MENZIES AVIATION

Data Protection Policy

January 2021

Prepared by: **Andrew MacQueen, Group Data Protection Officer**

People. Passion. Pride. Since 1833.

Policy Statement

John Menzies plc and all Group subsidiary companies (together the "**Group**") are committed to privacy and respecting the rights of individuals with regard to the way in which we handle Personal Data. During the course of our activities we will collect, store and Process Personal Data about our employees, customers, suppliers and other third parties. We recognise that the correct and lawful treatment of this Personal Data will maintain confidence in our organisation, contribute to successful business operations and reduce the risk of privacy-related incidents arising.

The processing of Personal Data is regulated by the European Union's General Data Protection Regulation 2016/679 (the "**GDPR**"), laws complementing or amending the GDPR and/or any other local or regional data protection laws.

This Data Protection Policy sets out the rules that apply and the processes which should be followed by us when Processing Personal Data or contemplating the Processing of Personal Data. Group employees, customers, suppliers and other third parties are required to comply with this Policy when Processing Personal Data for or on our behalf.

A failure to apply the appropriate controls could constitute a breach of our legislative, regulatory and/or contractual obligations and may result in disciplinary action being taken, up to and including termination of employment or termination of a business relationship.

The purpose of this Policy is to specify and communicate to all employees the Group's policy on data protection to ensure good practice across the organisation.

Definitions

For the purposes of this Policy:

"**Personal Data**" means any information relating to an identified or identifiable individual ('data subject'); an identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

"Special Categories of Personal Data" means more sensitive Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; it also includes Genetic Data, Biometric Data and data in relation to health, an individual's sex life or sexual orientation. "**Biometric Data**" means Personal Data resulting from specific technical Processing relating to the physical, physiological or behavioural characteristics of an individual, which allow or confirm the unique identification of that individual, such as facial images or dactyloscopic data.

"**Controller**" means the organisation/person which, alone or jointly with others, decides and determines the purposes and means of the Processing of Personal Data (e.g. The Group is the data controller for its own employees' personal data); where the purposes and means of such Processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

"**Processor**" means an organisation/person which Processes Personal Data on behalf of the controller (e.g. IT service providers).

"**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. "**Process**" will be interpreted accordingly.

"**Consent**" means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

"DPO" means the Group's Data Protection Officer formally appointed to assist, guide and monitor Group's compliance with the data protection regulatory requirements.

"**Data Protection Governance Framework**" means the type of framework that defines the ways and methods through which the Group will implement and manage data protection, as detailed in **Appendix A** of this Policy

"Supervisory Authority" means an independent public authority which is established by a Member State means an EU independent public authority that is responsible for enforcing data protection laws (e.g. the UK's Information Commissioner's Office ("**ICO**")).

"Record of Processing Activities" means a record of all the Processing Activities of Personal Data undertaken by the Group that shall include the name and contact details of the Controller, categories of individuals, categories of Personal Data Processed and any other operations conducted with the Personal Data.

Scope

This Policy applies to all Group employees and covers all Group companies, including subsidiary and joint venture companies in which we have a majority or controlling interest; in particular, to all those with authorised access to Personal Data Processed by the Group, irrespective of status (including temporary staff, contractors, consultants and suppliers); and

This Policy does not form part of any Group employee's contract of employment and may be amended by John Menzies plc, in its absolute discretion, at any time.

Our Group operates in over 30 countries and there may be occasions when local laws, regulations or customs conflict with this Policy. If you have any queries or concerns as to the correct procedure to follow or the appropriate mode of conduct, please do not hesitate to contact the DPO.

You must ensure you always reference the current version of this Policy which will be available on the Group Intranet. Any printed or downloaded versions of this Policy will be classed as uncontrolled. Where this Policy makes reference to other Group policies and procedures, you must review and consult them for more detailed information and guidance.

Data Protection Principles

The GDPR is underpinned by *six core principles* that must be followed when an organisation collects, Processes and stores an individual's Personal Data i.e.:

1. **Lawfulness, fairness and transparency**

   Any use of the Personal Data should be processed lawfully and have a legitimate ground for the processing. At the time the Personal Data is being collected, individuals should receive detailed information and be made aware of the processing operations of their data, mainly what types of Personal Data we intend to process, what is the reason of such processing, how long it would be stored, the list of third parties to whom it might be transferred.

2. **Purpose Limitation**

   Before starting and during the processing operation, we must determine and be explicit about the purpose we need to process the Personal Data of the individuals. In that regard, any personal information must be collected and used solely to fulfil that purpose and not further used for other incompatible purposes with the initial one.

3. **Data minimisation**

   Personal Data collected for a specific purpose must be adequate, relevant and limited to only what is necessary in relation to the purposes for which they are Processed.

4. **Accuracy**

   Personal Data must be accurate and, where necessary, kept up to-date. Inaccurate data can cause business disruptions and affect the rights and interests of the individual. In that regard, every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5. **Storage Limitation**

   Personal Data must be kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the Personal Data are processed. After the Processing has fulfilled its purpose, the data should be destroyed or anonymised that will make the identification of the individuals impossible.

6. **Integrity and Confidentiality**

   Personal Data must be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

It is important that we all ensure we adhere to these principles whenever we are Processing Personal Data and with the complementary policies listed in **Appendix A** We must also ensure that any third party Processing Personal Data for or on our behalf is also adhering to these principles.

All of these principles are underpinned by the principle of *accountability,* which means we must embed GDPR compliance into the fabric of the organisation in the way we Process Personal Data. This includes implementing the necessary data protection-related policies and procedures, providing the relevant data protection training to our employees and a process of awareness-raising (e.g. regular data protection communications).

Roles and Responsibilities

Employees

- All Group employees are responsible for the Personal Data records they create, collect, use and store.
- Everyone who has access to the Personal Data has the responsibility for ensuring data is collected, stored and handled in accordance with the data protection principles, this policy and any other complementary policies.
- Access to Personal Data should be allowed to employees, vendors, contractors and other people only on a need-to-know basis necessary for the performance of their responsibilities and should not be disclosed to unauthorised people, either internally or externally.
- Personal Data should be regularly reviewed and updated where necessary and should be deleted if no longer required for the purpose for which it was collected and further processed.
- All Group employees must ensure that the DPO is involved, where needed, in all issues relating to the protection and safeguarding of Personal Data in a proper and timely manner.

Line Managers

- Line Managers are directly responsible for implementing this Policy within their business function/unit/division and for their team's adherence to it.
- The DPO has direct responsibility for maintaining this Policy and providing advice on its implementation.

Data Protection Officer

The Processing of Personal Data undertaken by the Group requires us to appoint a DPO who is responsible for:

- monitoring compliance with the GDPR and other data protection laws, regulations and standards;
- informing and advising the Group and its employees of their data protection obligations;
- advising on Data Protection Impact Assessments ("DPIAs", in relation to which see section 14 below), managing internal data protection activities, training Group employees and conducting internal audits;
- co-operating with any Supervisory Authority;
- acting as a point of contact for: (i) any Supervisory Authority; and (ii) individuals whose Personal Data is Processed (e.g. Group employees);
- reporting directly to the highest level of Management within the Group on data protection-related matters; and
- keeping a record of all of the Group's data Processing activities.

The DPO will be supported by Group Legal and other Group functions as necessary

Overview of Key Data Assets

We Process Personal Data from a wide range of individuals, including our employees and contractors (current and former), the employees of our customers and suppliers (current and potential) and other members of the public.

The categories of Personal Data can be summarised as follows:

- employee and individual contractor data (e.g. name, address, email address, telephone number, date of birth, age, gender and national tax ID);
- service user data (e.g. name, address, email address, telephone number, frequent flyer number, travel requirements and delivery instructions); and
- customer employee and contractor data (e.g. name, email address, telephone number and employment start date).

This Personal Data may be collected from the individuals themselves (e.g. from CVs, job application forms, business cards or through corresponding with us by mail, telephone, email or otherwise), via the intranet and through other sources. Such other sources might include time sheets, telephone logs, security cameras, internet access logs and emails. In addition, we may collect Personal Data from third parties and from published sources such as newspapers, websites and annual reports.

Occasionally Personal Data collected by us may, where this is necessary for business purposes, include Special Categories of Personal Data, such as Biometric Data used for access control or time and attendance systems. Special Categories of Personal Data can only be Processed under strict conditions.

Such Special Categories of Personal Data are stored across various Group systems and applications including our Physical Access Control systems that are used to capture the Personal Data of Group employees, including images and Biometric Data. This Personal Data is used to secure Group locations and create access control records and Group ID cards.

Rights of the Individual

Individuals have a number of rights under the GDPR including:

1. **The Right to be Informed**
   The Group will ensure that all individuals are aware of the way in which their Personal Data will be obtained, held and disclosed and the information provided must be concise, transparent, intelligible and easily accessible. Typically, this will be achieved through privacy notices which are available internally or on the Group's website(s). If an individual requests this information, it must be provided to them.

2. **The Right of Access**
   Individuals have a right to access the Personal Data which the Group holds on them.

3. **The Right to Rectification**
   Individuals have a right for Personal Data that is inaccurate or incomplete to be rectified by the Group.

4. **The Right to Erasure (/ Right to be Forgotten)**
   An individual can request the removal or deletion of their Personal Data that is held by the Group.

5. **The Right to Restrict Processing**
   Individuals have the right to restrict how their Personal Data is used by the Group.

6. **The Right to Data Portability**
   Individuals can obtain a copy of their Personal Data to re-use it for their own purposes or ask for it to be transferred to other organisations.

7. **The Right to Object**
   Individuals have the right to object to the Group using their Personal Data in certain circumstances, the most common of which will be for direct marketing.

8. **Rights in Relation to Automated Decision-Making and Profiling**
   In certain circumstances, individuals have the right not to be subject to a decision when it is based on automated Processing.

Generally, the individual is entitled, and the Group where acting as a Controller must ensure, the request being actioned is free of charge, without undue delay and in any event within one month of receipt of the request. If you think you have received any such requests, the DPO should be contacted for advice as soon as possible.

Breach Notification

A Personal Data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by the Group. Examples of Personal Data breaches might include sending an email to the wrong address, losing hard copy records or electronic devices which contain Personal Data, or disclosing Personal Data to someone without the appropriate authority.

Any such data breaches or 'near misses' (i.e. where a data breach is narrowly avoided) must be reported to the DPO as soon as the breach or near miss is discovered. In certain circumstances, the DPO may be required to report a data breach involving Personal Data to the ICO within 72 hours of a breach being discovered; it is therefore important to report the breach without undue delay.

The **Information Security Incident Policy** provides further information in this regard, including how to report a breach.

Data Retention

The GDPR requires that the Group retains Personal Data only for so long as is necessary in connection with the purpose(s) for which it was collected. The retention periods for the Processing that is undertaken by the Group are detailed in the **Data Retention and Destruction Policy** (and supporting Schedule).

It is the responsibility of all Group employees to understand and apply the **Data Retention and Destruction Policy**.

The DPO will review the time periods set out in the **Data Retention and Destruction Policy** on an annual basis.
You should take steps to regularly delete unnecessary Personal Data from your inboxes and shared drives and, if retention is necessary, ensure the Personal Data is retained on the correct application / system.

Data Sharing

The Group shares Personal Data with third parties. These third parties can be categorised broadly as follows:

- partners (e.g. an external payroll Processing company);
- suppliers (e.g. IT support and maintenance providers);
- non-contractual parties (e.g. law enforcement agencies); and
- litigation sharing parties (e.g. lawyers).

When Personal Data is being shared, we must ensure that processes are followed and measures are put in place which adequately safeguard the Personal Data.

Any such sharing of Personal Data must be done in accordance with our **Data Sharing Policy**.

DPIA and Data Protection by Design and by Default

The GDPR requires the Group to conduct a Data Protection Impact Assessment ("DPIA") before carrying out Processing of Personal Data in particular circumstances.

The GDPR also requires the Group to have measures and processes in place that demonstrate that privacy has been factored into all new business processes, IT systems, projects, products or services where relevant. This is known as "privacy by design" and "privacy by default".

In practice this means we must conduct a screening at the outset of all new projects / initiatives which involve the Processing of Personal Data to identify those that may require a DPIA. This may include the procurement of a new IT system / application, the collection of Personal Data through a new channel or the sharing of Personal Data with a new third party.

The DPIA process, as set out in the **DPIA Policy**, should be followed for all Processing that requires one. In particular, consult with the DPIA Screening Questions to assess whether a DPIA is necessary. If you are unsure about the need for a DPIA, the DPO should be consulted for advice.

The DPO maintains records of all DPIAs conducted, together with responses to DPIA Assessment Questions and recommendations.

Procurement and Vendor Management

When the Group engages with third parties, whether for the supply of goods, services or if it is proposing to acquire a new product, system or application, we must take account of the requirements of data protection as early in the process as is practically possible.

In many instances, it will be helpful and appropriate to carry out a DPIA to support any other due diligence requirements.

Contracts with third parties providing services to the Group which do, or may, involve the Processing of Personal Data must include the mandatory data Processing clauses which Group Legal will advise on. All such agreements are subject to approval and sign-off by Group Legal and the appropriate input from the DPO.

Data Protection Audits and Monitoring

The DPO will monitor compliance with the Group's data protection-related policies.

Our central Risk function will, on a regular basis, audit the business practices relating to data protection, including compliance with the data protection related policies.

Any known, suspected or potential violation of this Policy must be reported promptly to your Line Manager or to the DPO or through **SpeakUp, the Group's Whistleblowing Hotline**, in accordance with the reporting provisions detailed in the Code of Conduct.

The DPO has direct responsibility for maintaining this Policy and providing advice on its implementation.

If you are unsure about the contents of this Policy or the procedures contained within it, or have any relevant queries, please contact the DPO at: dataprotection@menziesaviation.com / John Menzies plc, 2 Lochside Avenue, Edinburgh Park, Edinburgh EH12 9DJ.

Training

A range of data protection training has been designed, taking into account the roles and responsibilities of our employees, and the types of Personal Data they may Process. Failure to complete the data protection training provided to you may, may result in disciplinary action.

Appendix A: Schedule