Data Protection Policy

Adopted May 2018

John Menzies plc

Document Name	Data Protection Policy		
Owner	Group Data Protection Officer		
Type	Policy		
Audience	All employees of the John Menzies plc Group, customers, suppliers and other third parties		
Classification	Internal		
Document Reference			
Issue Date	May 2018		
Authorised by	John Geddes, Group Company Secretary & Corporate Affairs Director		
Version Number	Author	Changes	Date

1. Policy Statement

1.1. John Menzies plc (the "**Company**") and the wider John Menzies plc group (the "**Group**") (together "**we**"/ "**our**"/ "**us**") 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.

1.2. This Data Protection Policy sets out the rules which 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.

1.3. 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.

1.4. This Policy makes reference to other policies and procedures which you should review and consult for more detailed information and guidance.

1.5. The DPO should be notified as soon as possible in the event of any conflict between the contents of this Policy and any other Group policy or procedure.

1.6. If you are unsure about the contents of this Policy or the procedures contained within it, please contact the DPO at: dataprotection@johnmenziesplc.com.

2. Definitions

For the purposes of this Policy:

"**Biometric Data**" means Personal Data resulting from specific technical Processing relating to the physical, physiological or behavioural characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or fingerprint data.

"**Consent**" means any freely given, specific, informed and unambiguous indication of an individual's wishes by which they signify agreement to the Processing of their Personal Data.

"**Controller**" means the organisation which determines the purposes and means of the Processing of Personal Data (e.g. John Menzies plc); think of a controller as a "data owner".

"**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 the Schedule to this Policy.

"**DPO**" means the Group's Data Protection Officer, contactable at dataprotection@johnmenziesplc.com / John Menzies plc, 2 Lochside Avenue, Edinburgh Park, Edinburgh, EH12 9DJ.

"**Genetic Data**" means Personal Data relating to the inherited or acquired genetic characteristics of a natural person that gives unique information about the physiology or the health of that natural person and results, in particular, from an analysis of a biological sample from the natural person in question (e.g. from swabs).

"**Personal Data**" is a broadly defined term and means any information relating to an individual who can be identified, directly or indirectly, from such data e.g. name, email address, IP address and mobile telephone number. Descriptions of individuals with sufficient specificity will also be considered Personal Data.

"**Processing**" means any use of Personal Data e.g. storage in databases, input onto systems and applications, sharing with law enforcement agencies or creating customer accounts. The act of typing a customer name into a spreadsheet is an example of Processing Personal Data. "**Process**" will be interpreted accordingly.

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

"**Pseudonymisation**" means the process of replacing most identifiers of Personal Data with artificial identifiers or pseudonyms; the Personal Data can no longer be attributed to a specific individual without the use of additional information which is stored separately. Note that pseudonymous data is still regulated as Personal Data and "**Pseudonymised**" will be interpreted accordingly.

"**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.

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

3. Purpose

3.1. Superseding the UK's Data Protection Act 1998, the European Union's General Data Protection Regulation ("**GDPR**") takes effect on 25 May 2018. The principal aim of the GDPR is to protect the Personal Data of individuals in EU countries. Significant fines can apply if there is a breach under the GDPR.

3.2. 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.

4. Scope

4.1. This Policy applies:

(a) to all Group employees and covers all Group companies, including subsidiary and joint venture companies in which we have a majority or controlling interest;

(b) 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

(c) in relation to the Processing of Personal Data:

i. collected about individuals who are resident in Europe or who contact us, or make an order, booking or purchase through our websites, apps or call centres;

ii. of all Group employees;

iii. of employees of the Group's corporate customers; and

iv. from business contacts such as third party vendors, contractors and suppliers.

4.2. It is acknowledged that as the Group operates in over 30 countries 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 contact the DPO.

4.3. The general principles set out in this Policy should, however, be followed globally across the organisation to ensure compliance with the Data Protection Governance Framework, detailed in the Schedule to this Policy.

4.4. 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.

5. Roles and Responsibilities

5.1. All Group employees are responsible for the Personal Data records they create, collect, use and store.

5.2. Line Managers are directly responsible for implementing this Policy within their business function/unit/division and for their team's adherence to it.

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

5.4. 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.

6. Data Protection Principles

6.1. 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.:

(a) Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
(b) collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes ('purpose limitation');
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed ('data minimisation');
(d) accurate and, where necessary, kept up to-date; 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 ('accuracy');
(e) 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 ('storage limitation'); and
(f) 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 ('integrity and confidentiality').

6.2. It is important that we all ensure we adhere to these principles whenever we are collecting and/or Processing Personal Data. We must also ensure that any third party collecting and/or Processing Personal Data for or on our behalf is also adhering to these principles.

6.3. The key, overriding principle of the GDPR is accountability and we have established a Data Protection Framework, detailed in the Schedule to this Policy, to underpin this.

7. Overview of Key Data Assets

7.1. 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.

7.2. The categories of Personal Data can be summarised as follows:

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

7.3. 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.

7.4. 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.

7.5. 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.

7.6. Each type of Personal Data Processing that we undertake must fall under one of the six lawful bases for processing (as defined in the GDPR). This will be included in our record of Processing activities.

7.7. We all have a responsibility to look after the Personal Data that we work with. In electronic form it must be kept secure in line with our IT Policy. Where it exists in hard copy, we should apply the same principles to keep it secure and away from those with no business need to see it.

8. Data Protection Officer

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

(a) monitoring compliance with the GDPR and other data protection laws, regulations and standards;
(b) informing and advising the Group and its employees of their data protection obligations;
(c) 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;

(d) co-operating with any Supervisory Authority;
(e) acting as a point of contact for: (i) any Supervisory Authority; and (ii) individuals whose Personal Data is Processed (e.g. Group employees);
(f) reporting directly to the highest level of Management within the Group on data protection-related matters; and
(g) keeping a record of all of the Group's data Processing activities.

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

9. Rights of the Individual

9.1. Individuals have a number of rights under the GDPR including, but not limited to,:

(a) **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.
(b) **The Right of Access**
Individuals have a right to access the Personal Data which the Group holds on them.
(c) **The Right to Rectification**
Individuals have a right for Personal Data that is inaccurate or incomplete to be rectified by the Group.
(d) **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.
(e) **The Right to Restrict Processing**
Individuals have the right to restrict how their Personal Data is used by the Group.
(f) **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.
(g) **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.
(h) **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.

9.2. In most cases and with the exception of (a) The Right to be Informed, the individual is entitled to the request being actioned 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.

9.3. The GDPR introduces a number of new or enhanced rights for individuals regarding their Personal Data which is Processed by Controllers such as John Menzies plc. We must respond to requests as soon as possible and under the GDPR will generally have a deadline of one month to do so (subject to extensions in certain restricted cases).

10. Breach Notification

10.1. 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.

10.2. 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, there is a requirement 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.

10.3. The Data Breach Policy provides further information in this regard, including how to report a breach.

11. Training

11.1. All Group employees are required to complete data protection training during their onboarding process with the Group. Refresher training will be provided on an annual basis.

11.2. Specialised training will be provided for specialist job roles and you will be notified separately if your role qualifies for such training.

11.3. Failure to complete the data protection training provided to you may, in certain circumstances, constitute a disciplinary offence.

12. Data Retention

12.1. 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 Policy (and supporting Schedule).

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

12.3. The DPO will review the time periods set out in the Data Retention Policy on an annual basis.

12.4. 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.

13. Data Sharing

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

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

13.2. 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.

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

14. Data Protection by Design and by Default

14.1. The GDPR requires the Group to conduct a DPIA before carrying out Processing of Personal Data in particular circumstances.

14.2. 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".

14.3. 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.

14.4. The DPIA process should be followed for all Processing that requires one.

14.5. Please see the Data Privacy Impact Assessment Policy for further information. 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, please contact the DPO.

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

15. Procurement and Vendor Management

15.1. 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.

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

15.3. 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.

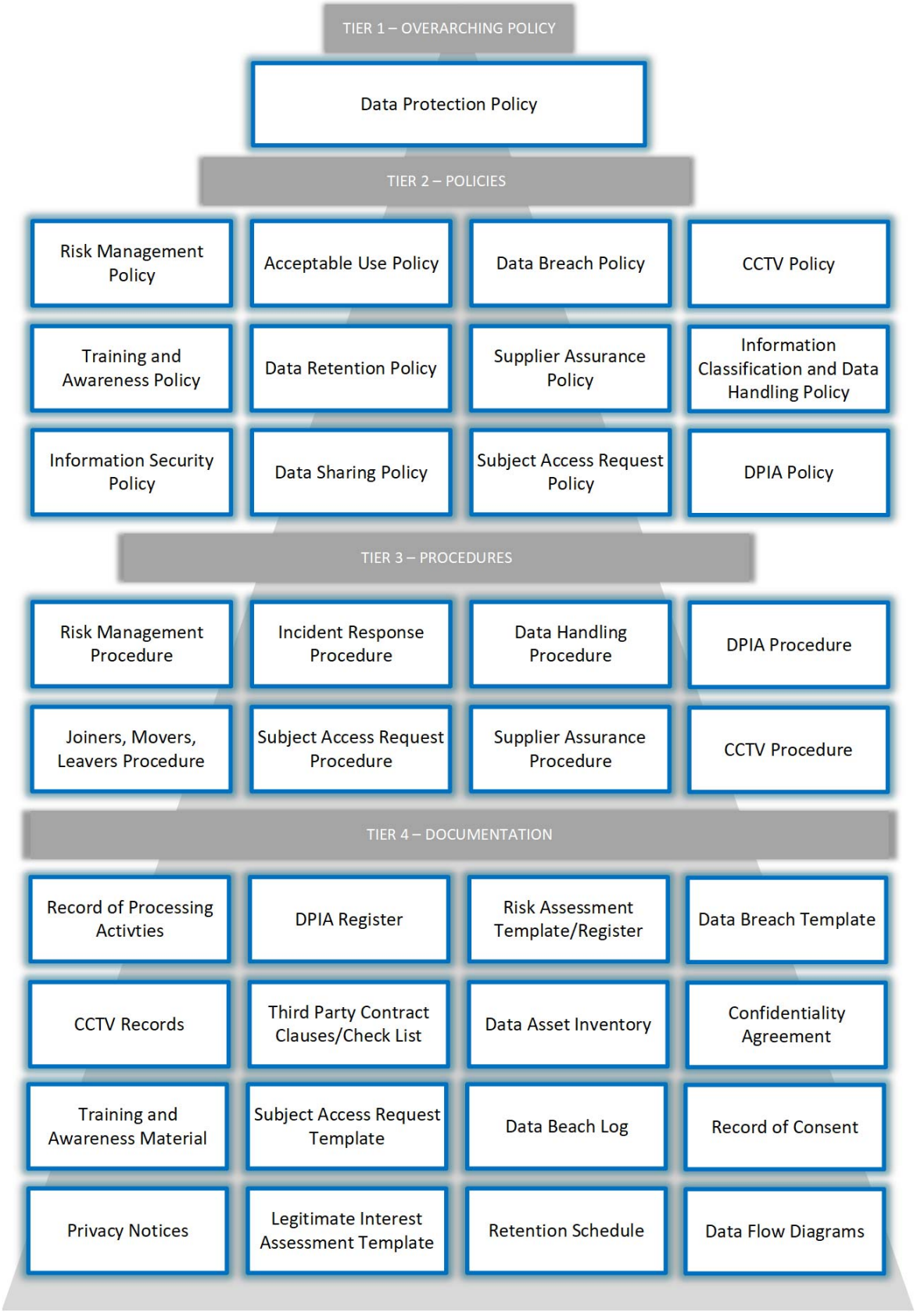
16. Data Protection Audits and Monitoring

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

16.2. 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.

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

Schedule


TIER 1 – OVERARCHING POLICY
Data Protection Policy
TIER 2 – POLICIES
Risk Management Policy
Acceptable Use Policy
Data Breach Policy
CCTV Policy
Training and Awareness Policy
Data Retention Policy
Supplier Assurance Policy
Information Classification and Data Handling Policy
Information Security Policy
Data Sharing Policy
Subject Access Request Policy
DPIA Policy
TIER 3 – PROCEDURES
Risk Management Procedure
Incident Response Procedure
Data Handling Procedure
DPIA Procedure
Joiners, Movers, Leavers Procedure
Subject Access Request Procedure
Supplier Assurance Procedure
CCTV Procedure
TIER 4 – DOCUMENTATION
Record of Processing Activties
DPIA Register
Risk Assessment Template/Register
Data Breach Template
CCTV Records
Third Party Contract Clauses/Check List
Data Asset Inventory
Confidentiality Agreement
Training and Awareness Material
Subject Access Request Template
Data Beach Log
Record of Consent
Privacy Notices
Legitimate Interest Assessment Template
Retention Schedule
Data Flow Diagrams