Data Security and Cyber Resilience

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.

The advent of GDPR legislation is one of a number of factors that has codified and improved data security. At the same time, proliferation of data in media buying, combined with advances in cyber-threats, has increased the complexity and challenges inherent in providing the service.

Republic of Media maintains best in class Cyber-Security, Data Retention and Data Protection policies to ensure framework client data is protected and threats are protected against.

Cyber essentials

Republic of Media is Cyber Essentials certified (Certification number: [redacted] and is working towards Cyber Essentials Plus. We are in the process of becoming IAB Gold Standard certified and will have that in place by September 2019.

Cyber-security

Cyber threat and data breaches are seen as a significant business risk at Republic of Media and are an ongoing priority for the Board of Directors. The Board is committed to management and mitigation of the risk through effective strategies, policies and use of technology. Cyber resilience is the responsibility of Managing Director [redacted], with Contract Manager [redacted] responsible for ensuring standards are in line with our Framework contract requirements.

The threat from cyber-attack has never been higher and evolves constantly. Republic of Media is committed to continuous improvement and agile adaptability in our data security and cyber resilience. We take concrete actions including software review, certification review and media supplier audits. We leverage our memberships of the IPA, Advertising Association, Marketing Society and Google Premier Partner Status to understand and implement best practice.

We comply with all relevant legislation and review future legislation (such as that resulting from the EU NIS Directive) to take appropriate action. Our [redacted]s required to report on emerging trends and threats on a quarterly basis, while our [redacted]provides day to day review. Together they deliver an action plan for development and implementation.

We take steps to ensure understanding of developing cyber threats. An example includes Managing Director [redacted]attending a briefing with the Commander of Met Police [redacted] organised by ISBA, which highlighted evolving threats from terrorism and cyber-crime.

Staff are trained in data security and cyber resilience as part of our L&D framework, administered by Board Director [redacted]

Republic of Media are proud to have had zero cyber security or data breach issues in our history.

Administration and improvement

Administration and record control of our data security and cyber resilience strategies are the responsibility of Financial Director [redacted] reporting to the Board of Directors. Policy review at Board level is annual with quarterly review by an external IT consultant. Contract Manager [redacted] s the Board member responsible for ensuring policies meet Framework and Scottish Public Sector standards.

Future risk assessment is the responsibility of the Board with [redacted] – our data and technology executive – tasked with tracking and reporting developments in data security and cyber-threats.

Data Transfer

In nearly all instances for Framework clients, Republic of Media will act as a Data Processor and not as a Data Controller. In line with GDPR Legislation terms, we will generally be a Data Controller whenever we process the personal data of our staff and the staff of our business partners and clients as well as consumer personal data if we process it for our own purposes (such as when we build our own proprietary databases). When we are a Data Controller our Data Protection policy will apply. When we are a Data Processor, our Data Retention Policy will apply.

Encrypting data whilst it is being transferred from one device to another (e.g. across the internet or over a wireless connection) provides effective protection against interception of the communication by a third party whilst the data is in transfer. We will use encrypted communication when transmitting any data over a wireless communication network (e.g. Wi-Fi) or when the data will pass through an untrusted network.

Data can be transformed into an encrypted format and transferred over a non-secure communication channel yet still remain protected. An example would be sending an appropriately encrypted attachment via email. Republic of Media uses Transport Layer Security (TLS) or a Virtual Private Network (VPN) to provide assurance that the content of the communication cannot be understood if intercepted.

Republic of Media Ltd. will not accept any physical transfer (e.g. USB) of Personally Identifiable Information (PII) for use or exchange internally or externally on the data controller's behalf. Official data or PII will not be stored on solid-state drives or memory sticks.

Official-sensitive (or higher) data will be encrypted and any transfer signed off at Account Director level or above. All other data and communication will be treated as Official and handled securely.

Third party vendors

Where data is transferred to a third party media supplier (e.g. a digital network for profiling), Republic of Media would ensure the media owner uses a third-party data handler [redacted] so that all PII-style data is syndomised and anonymized. Vendors are audited and contracted to our Brand Safety standards and IAB Gold Standard IO which ensures they cannot utilise Framework data for reasons other than specified.

Demand Side Platform

Where Framework partners access [redacted] inventory, partner DMP or data will be kept entirely separate and 100% transparency view will be provided including partner access to the platform.

Data storage

Any PII data required to be stored is encrypted prior to upload to our cloud based storage. The cloud provider, or other third-party, is therefore unable to gain access to the personal data whilst it is stored in the cloud.

For both the safe transfer and accessible end point storage of PII, or confidential client data, our provider, adhering to the standards of E.U. General Data Protection Regulation (GDPR), is [redacted] is committed to complying with the E.U. GDPR for [redacted] Cloud Platform services. [redacted] delivers full disk encryption for all data at rest using AES256 or AES128.

Data is stored in shared, secured drives on our [redacted] Cloud servers with access limited to authorised Framework teams to reduce the chance of accidental or malicious access.

Data retention

Our Data Destruction policy mandates that we only keep data for as long as it is needed for the purpose it was collected (or for a further permitted purpose) and also:

- securely destroy outdated records (to US DoD standards), or on request/ end of contract
- optimise the use of space; and
- minimise the cost of record retention.

Exception management (e.g. data retained for litigation) is only at the approval of Managing Director [redacted]

Any employee who fails to comply with Data Policies may be subject to disciplinary action, up to and including dismissal. Staff contracts cover confidentiality as well as compliance with Data Policies.

3rd Party Contracts (e.g. with Outdoor media buyer [redacted]) extend the same levels of protection, destruction, confidentiality and compliance.

Network security and controls

Republic of Media operates a [redacted]. Wifi at each site is provided by [redacted] secured by [redacted]. All computers are domain joined and have firewalls enabled by our IT administrator. A Firewall [redacted] is placed at the [redacted] Remote workers have secured wifi connections from laptops to ISP Router/Firewall.

[redacted]s removed from devices and installation is by administrator approval and limited to a defined whitelist of secure products. Suppliers must provide regular security updates (patch management) across all operating systems and software. We use a third-party patch management solution [redacted]to install all operating system updates with [redacted]days of release.

Anti-malware software is installed on all computers, including malicious website scanning. Approved application whitelisting is used on all mobile devices. Phishing and anti-spoofing protocols are built into our Malware controls as well as staff training programme.

Complex password protocols require changes every [redacted]days and are monitored by administrators.

User controls ensure access is provided only to authorised individuals and provides the minimum level of access to applications, computers and networks.

Continuity and recovery

Republic of Media maintains two offices (Manchester and Edinburgh) with [redacted]. Each office acts as an always-on back up, recovery and continuity centre for the other. In the event of any loss of access to Edinburgh office data or facilities, all services would be provided from the Manchester office with no down time, as per our Disaster Recovery policy.

Disaster recovery is tested quarterly with the policy reviewed annually in April by the Board of Directors.

Republic of Media also has a **Cyber Incident Response Plan** which outlines the process of communication, response and recovery in the event of an incident.

Republic of Media is committed to due diligence in our supply chain and will responsibly audit and evaluate framework media suppliers to the standards of Schedule 1.