensuring that the data we collect is adequate and relevant

We aim to comply with the accuracy principle by:

* ensuring that personal data is accurate and kept up to date where necessary
* taking particular care to ensure accuracy where our use of personal data has a significant impact on individuals

We aim to comply with the storage limitation principle by:

* only keeping personal data in an identifiable form as long as is necessary for the purposes for which it is collected or where we have a legal obligation to do so
* deleting personal data or rendering it permanently anonymous once we no longer need it

We aim to comply with the integrity and confidentiality principle by:

* ensuring that we have appropriate organisational and technical measures in place to protect personal data

We aim to comply with the accountability principle by:

* ensuring that records are kept of our personal data processing activities
* carrying out Data Protection Impact Assessments for any high-risk personal data processing
* appointing a Data Protection Officer to provide independent advice and monitoring of our personal data handling, ensuring that they report to the highest management level of the department
* implementing internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with data protection law

f. How long we keep your data for

We keep *special category data* and *criminal offence data* only for as long as it is necessary or for as long as we are legally required to do so. We retain and destroy personal data securely in line with general retention and disposal policies.

g. How to contact us

If you have any questions about this document, you can contact the Data Protection Officer, Robert Fairweather, at the Administration of the British Indian Ocean Territory:

Data Protection Officer

British Indian Ocean Territory Administration,

King Charles Street

London

SW1A 2AH

Email: [BIOTadmin@fcdo.gov.uk](mailto:BIOTadmin@fcdo.gov.uk)

h. How to make a complaint

You may also make a complaint to the Commissioner. He can be contacted at:

The Commissioner,

British Indian Ocean Territory Administration,

King Charles Street

London

SW1A 2AH

Email: [BIOTCommissioner@fcdo.gov.uk](mailto:BIOTCommissioner@fcdo.gov.uk)

Changes to this notice

We encourage you to reread this document occasionally as we aim to update it regularly, in order to keep you fully informed about how we use your personal information.

This document was created on 15 October 2024.