MBJ's Data Privacy Policy

Vision and Strategy

As the operator of Jamaica's largest international airport, MBJ Airports Limited ("MBJ" or "the Company") is committed to the safety and security of all Airport users and stakeholders. In compliance with the provisions of applicable laws and regulations, MBJ will only process personal data in accordance with the rights of the data subject while observing the principles of legality, consent, information, quality, purpose, accuracy, limitation and protection.

Data Protection Policy

It is necessary for MBJ to process personal data so that it can function effectively and successfully for the benefit of all Airport users and stakeholders. The security and management of such data must be undertaken in such a way that the privacy of each person who submits personal data to MBJ ("the data subject") is protected through the lawful and appropriate use and handling of their personal information.

The use of all personal data by MBJ is governed by the Data Protection Act of Jamaica ("DPA").

All employees and contractors with the Company have a responsibility to adhere to the Data Protection Principles outlined in the DPA and in this Data Protection Policy. Other relevant policies include the:

- Data Retention and Disposal Policy
- Information Technology Acceptable Use Policy
- Information Security Policy
- User Security Policy
- Incident Response Plan
- Privacy Notice and Privacy Policy
- Data Subject Access Request Policy

If you have a question about this Data Protection Policy or an area of concern about data protection matters, please contact MBJ's Data Protection Officer (DPO), Attention: DPO at dataprotection@mbjairport.com.

Standards for Processing Personal Data

There are eight (8) Standards for Processing Personal Data:

1. Fairness and lawfulness- Personal data must be processed fairly and lawfully and must not be obtained by deception or any misleading information.
2. Purpose limitation- Personal data must only be obtained for a specific and lawful purpose and must not be processed in any manner incompatible with those purposes.
3. Data minimization- Personal data must be adequate, relevant, and must only be limited to the purpose for which it is being processed. The data collected by MBJ must be relevant to the specified purpose it was collected for and must not be more than what is reasonably required.
4. Accuracy-Personal data must be accurate and, where necessary, kept up to date. MBJ will not be in breach of this standard if the inaccurate data was provided by the data subject or a third party, however, MBJ should take reasonable steps to verify the accuracy of the data.
5. Storage limitation- Personal data must not be kept for longer than is necessary and must be disposed of in accordance with the Act, if specified. This is, however, subject to any applicable retention periods prescribed by law. MBJ must inform the data

subject of the expected period of retention of their personal data, and this must be clearly set out in a privacy notice.

6. Rights of data subject - Personal data must be processed in accordance with the rights of the data subject. Some of these rights include the right to access the data and the right to prevent processing of the data in certain specified circumstances.
7. Implementation of technical and organisational measures- Personal data must be protected using appropriate technical and organisational measures so as to prevent unauthorised or unlawful processing of the data as well as any accidental loss or destruction of, or damage to, the data.
8. Cross-border transfers- Personal data shall not be transferred to a State or territory outside of Jamaica unless that State or territory ensures an adequate level of protection for the rights and freedoms of the data subjects in relation to the processing of personal data.

MBJ is committed to upholding the Data Protection Standards. All personal data under our control must be processed in accordance with these principles.

Personal data may only be considered lawfully processed:

- Where MBJ has the consent of the data subject
- Where it is in MBJ's legitimate interests and this is not overridden by the rights and freedoms of the data subject.
- Where necessary to meet a legal obligation.
- Where necessary to fulfil a contract, or pre-contractual obligations.
- Where MBJ is protecting someone's vital interests.
- Where MBJ is fulfilling a public task, or acting under official authority.

Where processing is based on consent, the data subject has the option to withdraw their consent easily and at any time. Where electronic direct marketing communications are being sent, the recipient should have the option to opt-out in each communication sent, and this choice should be recognised and adhered to by us.

Data Minimisation

Data collection processes will be regularly reviewed by the Data Governance Group to ensure that personal data collected and processed is kept to a minimum.

- MBJ will keep the personal data that its collects, use and share to the minimum amount required to be adequate for its purpose.
- Where MBJ does not have a legal obligation to retain some personal data, it will consider whether there is a business need to hold it.
- MBJ will retain personal data only for as long as it is necessary to meet its purpose. Our approach to retaining and erasing data no longer required will be specified in the retention policy and schedule. This schedule will be reviewed annually.
- In the case of sharing personal data with any third party, only the data that is necessary to fulfil the purpose of sharing will be disclosed.
- Anonymisation and pseudonymisation of personal data stored or transferred should be considered where doing so is a possibility.

Accountability

- The Data Protection Officer ("DPO") has the specific responsibility of overseeing data protection and ensuring that MBJ complies with the data protection principles and the DPA.
- The DPO will ensure that MBJ's regular processing activities are documented. Such documents shall be kept up to date and demonstrate how the data protection principles are adhered to by the Company's activities. Individual members of staff have a duty to contribute to ensure that the measures outlined in this policy are accurately reflected in the Company's practices.
- The Data Governance Group monitors MBJ's compliance with relevant policies and regulatory requirements in respect of data protection as part of the Company's Data Management Strategy. The Data Governance Group consists of the DPO, the Legal Counsel, the Chief Financial Officer, the Human Resource Manager, the IT Manager and the Security Manager.
- All employees, volunteers, consultants, partners or other parties who will be handling personal data on behalf of MBJ will be appropriately trained and supervised where necessary.
- The collection, storage, use and sharing of personal data will be regularly reviewed by the Data Protection Officer, the Data Governance Group, and any relevant business area.
- MBJ will adhere to relevant codes of conduct where they have been identified and discussed as appropriate.
- Where there is likely to be a high risk to individuals rights and freedoms due to a processing activity, MBJ will first undertake a Data Protection Impact Assessment (DPIA) and consult with the Office of the Information Commissioner (OIC) prior to processing if necessary.

Use of External Data Processors

- MBJ will only use or appoint external data processors that can provide sufficient guarantees around compliance with the DPA and that the rights of data subjects will be protected.
- Where an external data processor can demonstrate that they adhere to approved codes of conduct or certification schemes, this should be taken into consideration for choice of supplier.
- Where MBJ uses a processor, a written contract with compulsory privacy terms must be in place.

Organisational Measures

- All devices owned by MBJ will have hardware encryption set up by default where possible, including laptops, mobile devices and removable media.
- Physical documents containing personal data must be stored in locked filing cabinets with access only allowed to authorised personnel.
- All staff, contractors, temporary workers, consultants, partners or anyone else working on behalf of MBJ and handling personal data are bound by the DPA and this Policy.
- Where any contractor, temporary worker, consultant, or anyone else working on behalf of MBJ fails in their obligations under this Policy, they shall indemnify MBJ against any cost, liabilities, damages, loss, claims or proceedings that may arise from that failure.

The Role of the DPO

MBJ has chosen to do so as part of demonstrating its accountability and ensuring its compliance with data protection requirements.

- The DPO assists MBJ to:
    a) monitor our internal compliance
    b) inform and advise on our data protection obligations
    c) provide advice regarding Data Protection Impact Assessments
    d) act as a contact point for data subjects and the Information Commissioner's Office.
- The DPO advises the Data Governance Group and reports to MBJ's Executive Team on data protection matters.
- The DPO is easily accessible as a point of contact for staff for data protection issues and is identified as the point of contact in our privacy notice and other external material.
- The DPO identifies, organises and delivers training for staff and meets with new staff during their induction to discuss data protection matters, including this policy.
- The DPO is required to have appropriate knowledge of data protection law and best practice, and is provided with adequate resources to help them carry out their role. This might include appropriate training and accreditation where identified.
- The DPO is nominally responsible for carrying out responses to requests made by data subjects, reporting breaches and drawing up policies and procedures.
- This does not preclude another responsible member of staff for carrying out these duties.

PROCEDURES FOR STAFF

While this policy helps us to demonstrate how MBJ seeks to comply with data protection legislation and be accountable for our actions, all members of staff must comply with these procedures for processing or transmitting personal data. In addition, staff should be aware of and adhere to policies around the Acceptable Usage of IT Systems, and any other guidance issued in relation to cyber security and the use of personal data.

a) Always treat people's personal information with integrity and confidentiality. Don't hand out personal details just because someone asks you to.
b) Where personal data exists as hard copy, it should be stored in a locked box, drawer or cabinet, and not left where anyone could access it.
c) The transfer of hard copies should be passed directly to the recipient.
d) Staff are issued with encrypted USB devices for the secure transfer of personal data or sensitive information. No other removable media devices should be used to transfer these types of information without permission from the IT Manager.
e) The loss or theft of any device should be reported as soon as possible to the DPO, the IT Manager and the Security Manager.
f) Take care when connecting to public wi-fi connections, as these can

expose your connection to interception. If you're not sure if a connection is secure, do not connect to it.

g) Use marketing lists in CRM where appropriate. These can be used for follow up emails from a training session, or to send reminders prior to an event.

h) If you are thinking of sending marketing to individuals, consult with the DPO first, as there are certain laws that apply to electronic direct marketing. This could include anything that promotes the aims or purpose of MBJ, including promoting an event or seeking engagement.

i) Take care to email the intended recipient (especially where email address autocomplete is turned on). Use the 'bcc' field for emailing several people where using 'to' or 'cc' is not needed.

j) These procedures and policies also apply to the use of remote access to MBJ cloud systems. If you are using your own device to access personal data on Office365 (e.g. Outlook or Dynamics CRM), ensure that your device has a firewall and is password protected.

k) If you do have a question or are unsure about any of these procedures, contact the Data Protection Officer or the IT Manager.

RIGHTS OF DATA SUBJECTS

1. Under data protection laws, data subjects have certain rights:
   - **Right to be informed**. The right to be told how their personal data is used in clear and transparent language.
   - **Right of access**. The right to know and have access to the personal data MBJ hold about them.
   - **Right to data portability**. The right to receive their data in a common and machine-readable electronic format.
   - **Right to be forgotten**. The right to have their personal data erased.
   - **Right to rectification**. The right to have their personal data corrected where it is inaccurate or incomplete.
   - **Right to object**. The right to complain and to object to processing.
   - **Right to purpose limitation**. The right to limit the extent of the processing of their personal data.
   - **Rights related to automated decision-making and profiling**. The right not to be subject to decisions without human involvement.
2. MBJ will uphold individuals' rights under data protection laws and allow them to exercise their rights over the personal data MBJ hold about them. Privacy information will acknowledge these rights and explain how individuals can exercise them. Most rights are not absolute, and the individual will be able to exercise them depending on the circumstances, and exemptions may apply in some cases.
3. Any request in respect of these rights should preferably be made in writing to dataprotection@mbjairport.com.There is no fee for facilitating a request, unless it is 'manifestly unfounded or excessive',

in which case administrative costs can be recovered.

4. Requests that are 'manifestly unfounded or excessive' can be refused.

   A request may be manifestly unfounded if the individual clearly has no intention to exercise their right of access. For example, an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation; or the request is malicious in intent and is being used to harass an organization with no real purposes other than to cause disruption.

A request may be excessive if: it repeats the substance of previous requests and a reasonable interval has not elapsed; or it overlaps with other requests.

5. MBJ will take reasonable measures to require individuals to prove their identity where it is not obvious that they are the data subject.
6. MBJ will respond to the request within one month from the date of request or being able to identify the person, unless it is particularly complex (in which case MBJ will respond in no longer than 90 days).
7. The DPO will ensure that required actions are taken and that the appropriate response is facilitated within the deadline.
8. The DPO will draw up procedures for responding to requests where necessary, for example, for facilitating Subject Access Requests.

REPORTING OF BREACHES

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

1. All members of staff should be vigilant and able to identify a suspected personal data breach. A breach could include:
   - loss or theft of devices or data, including information stored on USB drives or on paper
   - hacking or other forms of unauthorised access to a device, email account, or the network
   - disclosing personal data to the wrong person, through wrongly addressed emails, or bulk emails that inappropriately reveal all recipients email addresses
   - alteration or destruction of personal data without permission
2. Where a member of staff discovers or suspects a personal data breach, this should be reported to the DPO as soon as possible.
3. Where there is a likely risk to individuals' rights and freedoms, the DPO will report the personal data breach to the ICO within 72 hours of the organisation being aware of the breach.
4. Where there is also a likely high risk to individuals' rights and freedoms, MBJ will inform those individuals without undue delay.
5. The DPO will keep a record of all personal data breaches reported, and follow up with appropriate measures and improvements to reduce the risk of reoccurrence.