Compliance Assurance Statement

1. Introduction

This statement relates to Forbes Solicitors LLP ("we", "us", "our"), a Partnership, registered in the United Kingdom with SRA registration number 46408 and having its registered address at Rutherford House, 4 Wellington Street (St Johns), Blackburn, BB1 8DD.

We recognise and accept our responsibilities as outlined in the General Data Protection Regulation ((EU) 2016/679) as applied by the Data Protection Act 2018 ("UKGDPR") and other legislation enacted in the UK in respect of the protection of personal data.

We are a sole or joint "Data Controller" for the purposes of data protection legislation. Whilst we do not make the majority of decisions regarding the purpose of the processing we undertake for clients in the provision of services we determine the manner of processing in many cases and in any event are subject to professional obligations which may override and be contrary to the instructions of our clients. In these situations, we will exercise judgment over and above that of a "Data Processor".

We are committed to ensuring the security and protection of all personal data that we process and to provide a compliant and consistent approach to data protection.

One of the key components of the UKGDPR is the concept of accountability contained within Article 5 (2), a new element of data protection legislation. We are required to demonstrate compliance with the UKGDPR data protection principles which specify that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is collected; and
- 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.

Our appointed Data Protection Officer (DPO) is Daniel Milnes, Partner and Head of Governance, Procurement & Information and we ask that you direct any questions regarding our compliance with UKGDPR to DataProtectionOfficer@forbessolicitors.co.uk.

2. Principle 1: Lawfully, fairly and transparently

2.1. In providing services we will only process personal data on instructions from our client as co-controller or where required by law or by our compliance and quality policies and procedures. We also act as controller for data about our staff and Partners and in relation to recruitment and marketing and business development activity.

2.2. We will manage any disclosure of personal data to a third party (including a sub-contractor) where instructed or required by law or by our compliance and quality policies and procedures.

2.3. We will document and maintain a record of the personal information that we process. This record contains the following information:

a) Our name and contact details;
b) The purposes for which we process personal information;
c) A description of the categories of personal information collected from individuals;
d) A description of the categories of individuals whose personal information is collected;
e) A description of the categories of third parties with which personal information is shared;
f) If applicable, the name of any countries or organisations outside the UK to which personal information is transferred;
g) If applicable, the safeguards in place for transfers of personal information outside the UK;
h) The retention periods for how long personal information is kept; and
i) A general description of technical and organisational security measures in place to safeguard personal information.

2.4. We will ensure that appropriate Privacy Notices have been provided and are sufficient in scope and kept up-to date in order to meet the transparency requirements under the UKGDPR. These notices will include the following information in accordance with Article 13 of the UKGDPR (and similar information where Article 14 applies):

a) The identity and the contact details of the controller;
b) The contact details of our DPO;
c) The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
d) Where the processing is based on point (f) of Article 6 (1), the legitimate interests pursued by the controller or by a third party;
e) The recipients or categories of recipients of the personal data, if any;
f) Where applicable any transfers of data to a third country or international organisation;
g) The period for which the personal data will be stored;
h) The existence of individual rights and the nature of those rights;
i) Where the provision of personal data is a statutory or contractual requirement or a requirement necessary to enter into a contract the possible consequences of failure to provide that information; and
j) The existence of automated decision making, including profiling information about the logic involved as well as the significance and the consequences of such processing.

3. Principle 2: Purpose Limitation

3.1. We will process personal data only to the extent and in such a manner as is necessary to

fulfil the purpose(s) of processing and shall not process personal data other than for the applicable permitted purpose(s). We will keep and maintain a record of any processing.

3.2. Any processing will be undertaken in accordance with your written instructions.

3.3. Where providing services we will not store, copy or use personal data except as necessary

for the performance of our obligations under our contract for the provision of legal services and associated purposes such as professional regulation and insurance.

3.4. Personal data will not be used directly or indirectly to market, solicit or offer any service to data subjects other than as permitted by UKGDPR and other legislation.

4. Principle 3: Data Minimisation

4.1. When obtaining personal data for any purpose(s), we will obtain enough information to perform our obligations properly. Where we obtain or hold information from or about clients, third parties or colleagues that is not relevant to our role that information will not be used or disclosed in the performance of that role. Our ISO procedures specify what information is required for those purposes.

4.2. Data minimisation is also an appropriate consideration to ensure that only the essential data from among those held by us are used to undertake a particular task.

5. Principle 4: Accuracy

5.1. We will ensure that personal data are adequate, relevant and limited to what is necessary in relation to the permitted purposes.

6. Principle 5: Storage Limitation

6.1. Our ISO policies address retention periods for personal data and the period of time for which information should be retained. This is different for different types of personal data relating to different purposes of processing and includes information being retained and potentially shared with others after our work is complete or the end of employment or other engagement with us.

6.2. We have procedures in place to archive, erase or destroy any information in accordance with those policies.

7. Principle 6: Integrity and Confidentiality

7.1. Employees are all subject to confidentiality obligations in relation to the data they process for us as part of their roles and to policies prohibiting access to other data held by us that is not job-related. Steps have been taken to ensure the reliability and integrity of employees. Each employee has undergone and shall continue to receive reasonable levels of training in Data Protection Laws and in the care and handling of personal data.

7.2. We have implemented and will maintain the following appropriate technical, organisational security measures, processes and facilities which are sufficient to comply with UKGDPR. These form part of our ISO and Risk Management policies, in particular our Data and Computer Security Policy:

- We shall use the latest versions of anti-virus, and shall have adequate malware detection;
- Passwords changed every 90 days;
- Use of any form of portable storage media is restricted;
- Encryption and password protected emails are utilised where appropriate;
- Mobile devices - hard drive is encrypted, password protected and remote device wiping is applicable as required;
- Training;
- Clear desk policy;

- Locked filing cabinets;
- Segregation of client data including case management system file locks where appropriate;
- Locked printing; and
- Regular external cyber security testing.

7.3. We will ensure that any system on which we hold data including back-up data is a secure system. Should any data be corrupted, lost or degraded as a result of our default we will take steps to restore or procure the restoration of the data.

7.4. Where we share information with another party we will ensure that adequate data processing or data sharing terms are in place with appropriate safeguards. This written agreement will give effect to the information contained within this compliance assurance statement such that they apply to the sub-processor.

7.5. Any transfers of personal data outside the UK will only be undertaken where instructed or necessary and with appropriate security measures are in place.

8. Breach Notification

8.1. We have in place written procedures to be followed in the event of a security incident:

- We will if appropriate notify affected co-controllers or data subjects as soon as practicable unless prohibited by law;
- We will take steps to restore the security of the compromised systems files and information to contain the breach and minimise the impact;
- We will modify any policies to prevent such events occurring in the future;
- We will make a report to the ICO if required by the UKGDPR.

9. Dealing with Data Subject Requests

9.1. Upon receipt of a data subject access request or a request to rectify, block or erase any personal data in relation to data under the joint control of ourselves and another controller we will notify the other controller as soon as practicable.

9.2. We agree to provide assistance with any such request affecting co-controlled personal data where possible.

9.3. Where we are the sole controller or required to determine the appropriate response in relation to co-controlled personal data we will apply our policies and processes for dealing with data subject rights.