GDPR

Our Commitment to Data Protection

Menzies LLP and its subsidiaries are committed to keeping your personal data secure. This statement outlines the measures that we take to ensure that our staff, systems, policies, procedures and premises support this objective.

Staff

- We aim to embed data protection in our culture. New staff undergo compulsory training in data protection as well as annual refresher training.
- As part of their employment contracts, staff are required to adhere to policies including:
- ***Data Protection and Security***
- ***Electronic Information and Communications***
- ***BYOD Acceptable Use***

Policies and Procedures

- In addition to our internal policies, the following can be found on our website at https://www.menzies.co.uk/legal:
- Our Standard Terms of Business (STOB) - these are issued to all clients upon engagement or any significant change in service and include an outline of our obligations to protect data that we process during the performance of our services to clients.
- Privacy Policy (including data retention);
- Collection of Data;
- Cookie Policy.

Lawful Bases for Processing

- Our lawful bases for processing are outlined in our Privacy Notice.

Processors

- Where we engage third parties to process data on our behalf, we seek to ensure that they take appropriate technical and organisational measures to protect personal data.

Physical Security

- We use electronic access control and/or security/reception in all of our buildings. Staff are issued access fobs to only the building(s) that they normally work from.
- All office networking equipment is secured in lockable cabinets, contained in rooms with suitable environmental controls and secured. Regular reviews of access control are performed.
- The UK datacentre (DC) has 24 hour manned security, CCTV and Intruder alarms, remote hands are employed directly by the DC provider and security checked. Access to Menzies systems at DC is via a pre-approval list.

Secure Communication and Collaboration

- Major investment in our client portal which enables secure exchange of data content and communication between Menzies and our clients. Clients went live in September 2017 and a programme of service line migrations are currently underway.
- Secure encrypted email available with clients and third party institutions, both governmental and financial. TLS 1.1 and 1.2.

IT Infrastructure and Network Access

- Tier 3 datacentre (ISO9001, ISO27001, ISO22301 and PCI DSS) providing fully resilient servers, storage, switching and firewalls. (N+1) resilience for power failure.
- All network traffic is through a dedicated encrypted network (MPLS), internet connectivity is via centrally managed fully resilient firewalls.
- Data held centrally on dedicated hardware. Storage is not shared and is managed by Menzies IT.
- Published Security Policy complying with Cyber Essentials and Information Security Forum (ISF) best practice. Supported by Proxy based URL filtering, Anti-Virus protection, monitoring software and patching policies
- USB flash drives and internal drives use hardware-based encryption (BitLocker full disk encryption).
- Daily backup procedures backup data to an

alternative datacentre non-metro location.

Cyber Incident (CI), Business Continuity (BC) and Disaster Recovery (DR)

- Our Information Security Management System (ISMS) is based upon the controls of Confidentiality, Integrity and Availability (CIA). In the case of a CI, BC or DR incident known planned activities and accountable individuals would be brought together to ensure assessment, communication and actions are taken to minimise service disruption.
- Resilience has been designed into the IT operation and planning for incidents for our people and processes means that services can be run from any Menzies location or any alternative location.
- All data is backed up offsite (Fully Encrypted) and in the case of a significant disaster within the UK datacentre, services would be re-invoked from a Menzies office location. Menzies has additional resilience via cloud based services (secure email).
- Regular annual 'table top exercise' invocation, regular continuity testing of data recovery from backup.

Data Destruction

- Where possible, we no longer generate paper files but instead store our data digitally. Historic paper files are held in secure archive facilities and destroyed in accordance with our retention policies.
- Locked document security bins are located throughout all offices for the secure disposal of physical documents.
- Historic hard copy working paper files are stored in off-site secure 3rd party facilities with controlled secure disposal at the appropriate time.
- Hardware and equipment that has held personal data is destroyed by accredited facilities who provide us with certificates of destruction.
- Physical certified destruction of IT hardware and compliance to Waste Electrical and Electronic Equipment (WEEE) directive

International Transfers

- We will only transfer your data outside of the EEA in accordance with the requirements of the GDPR. Full details of our policies on international transfer can be found in our Privacy Notice and for clients, in our Standard Terms of Business.

Personal Data Breaches

- We have procedures in place to deal with Personal Data Breaches and staff are trained to recognise them and respond accordingly. Our internal Data Protection Representative will have overall responsibility for ensuring that breaches are dealt with in accordance with the requirements of the GDPR.

Data Controller Registrations

- Each of our legal entities, Menzies LLP, Menzies Corporate Finance and Menzies Wealth Management, is registered as a Data Controller with the ICO. Each of our insolvency practitioners is also individually registered where required by the insolvency regulator.

Rights in Relation to Your Information

- You have certain rights in relation to the personal information we hold about you, which are outlined in our Privacy Notice. Please contact us if you require assistance in relation to your rights.

Ethical Standards

- We are regulated by various professional bodies who require the firm and its employees to operate within their professional guidelines/code of ethics. Depending on the services that we are providing, we may be operating in accordance with any one or more of the following:
    - ICAEW Code of Ethics
    - FCA Code of Conduct
    - Insolvency Code of Ethics

How to Contact us about Data Protection

- If you have any queries in relation to Data Protection, please email our Data Protection Representative at dataprotection@menzies.co.uk.