GDPR Compliance Statement

We are assessing the provisions of the EU's General Data Protection Regulation (GDPR) with guidance from the Article 29 Working Party and the Information Commissioner's Office (ICO). We have appointed an internal project manager and an external data protection consultancy firm to run a formal project, the intention of which is to be GDPR compliant within the requirements of the provision. The project encompasses, but is not limited to the following:

Staff

- We aim to embed data protection in our culture. We shall undertake a comprehensive internal communication campaign to raise staff awareness of GDPR using posters, chrome bit messages, screen savers and informal awareness training sessions.
- We intend to put all staff through a formal training session, with some staff earmarked for specialist training due to their roles to enable us to maintain our compliance with the regulations.
- We will be training all staff on how to recognise and respond to Subject Access Requests.
- Staff employment contracts, which include clauses that will change under GDPR, are being reviewed. Staff contracts require our staff to adhere to our DATA PROTECTION AND SECURITY policy and our ELECTRONIC INFORMATION AND COMMUNICATIONS policy, which are both also under review.

Systems

- We have made a major investment in developing a client portal to enable secure exchange of messages and attachments between Menzies and our clients. Our first clients went live on this in September 2017 and it is being progressively rolled out to our client base. The portal will also enable clients to manage their personal details and communication preferences.
- We are reviewing our systems, including cloud services, to ensure that they meet any specific requirements of GDPR.
- We are currently working toward Cyber Essentials Plus certification to ensure that our systems are adequately robust to minimise the risk of data breach via cyber-attack.

IT Infrastructure and Network Access

- We use a 3rd party tier 3 data centre in London providing us with fully resilient servers, storage, switching and firewalls. All devices are monitored and maintained by the data centre staff. The data centre boasts 6 x 500 kVA UPS (N+1), 4 x 1MW generators and N+1 A/C systems.
- Connectivity to the data centre from Menzies offices is by way of a secure MPLS network with private VPN tunnels.
- Data is stored at the data centre in a dedicated SAN in a private rack for Menzies. Storage is not shared and is under our control.
- Network access for staff is controlled by AD security. Websense (Forcepoint) URL filtering is in use. Sophos anti-virus is deployed across the network, including all endpoints. Virus pattern updates are automatically downloaded when available. Security alerts are reviewed daily. Network password complexity is enabled, requiring users to change their password every 90 days.
- Kingston DataTraveller USB flash drives containing hardware-based encryption are available for staff use if data is to be taken offsite. All laptops are installed with either TrueCrypt or BitLocker full disk encryption.
- Our daily backup procedures backup data to a dedicated server in the data centre and then

replicated offsite.

Policies and Procedures

- Our Standard Terms of Business (STOB), which are issued to all clients upon engagement or any significant change in service, outline our current data protection policy. These are being reviewed and new GDPR-compliant versions will be released. We will be aiming to issue new engagement letters to all clients, along with the amended STOB, upon the annual renewal of each client's services. Our STOB are accessible from our website: https://www.menzies.co.uk/legal/.
- The terms of use of our website are also being updated, including:
  - Privacy Policy;
  - Collection of Data;
  - Cookie Policy.
- We are reviewing all current policies and business processes and identifying where we need to implement new, or amend existing ones, to be GDPR compliant.
- Our data retention policy is generally six years plus the current year or as required by law, after which records are destroyed.

Suppliers

- We are reviewing supplier contracts and contacting our suppliers to determine their GDPR compliance.

Physical Security

- We use electronic access control in all of our buildings and staff are issued access fobs to only the building(s) that they normally work from.
- 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.

Disaster Recovery

- Having our staff spread over 7 physical offices, the use of a professional third party hosting organisation for our servers, storage, switching and firewalls and offsite daily back up procedures, we are of the opinion we are reasonably well placed to deal with a disaster.
- We are a Partner-led business with Partners involved on a daily basis at each office. In the unfortunate event of an office being unavailable for whatever reason it would be possible to relocate the staff from that office to either work from one of the other offices or from home within a few hours.
- In a worst case scenario, with IT being compromised entirely, the hosting, networking and storage suppliers are working on a “best endeavour” basis to get us up and running as quickly as possible. Should this fail we have the space and networking capabilities in our Woking office to build replacement servers, reload the software and restore the data from backup. Clearly there would be a few days' lead time but such an arrangement is workable as a last resort.