Media Buying – The Media Shop – Question 1.6.2

Tenderers should describe their procedures for storing, retaining and transmitting data between the Contractor, the Framework Public Bodies (and sub-contractors where applicable) to ensure compliance with the Statement of Requirements (Schedule 1) and to ensure continuity of service and protection against cyber-attacks. Answers should include (as a minimum):

- Details of where data will be stored and how it will be secured including processes, software and standards and must include measures put in place with sub-contractors (where applicable);
- Details of how data will be securely transmitted between the Framework Public Body, the Contractor (and sub-contractors where applicable) including processes, software and standards;
- Details of how the data will be secured at rest (end point security) both at the Contractor's premises (and their sub-contractors premises where applicable);
- Details of processes followed including those for assessing future risks;
- Testing of Disaster Recovery policies and procedures, including the dates, duration and frequency;
- Methods for the back-up and continuity to deliver services should an incident occur including manpower and access to equipment;
- Methods and processes in place to mitigate against cyber-attack and crime using online technologies including processes, software and standards;
- Destruction policies and processes including policies, processes and software. This should include the measures put in place with sub-contractors where applicable;
- Tenderers should also provide details of any standards applicable in this area (e.g. ISO 27001, ISO 22301, ISO/IEC 20000, Cyber Essentials/Cyber Essentials Plus or their equivalents).

(Weighting 100% - Word Count 1,500)

DATA PROTECTION & INFORMATION SECURITY

The Media Shop is committed to the safe and secure handling, transmitting and storing of data, to defend against potential misuse of data, cyber-attacks, or crime using digital technologies. We have worked with Framework Public Bodies for over 26 years without a breach of security.

1. PROFESSIONAL IT SUPPORT

[redacted] one of the UK's leading IT solutions companies manages all our ICT systems and processes. They are ISO: 9001 accredited, the international standard that specifies requirements for a quality management system (QMS).

[redacted] ensures we protect the confidentiality, integrity and availability of data stored on devices which connect to the Internet, including desktop PCs, tablets and smartphones, all types of server and networking equipment.

Our security systems provide protection against the most common internet-based threats to cyber security — particularly, attacks that use widely available tools and demand little skill, including hacking, phishing, and password guessing.

[redacted] has undertaken an audit of our systems in 2019 and have confirmed that our security procedures comply with the UK Government Cyber Essentials standards. We are therefore committed to undertaking the certification process in summer 2019.

2. DATA SECURITY POLICY

The Media Shop has a written data security policy which forms part of a new employee induction process. The policy is updated on an annual basis by the Senior Management Team.

All staff are made familiar with our procedures for data protection and securing against cyber-attack at their staff induction. All staff must comply with the policies, and departure from these policies and procedures will result is a disciplinary matter. We send out bi-annual reminders of our policies to all staff.

The policy includes instruction on the following procedures.

Data Security Processes and Procedures:

Requirement	Our Approach
1. Data storage	All data is stored on our [redacted] server.
2. Data security	Our data security procedures include: • Systems protected at the endpoint by [redacted] for malware detection and at the perimeter with a [redacted] firewall; • Computers/files are password protected; • personal data on laptops and other portable devices is kept to a minimum; • manual filing cabinets containing personal data are locked and only accessible to authorised personnel; • confidential documents are not be left unattended on desks; • printers/photocopiers are passcode protected. • we ensure staff are appropriately trained to handle personal data safely and securely; • personal data is disposed of securely (by shredding, destroying or securely deleting electronic files); • security breaches are reported to DPO immediately; • server data is backed up daily; • back-up tapes are stored off site each night; • Office access – protected by [redacted] nd [redacted] The office is secured by an external building door, and an office door, both of which [redacted]
3. Secure data transfer	• Data is primarily transmitted by email or via a secure [redacted] intranet. • Sensitive data is password protected with password supplied in separate email.

4. How the data will be secured at rest (end point security)	• See answer to point 2 above.
5. Processes followed including those for assessing future risks	• Our IT support company, [redacted] advise us on emerging techniques and products that address risks relating to the IT infrastructure and data.
6. Testing of Disaster Recovery policies and procedures	• We have a robust Disaster Recovery policy in place. We have a Business Continuity Committee (BCC) who review our disaster recovery procedures and ensure they are up to date. Emergency activation and communication procedures are also updated and tested at this time. • We pay for [redacted] which covers server recovery in the event of server failure with response times in line with our standard Definition of Service.
7. Methods for back-up and continuity to deliver services should an incident occur	• Current server backup consists of [redacted] software and [redacted] removable hardware. Data on the server is backed up on a daily basis and the tapes are secured off site. We are able to reload the saved data and resume service delivery within [redacted] hours. • The BCC regularly review our disaster recovery procedures and ensure they are up to date. The committee is responsible for distributing a reminder to all staff on latest processes in the event of a data breach.
8. Methods and processes in place to mitigate against cyber-attack and crime	• [redacted] including dedicated anti-ransomware software [redacted] is in place.
9. Destruction policies and processes.	• All confidential data is shredded weekly. We also make use of [redacted] for bulk disposal of confidential information. • Redundant hardware is wiped of old data and disposed of via companies such as [redacted] (and other similar companies).
10. Details of standards applicable.	• [redacted] are compliant with the UK Government's Cyber Essentials standard. We are committed to going forward for certification in Summer 2019.

3. GDPR COMPLIANCE

The Media Shop acts as both a controller and a processor of data, and in both these roles is fully compliant with GDPR.

As a long-term member of the Institute of Practitioners in Advertising, we used the guidelines issued by their legal team, in conjunction with [redacted] in updating our processes and policies in 2018.

This included:

- An audit of the company's data processing and security processes in the context of the new GDPR regulations.
- Registering with the Information Commissioner.

- Appointing a Data Protection Coordinator [redacted] Managing Director, already held this responsibility).
- Refreshing our company policies, using the IPA's template policies as Best Practice guidelines, including:
    - Data Protection Policy
    - Data Protection Impact Assessment Policy
    - Data Retention Policy,
    - Individual Rights Policy
    - Data Incident Policy.

Procedures which are proportionate to our business and the risks associated with our activities are embedded throughout our agency processes, including staff induction and training. [redacted] undertakes an annual review of our processes to ensure we continue to comply with best practice.

Summary of Data Protection Processes:

Area	Procedure
Data Collection	We only collect personal data that we have a lawful reason for doing so.
Explicit Consent	We ask for explicit consent for storage of personal data, where we have no other lawful ground for processing it.
Individual Rights	We also allow individuals the right to access, correct or erase their personal data, or object to it being used for certain purposes.
Data Usage	Data is only used for the reason it was collected.
Data Transfer	We are aware that if we transfer data outside the European Union, we must ensure that the relevant country has an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
Data Accuracy	The Act says all data must be accurate and up to date, so we review the data we hold on an annual basis.
Data Storage & Security	Personal data must be kept secure at all times. We take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
Use of Data Out of the Office	When working away from the office we do the following: • ensure personal data stored on portable devices including memory sticks is encrypted and kept secure at all times; • avoid leaving papers or electronic devices lying around; • make sure members of the public cannot see confidential documents or computer screens.
Data Access Requests	We have a process in place to deal with requests by individuals to see personal data held by the company. Request and response recorded in writing.
Appointing a Data Processor	We have a written contract in place, confirming the data processor will only work on our instructions and will ensure sufficient data protection measures are in place.
Staff Training on GDPR	Staff are made aware of all GDPR policies at their staff induction, and reminded of them again at their annual appraisal.
Monitoring of Compliance	Management monitor compliance with GDPR by incorporating it into our annual business planning sessions.

Maintaining Records	As an SME, we only maintain records of activities related to [redacted] data processing or processing of sensitive data such as [redacted]
Data Processing Impact Assessments (DPIAs)	We undertake, record and document DPIAs for new projects where data processing is likely to result in a high risk to individuals; where a profiling operation is likely to significantly affect individuals; or where there is processing on a large scale of sensitive personal data. If the DPIA identifies a high risk situation, this will be referred to the ICO.
Data Breaches	In the event of a data breach, we commit to notifying the ICO within [redacted] f becoming aware of the breach.
Privacy Notices	We have appropriate privacy notices for all instances where we gather personal data as a data controller.
Supplier Compliance	When working with suppliers, we ensure they are vetted for compliance with GDPR. Annually reviewed.
Use of third parties	We acknowledge that if we choose to use a third party to manage data, we still have responsibilities under the Act as data processor.