

Audit Advisory Division- Privacy Notice

Audit Advisory Division

Treasury, IOM Government

Prospect House

27-29 Prospect Hill

Douglas IM1 1ET

Email- Enquiries.Audit@gov.im

Treasury Data Protection Officer

Email- DPO-Treasury@gov.im

Telephone: 01624 686393

This notice is intended to inform you and help you to understand your rights as a data subject, when your personal data is being processed by the Audit Advisory Division of the Treasury.

How and why we process personal Data:

Personal data is data which is related to you, when you can be identified from that data or from that data when combined with other information available in the public domain, or as part of any work we perform. The definition of personal data includes any expression of opinion about you.

Audit Advisory Division (AAD) is a Division of Treasury, who is the controller, when processing personal data. In this privacy notice, where we refer to Audit Advisory, we are referring to this Division of Treasury. We will only use your personal data when the Data Protection laws of the Isle of Man allow us to do so. Most commonly, we will use your personal data in the following circumstances:

- Where it is necessary in order for us to carry out our statutory functions in the public interest or, in the case of special categories of personal data, for reasons of substantial public interest. Our audits and examinations help to scrutinise public spending, hold government to account, drive improvement in public services and protect the public against dishonesty. This work serves a substantial public interest.
- Investigations include:
 - **Financial Irregularities**- in accordance with the IOM Government Financial Regulations and IOM Post Office Financial Regulations, reports of Financial Irregularities must be reported via the S1 form. Information provided on the form is provided in confidence, and investigated under a statutory function in the public interest of

preventing or detecting unlawful acts and preventing the public against dishonesty.

Personal data may be collected as part of the report and/or investigation, and may be shared for the detection or prevention of crime. Audit Advisory Division processes data whereby individuals have raised concerns relating to, but not limited to: criminal activity; financial malpractice or fraud; financial mismanagement or corruption; material breaches of legislation; material risks to financial services; material breaches of regulatory standards; bribery; improper conduct or unethical behaviour, and will carry out an investigation accordingly.

- Under the **Whistleblowing** Policy, IOM Government Financial Regulations, IOM Post Office Financial Regulations and Employment Act 2006, Audit Advisory Division processes data whereby individuals have raised concerns relating to, but not limited to: criminal activity; financial malpractice or fraud; financial mismanagement or corruption; material breaches of legislation; material risks to financial services; material breaches of regulatory standards; bribery; improper conduct or unethical behaviour, and will carry out an investigation accordingly.
- Similar to Whistleblowing and Financial Irregularity investigations, personal data will be processed as part of an investigation following a report via the **Integrity Line**. The Integrity Line provides an easy process where IOM Government Employees can report instances of wrong-doing. Reports can be anonymous, but where provided, personal data of the reporter will be processed as part of the investigation. In addition personal data of individuals about whom allegations are raised within such reports will be processed as part of the investigation.

For example:

'Kate Martin raises an Integrity Line complaint alleging that her co-worker Samantha Ryan has duplicated expense claims for the last 6 months.' In this instance the personal data of the reporter and the individual about whom the allegation has been raised, will be processed.

Investigations may gather documentation and information from IOM Government Departments, Members of House of Keys and those involved in the subject matter of any investigation.

Personal Data will include but is not limited to: Officers name; Contact Details; Employment Roles; Correspondence concerning the matter; Opinions concerning the matter (including Interview Notes, Witness Statements and Written Submissions).

For the purpose of processing, Treasury is a Controller of personal data and the following are the legal reasons (in Article 6) which apply in respect of the subject matter of the investigation:

- 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;
- Processing is necessary for compliance with a legal obligation to which the controller is the subject.

Whilst we will endeavour for Special Category data to be anonymised, there may be circumstances where this is not appropriate. This data will be processed under the data protection legislation that applies in the Isle of Man, namely the Data Protection (Application of GDPR) Order 2018 (referred to as "the Applied GDPR"), Article 9,2((f) where the processing is necessary for the establishment, exercise or defence of legal claims) , and/or Article 9,2((g) processing is necessary for reasons of substantial public interest).

Where a submission to the Investigation is made in person via formal Interview, in writing via formal Witness Statement or Written Submission, the person making the submission will be identified in the final report which will be issued to the Designated Manager, being the Director of Audit Advisory of the Isle of Man Government, with intended onward distribution to other government entities.

Data collected as part of the investigation may be shared with other Designated Bodies as defined in the Treasury Financial Regulations and the Isle of Man Constabulary to ensure the completeness of the investigation.

Transfer of personal data to include transfers to any third party countries or international organisations is not anticipated.

Your data may also be shared when investigations require Audit Advisory Division to:

- Take legal advice in respect of the Investigation
 - Deal with queries or complaints in relation to the conduct of an Investigation
 - Report suspected or actual criminal activity
 - Make or respond to a legal complaint, claim or application, or comply with a legal obligation (including a court order).
- Sometimes, as part of an investigation, personal data may be processed under AAD's **Tender Appeal** process. This data is usually limited to the person who has requested the review, but may extend to the details of those who submit tenders, and any relevant data uncovered as part of the investigation.

Under 'FPN C.08 Tendering' of the IOM Government's Financial Regulations, AAD undertake tender appeal investigations. The appeal is directed to AAD through the powers assigned in Section 8(1) of the Treasury Act 1985, with AAD acting as an independent body suitable to undertake the investigation.

- Personal Data collected as part of an **audit** - sometimes, as part of our audit testing across IOM Government Departments, Statutory Boards and Offices, we require evidence that processes are being undertaken, this may include personal data, depending on the area of audit. Under Regulation 6(3) of The Accounts and Audit Regulations, 2018, and Section 8(1) of the Treasury Act 1985, the Division can be granted access to records for the purpose of the audit.

Whilst we will endeavour for Special Category data to be anonymised, there may be circumstances where this is not appropriate. This data will be processed under the Applied GDPR, Article 9,2)g.

Audit Advisory will not collect data directly from Data Subjects outside of the audit subject. Data will be anonymised where possible, and identifiable data will be collected on a minimal basis.

- Data Collection for **staffing purposes**. This may contain some special categories of data, including health and sickness information that employees choose to share, working hours, and Personal Development Reviews. We will always endeavour to minimise data collection to what is necessary, and we will only share data outside of the Department when it is required (OHR, PSPA, when there is a legal requirement to do so).

Please note that OHR collect employment data as part of the terms of your employment, more information can be found on their Privacy Notice (<https://hr.gov.im/privacy-notice/>).

Our legal basis for processing your information

In accordance with the requirements of the Applied GDPR, we will only process your personal information if there is a legal reason to do so.

The lawful basis of processing which apply to the work of the Audit Advisory Division include (ref-Article 6.1 Applied GDPR):

- Consent- The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- Contract- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering a contract;
- Legal obligation- Processing is necessary for compliance with a legal obligation to which the controller is subject to;

- 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;

We will also retain your information where there is a requirement for historical or archiving purposes by the Public Record Office under the Public Records Act 1999.

In accordance with Article 6(3) of the Applied GDPR, the basis for the processing referred to above is laid down by Manx law, to which the Audit Advisory Division is subject. The Manx law meets an objective of public interest and is proportionate to the legitimate aim pursued.

We may rely on:

- The need to meet an obligation in carrying out statutory government functions (including but not limited to the Audit Act 2006, the Accounts and Audit Regulations 2018, the Treasury Act 1985, IOM Government Financial Regulations, IOMPO Financial Regulations).
- Where it is necessary in order for us to carry out our statutory functions in the public interest or, in the case of special categories of personal data, for reasons of substantial public interest.
- The need to meet a request you have made for information or a service.
- The need to prevent or investigate suspected or actual violations of law.
- Contractual obligations.
- The need to retain information for historical or archiving purposes by the Public Record Office under the Public Records Act 1999.

Types of Personal Information we collect about you

Category of information	Examples of that type of information
Personal details	Name, email address, telephone number, address.
Employment details	Past, current and prospective employers, salary, pension scheme details, appraisal/ review documents.
Financial Information	Financial applications, accounts, invoices, tender documents, financial irregularity investigation documents.
Investigation data	Officer names, contact details, employment roles, correspondence, interview notes, written submissions, witness statements.

Government Identifiers	Driving Licence number, car registration, National Insurance number, tax reference.
Other Information	Feedback, comments, complaints, enquiries, Subject Access Requests.
Personal Identification Information	Title, Date of Birth, Nationality, gender.
Education and training details	Academic qualifications, training courses, CPD details.
Family, lifestyle and social circumstances	Dependents, marital status, next of kin and contact details, working hours, holidays.
Audit evidence	Dependent on audit topic- may contain personal data, in some instances may be special category data, including Health Data and Criminal Offence Data.

We may process certain special categories of information for specific and limited purposes during the course of an audit (particularly audits of Manx Care, Department of Education Sport and Culture, and IOM Constabulary).

How long do we keep your personal information?

We will only keep your information for the minimum time necessary. This may be to:

- Respond to an enquiry from you
- Confirm the transfer of information to the Department, Office or Board providing a service you have requested
- Meet Isle of Man Government Financial Regulations
- Meet statutory requirements
- For the purpose of an audit or investigation
- To analyse the use and quality of our services and to make improvements.

Records are only retained for longer term periods if their retention can be justified for statutory, regulatory, legal or security reasons, or for their historic value, but the standard retention period for records held is 6 years +1. Our Retention Schedule can be requested from the Data Protection Officer.

How we keep your information secure

The Isle of Man Government network drive folders are assigned with restricted access to officers within Audit Advisory to ensure that information is only visible to those who need access for the purposes of their job role. Servers are maintained by Cabinet Office,

Government Technology Services. Hard copy documents are kept in locked storage at Treasury Offices, as specified in Audit Advisory Division's Retention Schedule.

The security and confidentiality of your information is very important to us. We will ensure that:

- Safeguards are in place to make sure personal information is kept securely
- Only authorised staff are able to view your information
- Your personal information will not be disclosed to any third party without your prior consent or where required to do so by law.

We may share your information with or between other Government Departments, Statutory Boards and Offices to provide a service or information you have requested, where there are arrangements in place to do so. This may also be done for the purpose of an investigation into a financial irregularity, a whistleblowing report, a tender appeal, or for an investigation generated through the Integrity Line.

Your Rights

You have the right to:

Request access to your personal data (commonly known as a "Data Subject Access Request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. Please note that as part of the Isle of Man Government statutory functions some information may need to be retained. We will retain your information for the period required to fulfil the purposes set out in this Policy and when there is a legal obligation to do so. For the purpose of Investigations, it may be possible to revoke consent, however it cannot be guaranteed, as the data may be subject to onward disclosure.

Object to processing of your personal data where the processing is based on our exercise of our statutory functions in the public interest and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you

need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

The rights listed above are subject to some exceptions and limitations. If those are relevant when you ask to exercise your rights we will tell you.

If you are unhappy with the way we deal with your personal information you can submit a complaint to Treasury's Data Protection Officer who will work with you to resolve any issues.

Email: DPO-Treasury@gov.im

Telephone: [01624 686393](tel:01624686393)

Address: [Data Protection Officer](#)

[Treasury](#)

[First Floor, Central Government Offices](#)

[Prospect Hill](#)

[Douglas, IOM](#)

The [Isle of Man's Information Commissioner](#) is the independent authority responsible for upholding the public's information rights and promoting and enforcing compliance with the Island's information rights legislation. Further information can be found on the [Information Commissioner's website](#) (inforights.im).

You have the right to request the Information Commissioner to undertake an assessment as to whether the processing of your personal data has been carried out in accordance with the provisions of the Manx Data Protection Legislation, including the Data Protection Act 2018 and orders made under it, namely the Data Protection (Application of GDPR) Order 2018, the Data Protection (Application of LED) Order 2018, and the GDPR and LED Implementing Regulations 2018.

Requesting access to your personal information

Under the Applied GDPR you have a right of access to your personal data and to check the accuracy of that data by making a **Subject Access Request**.

A subject access request is made by contacting the [Data Protection Officer](#) (DPO) of the Department, Office or Board that collects the information.

To make a request of the DPO for Treasury contact:

DPO, Treasury
Financial Governance Division,
First Floor,
Central Government Offices,
Bucks Road,

Douglas,
IM1 3PX,
Isle of Man

Subject access requests must be responded to promptly and in any event within one calendar month.

You have the right to request the Information Commissioner to undertake an assessment as to whether the processing of your personal data has been carried out in accordance with the provisions of the Applied GDPR.

Will this Notice change?

This Privacy Notice may change. We will not reduce your rights under this Privacy Notice without your consent. If any significant change is made to this Privacy Notice we will provide a prominent notice on this website so that you can review the updated Privacy Notice.

This Privacy Notice may be replaced, or more information added, when you send feedback, ask to use a service online or make a payment for a service through our website. It will also be updated where there has been a change in processes within the Audit Advisory Division that includes personal data

This privacy notice was last updated in **March 2024**.