KEY SURVEY SECURITY FACT SHEET

Hosting & Infrastructure

- Key Survey is hosted in a state-of-the-art, SSAE-16 compliant colocation provided by CenturyLink (formerly Savvis) in Massachusetts, USA.
- All servers are 100% owned and operated by WorldAPP, the provider of Key Survey.
- WorldAPP does not enlist the services of any third-party cloud solutions and does not outsource any support for our production infrastructure.
- Our services leverage a three-tier architecture, with tiers separated both physically and logically.
- The architecture includes scalable load balancing with no SPFs (Single Points of Failure).

Data Security

Data Storage & Encryption

- In-transit data is encrypted via 256-bit TLS.
- Our servers store client data for the duration of an account and up to one year after it closes.
- Data may be deleted upon account termination by the owner's request.
- In the case of an unlikely technical failure, backup processes allow us to restore data availability and access in a timely manner.
- Customer data is segregated using unique user IDs.
- Encryption at rest using 256-bit AES is available by request for the data stored on servers.
- 256-bit at rest encryption is standard for data stored in mobile apps.

Authentication & Access Management

- Customer data resides securely on database servers behind multiple firewalls.
- Our staff may access Key Survey customer accounts only if the account owner grants such access and only for the period the account owner specifies.
- Internal policies limit which employees may access customer accounts.
- All authentication activity is logged.

US: +1 781 849 8118 | UK: +44 (0) 1252 551 600

Backups

- WorldAPP performs daily, weekly, and monthly backups of the Key Survey platform, which are stored on our servers for seven days, four weeks, and 12 months, respectively.
- On-site and off-site backups are available.
- Off-site backups are encrypted with PGP.

System Stability, Assessment & Monitoring

- All of our systems are monitored on a 24/7 basis by experienced technical professionals.
- Intrusion Detection System is in place to monitor and log suspicious network activity.
- We hold regular penetration tests on a quarterly basis.
- We enforce strong quality gates during the software development life cycle.
- Our clients are contractually guaranteed 99% uptime.

Key Survey Security Policies, Compliance & Certification

- Key Survey passes annual checks by TrustArc as part of WorldAPP's TRUSTe's Privacy Seal certification, signifying that our privacy statement and practices have been reviewed for compliance with the TRUSTe program.
- All employees undergo criminal background checks and reference checks.
- The Information Security policies in place are based on the requirements set forth by ISO 27001 standards.
- WorldAPP has implemented the required processes to ensure the Key Survey platform is in compliance with the GDPR:
  - We incorporated the data protection clauses of the GDPR into our contract templates.
  - We developed policies and procedures to address data subjects' requests.
  - We keep the data processing records required by the GDPR.
  - We appointed a Data Protection Officer to assure well-defined data protection control.
  - We appointed Designlogic Limited as an official representative of WorldAPP in the EU.
  - We conduct GDPR compliance training for the persons who are authorized to process personal data within the company.
  - We have a well-established mechanism of regular policies review to guarantee compliance with the data protection legislation.
  - We provide our customers with several options for safe and legitimate personal data transfer.
  - We are constantly implementing additional technical and administrative measures to secure personal data.