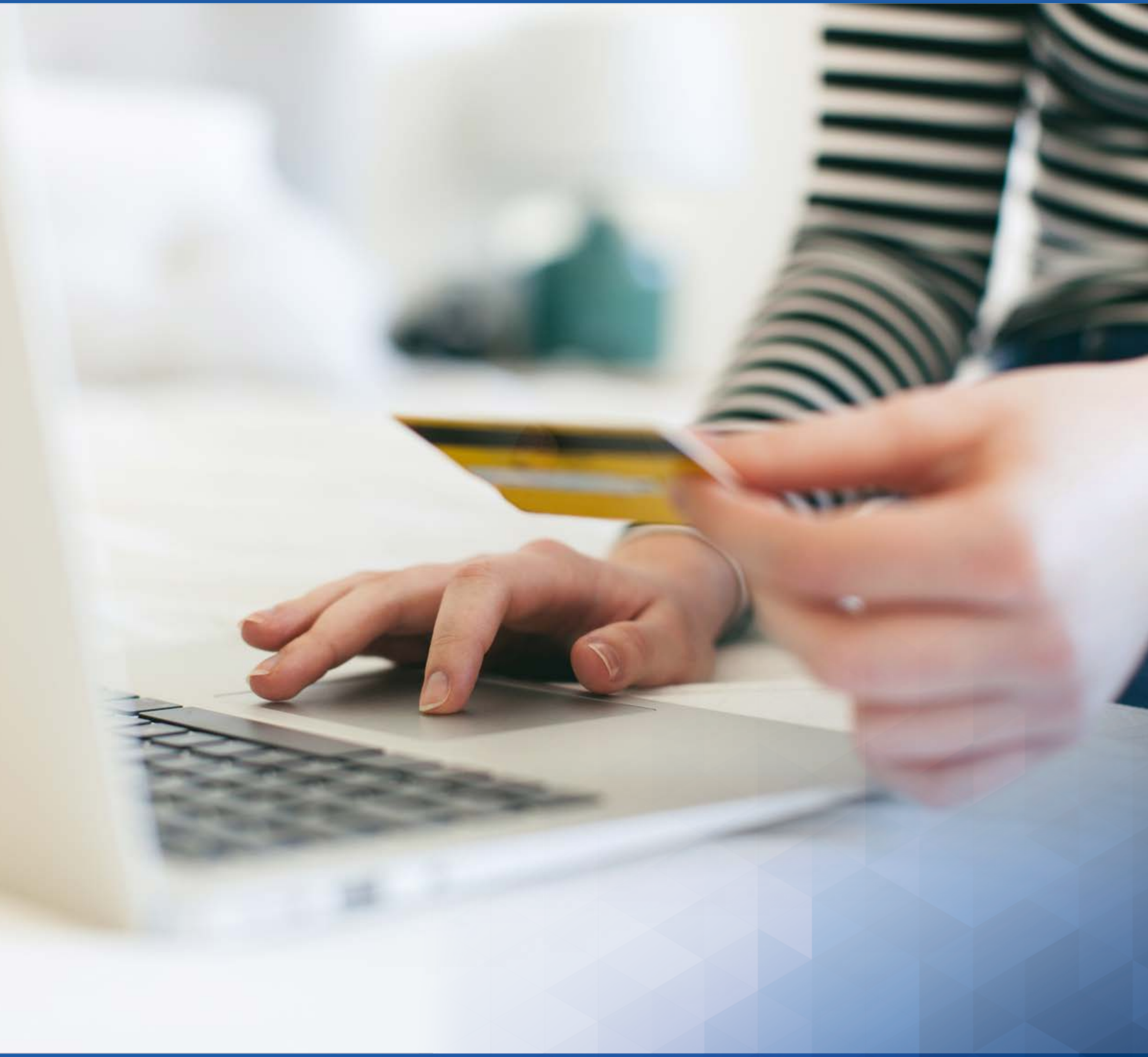
GIGYA

Information Security and Data Privacy Practices



Information Security and Data Privacy Practices

Introduction

As a leading SaaS Customer Identity & Access Management provider for enterprises, Gigya is committed to maintaining only the highest level of performance and security. Our platform is optimized to deliver maximum efficiency and scalability while protecting your data with a series of strict security and compliance standards. This executive summary provides an overview of Gigya's standards for the following four categories:

- Infrastructure: Our state-of-the-art data centers provide optimized performance and scalability.
- Data Security: ISO 27001 and ISO 27018:2014 certification and multiple levels of security protect your data with both physical and virtual safeguards.
- Compliance: Regional privacy compliance and built in social network terms of service functionality ensure responsible data management.
- Privacy Policies: Increased transparency of data practices fosters consumer trust and relationships.

Infrastructure

Gigya's robust infrastructure guarantees unprecedented performance and scalability with continuous data backup and constant protection.

State-of-the-Art Hosting and Physical Security

Gigya owns and operates its main U.S. server farm, hosted by one of the top data center providers in the world, Equinix. The Equinix data center is SSAE16-certified and is fully equipped with generator-backed UPS and redundant HVAC systems, as well as fire suppression, flood control and seismic bracing solutions to protect your data in the event of a power outage or natural disaster. The data center also enforces high security protocol, including 24x7 armed guards, multiple biometric checkpoints and full CCTV surveillance.

For more information about Equinix security and infrastructure, please visit: http://www.equinix.com/platform-equinix/platform-advantages/ibx-data-centers/

In 2016, Gigya opened another primary data center within the Russian Federation. With hardware wholly owned and operated by Gigya, this facility enables our clients with Russian customers to comply with that government's data residency requirements while ensuring that attributes stored in Russia remain discrete from all other international data.

Gigya also hosts multiple AWS (Amazon Web Services) virtual data centers in Ireland for European companies that prefer to store their data within the EU, and virtual data centers in Sydney, Australia are available for the APAC market. A full disaster recovery environment for the U.S. server farm is also maintained.

For more information about AWS security and infrastructure, please visit:
https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

Redundancy

Gigya supports full disaster recovery in the rare case of a data center outage. This includes real-time data replication to a separate physical location and transfer of critical data on-premise to provide continuous service and transparent recovery, with no data loss, in the case of hardware failure.

In the U.S., data centers are located in disparate geographical locations. The DR site has the same components and functionality of the production site and is updated upon any change in production. In order to verify the DR functionality and readiness, Gigya runs automated hourly sanity checks on the DR site.

In the EU and AU, Gigya utilizes AWS with two different availability zones for all offered services, where both availability zones are active and serving customers.

In Russia, Gigya utilizes two Selectel data centers located in disparate geographical locations, both are active and serving customers.

Performance

Gigya's platform was designed to scale horizontally on commodity hardware. Servers never exceed 20% utilization under normal circumstances, providing 5x capacity reserves in order to accommodate unforeseen spikes in traffic. Our performance is proven both by our regular handling of large bursts of traffic during some clients' live and breaking news events and by the many enterprise companies leveraging our platform to manage more than half a billion user identities.

Data Security

Gigya is ISO 27001 and ISO 27018:2014-certified and is registered with IQNet. Gigya invests considerable resources to ensure that the assets our customers entrust to us are safeguarded at all times by employing industry best practices and consistently keeping our information security management system and security practices up-to-date with the latest and most stringent policies and regulations.

Gigya has published a very detailed Self-Assessment Report to the Cloud Security Alliance STAR program in order to allow our customers to review our compliance with current security and privacy best practices.

Application Development Security

Security considerations play an integral role in every step of the product development process. During product specification, technical design, development and testing, security measures are continually tested, optimized and implemented. Gigya uses the OWASP top 10 list as a high-level security guideline during development.

OWASP guidelines can be found here:
https://www.owasp.org/index.php/Main_Page

Security At Rest

By default, Gigya encrypts all PII and other sensitive data at rest using the AES-256 algorithm, and hashes passwords with the NIST-approved PBKDF2 algorithm. In addition, to further protect access to the data, Gigya uses HMAC-SHA1 to digitally sign its requests and requires customers using the APIs to sign their requests to Gigya servers with the same algorithm. Alternatively, Gigya offers API access that is fully OAuth 2.0-compliant.

Access to information via Gigya's Administration Console is also protected through a two-factor authentication process and a powerful roles and permissions architecture, providing site administrators granular control over what individual Console users can see and use.

Security In Motion

Gigya uses a secure channel (TLS) when transferring sensitive data to and from its servers. In addition, REST API calls that perform critical operations, such as deleting users, are only permitted as server-to-server signed requests.

Compliance

Gigya maintains compliance with trusted organizations and social networks to ensure responsible data management.

Regional Privacy Regulations

Gigya offers multiple data centers (U.S., EU, AU and Russia), helping our multinational client base to meet in-region storage requirements. As a global company, Gigya is committed to safeguarding the privacy of its customers' PII (Personally Identifiable Information) according to local and international privacy laws. Gigya tracks relevant privacy regulations and any changes to those regulations, evaluating and addressing any impact they may have on the Gigya platform or Gigya's clients.

PCI DSS

Gigya does not collect, store, manage or transfer any credit card data on behalf of our customers, and is therefore not subject to the Payment Card Industry Data Security Standard.

COPPA

Though responsibility for complying with the Children's Online Privacy Protection Act (COPPA) falls to Gigya's customers, Gigya helps facilitate COPPA compliance by enabling age-gating for site access and preventing the storage of PII for users under 13 via our Registration-as-a-Service product. In addition, Gigya customers do not need to be concerned about COPPA compliance as a result of loading Gigya's JavaScript library, as Gigya never amasses user profiles across websites and only cookies users to the extent necessary for internal reporting and service support.

Social Network Policies

Gigya offers several tools to help our customers maintain social network policy compliance. These include:

Automatic Account Deletion: If a user revokes data access permission from a site's Facebook app, then all of his non-public profile information will be deleted from the site's database.

Automatic Account Updates: If a user logs into a site using Facebook and later updates his Facebook profile, his profile information will also be updated in the site's database to ensure the data is always fresh and up-to-date.

Security Tests and Audits

In order to test the security of the Gigya solution on a regular basis, Gigya has implemented several methodologies and practices to tighten the security of its offerings:

- Annual ISO 27001 and ISO 27018:2014 internal and external audits as part of the certification process.
- An automated vulnerability scan is performed once a month using a PCI Approved Scanning Vendor.
- Third-party security experts are contracted once a year to conduct extensive black-box penetration tests on Gigya's infrastructure.
- An international Bug Bounty program allows and encourages security researchers to test for and responsibly disclose potential vulnerabilities in the platform on an ongoing basis.
- Gigya uses an onsite state-of-the-art Automatic Static Code Analysis software to check for security weaknesses and vulnerabilities in its code base.

Penetration Tests

Special focus is naturally directed toward extensive application level penetration tests. These are conducted once per-year by third-party security experts as white-box penetration tests on the Gigya platform, based on the widely accepted OWASP methodologies.

Testing of security elements (potential and actual security flaws) that may enable various attacks by external attackers or malicious system users include, at the minimum:

- Unauthorized access to sensitive information tests
- Unauthorized modification of information tests
- Unauthorized deletion of information tests
- Unauthorized handling of audit information tests
- Performing of unauthorized operations or transactions
- Illegal impersonation of different users or entities
- Performing of unauthorized operations that will cause a Denial of Service (DoS)
- Exploitation of existing security controls to perform fraudulent activity

Gigya also welcomes its customers to perform their own penetration tests with prior coordination and scoping with us. Gigya will strive to fix any real security exposures found and properly disclosed to us in agreed upon time tables.

Privacy

Gigya operates according to strict privacy principles and is dedicated to building trust between our customers and their end users. We provide several tools to increase data collection transparency and inform users of how their data is being used.

Permission-based Social Login

When choosing to log into sites using their existing social profiles, users are shown a dialogue asking permission to access specific data points, such as their birthdays or locations, giving users total control over the information they share.

User Data Controls

When leveraging Gigya's Registration-as-a-Service forms for user registration and login, sites can easily expose functionality to their end users, allowing them to 1) download the data the site is storing in order to edit or delete that data as needed, and 2) delete their site account if they so choose.

Customizable UIs

All self-service forms are 100% customizable, enabling clients to include privacy notices, terms & conditions, marketing opt-ins, account preference fields and other notices in the UI.

Administrator Roles & Permissions

Gigya provides robust Roles and Permissions functionality that enables administrators to control the features and data that can be accessed by internal users. An administrator can create user groups and assign access on a very granular level, including by site/app ID, specific service and even API, ensuring end user PII is protected.

Additional Security Practices and Controls

Internal Access Control

Gigya has implemented access control and authorization mechanisms that are enforced at all levels of the information systems (application source code, operating system, database and the network level). Gigya employees are granted specific permissions based on their roles according to the 'least privilege' principle.

System Security Practices

Gigya's system security practices include: server and workstation OS hardening, patch management, auditing and event logging, and malware protection. Gigya also uses a provisioning system that automatically enforces the secure configuration and state of critical system settings and services. All management operations are executed over VPNs using Two-factor Authentication for admins.

Network Security Practices

Gigya's network security practices include: opening minimum necessary ports, segregating networks (production, development, testing environments), out-of-band secure network device management interfaces and network device hardening.

DDoS (Distributed Denial of Service) mitigation

Gigya uses a state-of-the-art anti-DDoS solution on premise for its U.S. data center combined with a cloud based DDoS mitigation service provider in the unlikely case there is a need to handle an extreme volume of traffic. For its AWS data centers Gigya relies on Amazon's ability to scale up in order to handle the increase in traffic.

Change Management

Gigya has a well-documented and organized change management approval and implementation process that is the key to an efficiently managed and secure service delivery.

Vulnerability Management

Since new security vulnerabilities are discovered on a daily basis, Gigya has adopted an information gathering process that includes the constant monitoring of relevant vendor security publications, security forums, communities and security alerts (e.g. US-CERT, BugTraq), issued by key industry players for newly published vulnerabilities.

Monitoring

Gigya provides both automatic and manual monitoring 24x7x365. Gigya's Network Operations Center team monitors every aspect of its services, down to the individual API level on every provider.

Routine manual tests on key aspects of Gigya's services occur every 15 minutes. Gigya sets predefined thresholds and events and adjusts capacity accordingly. This is relevant also in case a customer notifies Gigya in advance of certain upcoming events that require this customer to receive more resources for a specific point in time.

Backup and Recovery

Gigya employs a multi-layer data loss protection architecture with special emphasis on short MTTR (Mean Time to Recovery) in case of failure. All data is replicated in real time to standby servers in a secondary data center providing at least n+1 redundancy in two geographic regions. Critical data is also replicated on premise to provide n+2 redundancy and allow for immediate and transparent recovery, with no data loss, in case of hardware failure. In addition to these measures, disk snapshots and offline backups are also regularly taken. Gigya performs extensive restore tests twice per-year.

Business Continuity Plan / Disaster Recovery Plan

Gigya has a BCP with an RTO (Recovery Time Objective) of 15 minutes and RPO (Recovery Point Objective) of a few seconds, since data is replicated to standby systems in real time. Gigya performs extensive DRP tests twice per-year.

Incident Management

Gigya acknowledges that each security incident may require different treatment, depending on its nature, source, and potential impact. However, the general process of responding to a security incident will consist of the following steps:

- Immediate Response
- Information Gathering
- Root Cause Analysis
- Categorization
- Establishing a Response Plan
- Action (implementation steps)
- Conclusion and Learning
- Implementation of Corrective and Preventive Measures

About Gigya

Gigya's Customer Identity Management Platform helps companies build better customer relationships by turning unknown site visitors into known, loyal and engaged customers. With Gigya's technology, businesses increase registrations and identify customers across devices, consolidate data into rich customer profiles, and provide better service, products and experiences by integrating data into marketing and service applications.

Gigya's platform was designed from the ground up for social identities, mobile devices, consumer privacy and modern marketing. Gigya provides developers with the APIs they need to easily build and maintain secure and scalable registration, authentication, profile management, data analytics and third-party integrations.

More than 700 of the world's leading businesses such as Fox, Forbes, and ASOS rely on Gigya to build identity-driven relationships and to provide scalable, secure Customer Identity Management.

To learn how Gigya can help your business manage customer identities, visit gigya.com, or call us at 650.353.7230.

GIGYA | The Leader in Customer Identity Management

© 2016 Gigya, Inc. | 2513 Charleston Road #200, Mountain View, CA 94043 | T : (650) 353.7230 | www.gigya.com

Gigya does not own any end user data or maintain any other rights to this data, other than utilizing it to make Gigya's services available to our clients and their end users. Gigya acts as an agent or back-end vendor of its client's website or mobile application, to which the end user of our client granted permissions (if applicable). Gigya facilitates the collection, transfer and storage of end user data solely on behalf of its clients and at its clients' direction. For more information, please see Gigya's Privacy Policy, available at http://www.gigya.com/privacy-policy/.