TRINITY
McQUEEN

Privacy Policy

Policy Reference:	POL21
IS Classification:	Trinity McQueen Business Confidential
Date:	01/10/2024
Owner:	Joint Managing Director

1. Definitions

"CLIENT" means a natural or legal entity or an authorised signatory thereof, to whom Trinity McQueen provides Services.

"Trinity McQueen" means Trinity McQueen Limited, with legal offices at Victoria Wharf, Sovereign Street, Leeds, Yorkshire, LS1 4BA, England.

"General Term and Conditions" or "Terms" refers to Trinity McQueen's terms and conditions of sale (separate documents).

"Services" refer to all services, including Software as a service (SaaS), access and hosting, support, consulting, development, design, recruitment, telephone research, face-to-face moderation and interviewing and other services delivered to CLIENT by Trinity McQueen or third parties.

"Software" means any proprietary SaaS Software made available to CLIENT as an inherent part of provision of Services. Software shall mean any proprietary SaaS Software and Platforms, which may include but shall not be limited to all modules, widgets and/or additional features.

"Participant(s)" shall mean any and all named or specified (by password or other user identification) individuals authorised by CLIENT in order to use the Services for market research purposes, regardless of whether the individual is actively using the Software at any given time. CLIENT and any employees thereof are considered to be participants.

2. Scope

The purpose of this document is to demonstrate to CLIENT the compliance and IT security measures Trinity McQueen has in place to protect the data and privacy of participants, in line with EU General Data Protection Regulations and the UK Data Protection Act 2018 (GDPR thereafter).

3. Personal Identifiable Information (PII)

When conducting market research, Trinity McQueen will collect and process 'personal data' and 'sensitive personal data', as defined by GDPR. This statement focuses mainly on obligations and measures (by both parties) to protect PII during market research activities. Although Trinity McQueen will handle PII, it only reports data in aggregated form. No PII will be returned to CLIENT. All Trinity McQueen market research outputs are anonymised, as recommended by GDPR and the UK Market Research Society Code of Conduct.

4. Parties responsible

Three parties are identified, each with their own responsibilities towards GDPR compliance and maintaining an acceptable security level when handling and / or processing personal and sensitive data:

4.1. Trinity McQueen, which applies organisational, software and technical controls through its processes and procedures (summarised in this statement), in addition to consent and privacy statements agreed to by participants, prior to any market research being undertaken.

4.2. Third parties or sub-processors contracted by Trinity McQueen to collect and process data on its behalf, see 7.9.

4.3. CLIENT, who ensures that any PII given to Trinity McQueen, for the purposes of market research, complies with GDPR: specifically, articles relating to permissions granted from customers for PII to be used for market research purposes and moreover, to security when sharing and / or transferring PII to Trinity McQueen.

5. GDPR compliance

Trinity McQueen, as a Data Processor, has taken measures to ensure it is compliant with GDPR, which became law in May 2018. Namely;

5.1. Lawful basis or grounds for processing personal data applies as all participants give consent before taking part in market research with Trinity McQueen;

5.2. The purpose of processing and the legal basis therein is communicated to all market research participants;

5.3. Where consent is given, Trinity McQueen ensures this is freely given, specific (to the topic being researched), informed (so participants have information on which to choose or decline to take part), with an unambiguous, indication with clear affirmative action made by the participant;

5.4. Categories of personal data being collected and processed are communicated to all participants;

5.5. Consent is obtained for each separate processing activity;

5.6. Separate consent is obtained for initial or preliminary market research, any re-contact and any recordings, use of photos and videos for market research purposes only;

5.7. Explicit consent is gained if PII is to be transferred or processed to a territory not considered adequate by the UK & EU authorities;

5.8. Participants are informed of the source PII originates from and whether it came from publicly accessible sources;

5.9. Participants are informed of PII retention periods or criteria used to determine retention periods;

5.10. Participants are made aware of their rights pursuant to GDPR i.e. right to withdraw consent at any time, right to complain to the ICO and the right to be forgotten i.e. be removed from any data set, aggregated or anonymised or removed from any PII consent list;

5.11. Information is published and / or circulated as part of the process of gaining informed consent. Information is provided prior to participation in the research or data collection exercise.

6. ISO27001: Accreditation achieved

Trinity McQueen achieved ISO27001 accreditation for its Information Security Management Systems (ISMS) for Market Research Services in November 2018. Certificate was issued on 14th September 2021 and is valid until 10th December 2024.

Certificate number: 110135

7. Organisational measures and controls

7.1. Information security governance

Trinity McQueen's Information Security Group (ISG) meets every month, using an agenda which corresponds directly with the controls laid out under ISO27001:2013. Group officers include the DPO, Joint Managing Director and external IT and ISO27001 accreditation consultants. ISG terms of reference include securing ISO27001 accreditation and GDPR compliance, within our Organisation Context and Scope policy. Risks, incidents and breaches are all logged on the risk assessment register and treated in order of priority.

7.2. Contact with relevant authorities

Trinity McQueen is registered with the UK ICO (registration number: Z3622081) and therefore follows the UK Data Protection Act 2018 and obligations therein, specifically pertaining to the market research industry. By appointment of the Market Research Society (MRS), an independent professional standards body, Trinity McQueen (as a company partner) adheres to its Code of Conduct for practicing market research in the UK. The Code of Conduct, a self-governing charter, has been the foundation of trust between market research participants, market research organisations and clients since the 1950s and upon which most of the EU GDPR is based. Trinity McQueen may contact the ICO or MRS for the purpose of consultancy or reporting illegal activity by CLIENT or unauthorised persons.

7.3. Human resource security

Disclosure and Barring Service (DBS) checks are undertaken independently on Trinity McQueen staff by our HR Manager. Trinity McQueen employees oblige to conform with a non-disclosure clause and duty of care obligations relating to Information Security in employment contracts.

7.4. Information security awareness training

All staff participate in monthly Information and Cyber Security Awareness training, using a subscription based service, called Bob's Business.

7.5. Data protection impact assessments (DPIA)
These are conducted by project managers before projects are started and are stored centrally on Trinity McQueen's management information system (CMAP), to ensure compliance with PII handling, storage and protection protocols.

7.6. Handling, storing and protecting PII
All PII is classified as confidential and is stored in separate client folders on the Trinity McQueen network. These folders are deliberately not backed up to mitigate unnecessary replication. Access to PII on the network is restricted to two project managers and our DPO only. Trinity McQueen operates a no removeable media policy. Stored PII is zipped and password protected at rest and prevented from unauthorised emailing via MS Outlook quarantine controls. Furthermore, Trinity McQueen staff are prevented from using web mail such as Gmail or Hotmail, via firewall settings.

7.7. Retention and deletion of PII
All PII is retained for the duration of the market research project (typically 6-8 weeks). The DPO is notified of all completed, invoiced projects at the monthly ISG meetings (via the management information system, CMAP). PII from all completed projects is deleted from the network within 4 working weeks, unless otherwise dictated to by CLIENT in a separate contract.

7.8. Transferring PII
Transfer of PII transferred between CLIENT, Trinity McQueen and third-party sub-processors is done so via sFTP.

7.9. Supply chain management
Trinity McQueen will use third party sub-processors to collect and process data on behalf of CLIENT. Trinity McQueen will only do so with the prior consent of CLIENT. All sub-processors are audited via Trinity McQueen's Supplier Information Security Assessments. All sub-processors need to provide evidence of GDPR compliance and / or ISO27001:2013 accreditation. A mandatory non-disclosure clause is included in contracts with all sub-processors, SaaS Software providers, freelancers and third-party infrastructure partners. All sub-processors are based in UK or EU.

7.10. Incident management
Incidents are logged and reported to the DPO for review at monthly ISG meetings for treatment. Data breaches are reported immediately to CLIENT and the ICO. There have been no PII data breaches at Trinity McQueen since the company was incorporated in 2013.

8.0 IT security measures and controls

8.1. Acceptable use of hardware and network
Acceptable use of internal systems and hardware is covered by Trinity McQueen's Acceptable Use Policy and each individual employment contract signed by all Trinity McQueen employees.

8.2. Development and testing
Non-Trinity McQueen proprietary software development by third parties is only performed on local devices. Staging servers are physically separated from production servers. Testing and deployment is performed by authorised personnel only. Trinity McQueen ensures third party proprietary software providers carry out functional, usability, design and vulnerability tests all of which are performed on separate servers.

8.3. Encryption

Communication between Trinity McQueen, participants and the third-party proprietary Software is encrypted via SSL/HTTPS. Trinity McQueen ensures that any third-party proprietary Software uses 4096 bit encryption keys. Passwords are always stored as hashes.

8.4. Data backup

All CLIENT non-PII data is backed up on ISO27001:2013 data centres in UK. Data backed up using AES 256-bit encryption on an MPLS backbone 10 Gig data network, fully resilient running at 99.999% uptime. All non-PII data is stored for 2 years, archived after 3 and automatically deleted after 7 years.

8.5. Business continuity

To ensure business continuity Trinity McQueen maintains the following parameters. Recovery Time Objective (RTO) is 6 hours according to P1 incidents as described. Recovery Point Objective (RPO) is 24 hours according to daily backups. The BCP and DR service has been tested in the last 6 months.

8.6. Network security

Trinity McQueen's network connection is protected using a firewall, all incoming ports are blocked. The server stack consists of a network of servers that do not allow incoming internet traffic, except when accessed via a secure (2FA) VPN connection. Network health is monitored 24/7 by independent IT service provider, Koris 365.

8.7. Patch management

Workstation software is administered automatically by Manage Engine Desktop Central. Monthly Windows server hardening is managed by independent IT service provider, Koris 365.

8.8. Hard drive encryption and mobile device management

In place on all laptops (BitLocker) and company mobile devices (via MS Office 365).

8.9. Anti-virus and spyware protection

Trinity McQueen devices and systems are protected with anti-spyware (ESET) and anti-virus tools (Open DNS Cisco Umbrella).

8.10. Server penetration tests

Trinity McQueen uses a third-party supplier to conduct a penetration test on the internal network bi-annually**.**

9. *Physical security and controls*

9.1 Physical allocation

Premises where the Trinity McQueen network servers are located are monitored 24/7 by CCTV and manned security personnel (provided by managing agent, Hartnell Taylor Cooke). Access to our premises is via fob (first line) and physical key and keypad security code (second line), which is changed every 90 days. Access to the 'server room' is restricted to the DPO, Administrator and Joint MD.

9.2. Removable media

Removable media has been banned at Trinity McQueen since 2017.

9.3. Re-use of hardware

Any data-containing equipment is reset to default and double-checked for any data or software traces afterwards by our independent IT service provider, Koris 365.

10. *Data collection statement and disclaimer*

In delivering Market Research Services for CLIENT, Trinity McQueen acts solely as the data processor, unless a prior discussion and agreement with client has taken place to alter this status. As the data processor, Trinity McQueen has been commissioned by the CLIENT and is carrying out research activities to a specification approved by CLIENT. When commissioned by CLIENT, Trinity McQueen may contact the customers and other participants to complete research activities. CLIENT is ultimately responsible for communicating with customers the type of data to be collected, the terms of the processing and the purpose of data collection. Trinity McQueen will often work with the CLIENT to make sure this happens in accordance with GDPR compliance guidelines.

VERSION HISTORY

Version	Date	Author	Summary of changes	Review date
1.0.	23/03/2018	Robin Horsfield	Originated statement	29/03/2018
1.1.	5/04/2018	Rachael Walsh	Reviewed statement	11/04/2018
2.0	11/06/2019	Rachael Walsh	Reviewed Statement	11/06/2019
2.0	03/08/2020	Rachael Walsh	Reviewed Statement	03/08/2020
2.0	29/07/2021	Rachael Walsh	Reviewed Statement	29/07/2022
2.0	09/05/2022	Rachael Walsh	Reviewed Statement	09/05/2023
2.0	17/08/2023	Rachael Walsh	Reviewed Statement	17/08/2024
2.0	01/10/2024	Rachael Walsh	Reviewed Statement	01/10/2025

POLICY APPROVAL

Approved By: **Robin Horsfield**
Job Title: **Joint Managing Director**
Date: **October 24**

END OF DOCUMENT