EngagementHQ: Security & Compliance

Protecting your data is our highest priority

EngagementHQ is committed to complying with the standards of all jurisdictions in which we do business to provide a safe and accessible platform for your users. Here is how we're working to meet this commitment to information security and accessibility standards.

Compliance | Security | Privacy | Hosting | Accessibility | Compatibility

---

Compliance

ISO 27001

Our information security management system (ISMS) which underpins all of our operations has been successfully certified to ISO/IEC 27001:2013, the global standard for information security management.

GDPR

The European Union's General Data Protection Regulation (GDPR) protects European Union data subjects' fundamental right to privacy and the protection of personal data. Explicit consent is built into EngagementHQ, allowing the collection of personal details as well as the ability to respond to your data subjects' requests for access, correction, porting, restriction, or deletion of their data.

Security

We go to great lengths to protect the data we store for you.

Application

Our applications are continually monitored and tested for security weaknesses by our Engineering team. We perform regular and ongoing internal application security assessments to discover and mitigate potential weaknesses based on OWASP rating and methodology. We use automated tools as well as manual testing processes to make sure we are as secure as possible all of the time.

The operating systems and databases running our servers are continually monitored and patched with the latest security fixes by Rackspace. The web framework is

continually monitored and patched by our internal development teams. An independent third party carries out comprehensive Vulnerability Assessment and Penetration Testing (VAPT) of EngagementHQ once a quarter. Results of the latest VAPT are available upon request.

Data

All of the data created on the EngagementHQ platform belongs to you and your community, and as such, is governed by your policies. We retain data for the term of our contract within EngagementHQ and remove data from the platform within six months of a contract ending.

We have strict data access rules in place with detailed logging to prevent theft and misuse. Access is limited to key personnel involved in maintaining our services and support. Interaction with your data is only at your request. EngagementHQ provides role-based access controls with unique usernames and one-way password encryption to help you manage your own logins. SSL certificates and Single Sign On integration are available for further protection.

Data is stored within a mySQL database on AWS RDS with attachments stored within AWS S3. All data stored on AWS RDS is encrypted using AWS provided – AES-256-GCM encryption standards. Amazon RDS has multiple features that enhance reliability for critical production databases, including automated backups, DB snapshots, automatic host replacement, and Multi- AZ deployments.

Network

Our application is hosted on the large, Internet-scale, world-class infrastructure that benefits from the same engineering expertise that has built Amazon into the world's largest online retailer. AWS's networks are multi-homed across a number of providers to achieve Internet access diversity. We utilize the Amazon Virtual Private Cloud (VPC) to create an isolated ecosystem for EngagementHQ.

The AWS network uses proprietary mitigation techniques providing significant protection against traditional security issues such as Distributed Denial of Service (DDoS) Attacks, Man in the Middle (MITM) Attacks, IP Spoofing, Port Scanning, etc. Additionally, our inbound firewalls are configured to permit only the absolute minimum connectivity required to provide the service to our clients. Any changes to the access rules require authorization.

Privacy

Granicus makes no use of the personal information provided by your community. This is your data and we will only access this information to render assistance as part of a

support ticket. You have the power to [manage access directly](#) within the platform. Our [Privacy Policy](#) governs how we treat personal information on our platform.

Hosting

Infrastructure

Your EngagementHQ site is hosted on Amazon Web Services (AWS) infrastructure within your jurisdiction as below:

Country	Hosting Location
Australia	AWS, Asia Pacific (Sydney)
New Zealand	AWS, Asia Pacific (Sydney)
Canada	AWS, Canada (Central)
United Kingdom	AWS, EU (London)
United States of America	AWS, US West (Northern California)

AWS is the leading cloud services provider in the world. Their suite of products and services, security controls, scalability, reliability, astonishing number of datacenters, flexibility and continued innovation make them the absolute best choice for hosting in the cloud.

AWS cloud infrastructure meets the requirements of an extensive list of global security standards, including ISO 27001 and SOC. See the [AWS Compliance](#) page for more information.

Managed services

We have contracted Rackspace to manage our hosting environment 24×7. They provide us with operational and strategic support to ensure our systems are best-in-class, secure and available at all times.

Like AWS, Rackspace are a global company certified for a wide range of [international security standards](#) confirming their operations are safe and trustworthy.

Availability and disaster recovery

We guarantee 99.75% availability and our uptimes have historically remained above "three 9s" (99.9%). Our guarantee is backed by our SLAs. Even though we take all

conceivable measures to ensure our service to you is uninterrupted, as with life, major events completely beyond our control can interrupt our service. We take nightly backups and have a well-tested recovery plan in place to minimize potential disruption from major events.

Our Disaster Recovery plan is tested annually or when there is a major change in our environment, either to our infrastructure or application. Lessons learned from these tests are incorporated back into the plan.

Accessibility

EngagementHQ is compliant with version 2.1 of the Web Content Accessibility Guidelines (WCAG 2.1) to Level AA standards. An independent third party carries out a comprehensive Accessibility audit of EngagementHQ once a quarter. Results of the latest audit are available upon request.

While the guidelines set out in WCAG 2.1 recognize that it is not possible to conform for some types of content, we have undertaken a commitment to continually work on this and leverage new technology to further improve accessibility. We do this by keeping up to date with the latest advances in accessibility techniques and acting on recommendations from the quarterly audits. We also treat any issues identified by clients or participants as a matter of urgency and remain responsive to address the issues.

Device compatibility

EngagementHQ is designed for small and large screen sizes, providing an accessible and full functionality experience for the community from mobile phones, tablets, and desktop devices. EngagementHQ supports the full range of major browsers including:

- Microsoft Edge

- Chrome 40 and above

- Firefox 35 and above

- Safari 7 and above