Rival Security FAQ

To be read in conjunction with Rival Technologies Privacy Policy and Terms of Use.

What is your level of security governance?

Rival Technologies take information security as a company-wide priority. We have a dedicated security team that runs and maintains the SOC2, ISO27001, and HIPAA program. The Manager of Risk and Compliance is responsible for the program and reports to the CFO to maintain an appropriate level of executive oversight and independence from the operational and engineering departments. As part of our security program, we maintain a defined information security framework that outlines our policies and procedures, a developed Business Continuity Plan, Incident Response processes, conduct Security Awareness Training and Initiatives continuously, and perform both web application and comprehensive penetration tests.

What security architecture do you possess?

Rival's platform is a web application that enables researchers to create communities and conversational surveys (chats). Researchers interact with the platform by building chats, engaging invited or recruited participants to those chats, and then analyzing the results of these conversational research activities. Amazon Web Services ('AWS') is used to ensure cloud data centers meet security and privacy best practices.

What regulatory requirements do you adhere to?

Controls are in place to meet the GDPR, CCPA, and COPPA requirements.

Who owns the data?

Rival collects and processes data on behalf of their customers. In legal terms, we collect and use any personal information as a data controller. All chat surveys are built mindfully to collect only the necessary amount of data required for the purpose of that chat survey. It is for research purposes only and will be reported on in-aggregate.

Rival Security FAQ Continued

Are there protection measures in place for products and/or services that are being tested prior to public release dates?

Research participants would click through a non-disclosure agreement (NDA) in the chat, which would prevent them from disclosing information about the products and/or services that are being tested.

Who will have access to customer data?

Employee access to the systems that hold customer data is assigned based on role and business need, and all access is ticketed and approved by management.

What steps are taken to ensure the security of data transmission?

All data is encrypted at rest and in transit using strong cryptographic algorithms, as mandated by Microsoft's O365 product and AWS KMS. The company holds strict key management processes and segmentation between development, test, and production environments.

Where is data stored?

Data is stored and processed in the USA, Canada, or Australia, at the choice of the customer.

What additional security measures, if any, are in the pipeline?

Rival Technologies complies with SOC 2 (Type 2) and HIPAA requirements and is also ISO 27001 certified. We are continuously monitoring, reporting, and maturing our security framework.

More questions?

Please email security@rivalgroup.io for all your questions. Please coordinate with your contact from Rival to set up a meeting.