GDPR: DATA PROTECTION ASSURANCE STATEMENT

1. Restrictions on Sub-Contracting

The GDPR gives Data Controllers a wide degree of control in terms of the ability of the Processor to sub-contract. Data Processors require prior written consent. The Processor is required to inform the Controller of any new sub-Processors, giving the Controller time to object. If there is an objection, the sub-processing may not continue.

The lead Processor in a sub-contracting arrangement is required to reflect the same contractual obligations it has with the Controller in a contract with any sub-Processors and remains liable to the Controller for the actions or inactions of any sub-Processor.

As per 5.10 and 5.11 of GDPR Addendum we will inform the Controller of any new su-Processors, comply with any objections, and remain liable for the actions or inactions of sub-Processors.

2. Controller/ Processor contract

Data Processor activities must be governed by a binding contract. The binding obligations on the Processor must cover the duration, nature and purpose of the processing, the types of data processed and the obligations and rights of the Controller. There are a number of specific requirements including that the personal data is processed only on documented instructions from the Controller, and requirements to assist the Controller in complying with many of its obligations. The Data Processor has an obligation to tell the Controller if it believes an instruction to hand information to the Data Controller breaches the GDPR or any other law.

As per section 5.1.1 of GDPR Addendum we will inform the Controller if we believe an instruction is in breach of law.

3. Demonstrating compliance

GDPR requires organisations to demonstrate compliance. Processors are under an obligation to maintain a record of all categories of processing activities. These records must be provided to the Information Commissioner's Office on request. This must include details of:

- the Controllers they act for
- any other Processors
- a Data Protection Officer (DPO)
- the categories of processing carried out
- details of any transfers to third countries
- A general description of technical and organisational security measures.

Processors must assess their need to comply by understanding whether they have fewer than 250 employees. If so, and unless the processing does not pose a risk to the rights and freedoms of individuals, is not more than occasional and does not include special categories of data (sensitive personal data), then the requirements are reduced.

Our organisation has reviewed and understood the level of the requirement on it to comply with the General Data Protection Regulations.

4. Security

Processors, like Controllers, are required to implement 'appropriate' security measures. What is 'appropriate' is assessed in terms of a variety of factors including the sensitivity of the data, the risks to individuals associated with any processing or breaches of security, the state of the currently available technologies, the costs of implementation and the nature of the processing. These measures might include pseudonymisation and encryption. Regular testing of the effectiveness of any security measures is also required where appropriate.

As per section 5.2 of GDPR addendum – https://www.mkbrand.uk/compliance. We use a variety of measures including pseudo-anonymisation and encryption.

Where services include disposal of IT hardware – what standard of secure destruction is employed?

Within our office environment storage media is provided to a suitable 3rd party disposal company to ensure robust disposal.

The site itself is in an office with key card access, 24 hour CCTV and serviced security alarm.

With regards to hosting of customer data at Memset Ltd (Our hosters) their policy can be found here: https://www.memset.com/about-us/data-destruction-practises/

Data Controllers have a requirement to receive certification of the completed work.

Certification can be provided on request.

Where devices are removed from site, they are always protected by the following system security measures.

- **Password protected – complex 12 character passwords**
- **Firewall**
- **FileVault encryption**
- **Encrypted backups**
- **Multi-factor authentication**
- **Regular security updates**

5. Breach notification

There are enhanced breach notification requirements on both Data Controllers and Data Processors. Processors are required to notify their relevant Controller of any breach without undue delay after becoming aware of it. Controllers have 72 hours to notify the Information Commissioner's Office from the point the breach is detected, therefore reporting from the Processor to the Controller is required well within this time period. Your organisation will need to show evidence effective process to identify and report breaches of your security measures to the Data Controller promptly, allowing the Controller time to deliberate and comply with the 72 hour rule.

As per section 5.6 of GDPR addendum:
https://www.mkbrand.uk/compliance. We will notify the customer of any breach without undue delay.

6. Data Protection Officers

Both Controllers and Processors are required to appoint DPOs in certain situations, including where they are a public authority or body, where the data processing activities require regular monitoring of data subjects on a large scale, or where the core activities of the processing involve large amounts of special (sensitive) data or data relating to criminal convictions and offences. The primary role of the DPO is to assist the Processor with, and advise on, compliance with the GDPR. Processors may also choose to appoint a DPO even if they do not fall into one of the specified categories. Please state if you have appointed a DPO, or state that you have reviewed the requirement and determined that it is not applicable to your organisation.

We have reviewed the requirements and have not appointed a DPO.
We have appointed a compliance officer (Kevin Davies) and a SAR team (Kevin Davies and Mathew Hampshire)
as per Subject Access Request Policy: https://www.mkbrand.uk/compliance

7. Transfers to third countries

The Processor has to exercise a degree of independence from the Controller when deciding whether or not it can transfer personal data to a third country. While Processors are required to follow the relevant Data Controller's instructions with regard to the data processing, no matter what those instructions are, they may only transfer personal data to a third country (in the absence of an adequacy decision) if the Controller or Processor has provided appropriate safeguards and on condition that data subjects have enforceable rights in that country with respect to the data.

We will not transfer data to a third country without the written consent or request of the Controller.
As per section 5.8 of GDPR Addendum: https://www.mkbrand.uk/compliance

Signed by: 

Print name: Kevin Davies

Role within organization: Compliance Officer

Date: 01.09.2018