OMATIC'S GUIDE TO SECURITY AND PRIVACY STANDARDS

Introduction

The integrity, safety, and security of your data is critical to amplify your mission and must be a prerequisite to earn your trust as a partner. We value and protect your data as if it was our own.

Our Security Culture

Omatic has established a security culture for all team members that spans the entire employee life cycle from the first steps of recruitment, through the hiring and onboarding process, and as part of the ongoing training to raise awareness.

Team Member Background Checks

Omatic has a robust interview process that verifies each potential team member's education and previous employment, and performs internal and external reference checks. We conduct a background check on each new team member.

Security Training

All Omatic team members undergo security and HIPAA training as part of the onboarding process and receive ongoing security training throughout their Omatic career. Depending on their job role, additional training on specific aspects of security may be required that cover aspects on best practices, product design, and testing. We live by our 12 principles of Security.

Leadership Support

It starts at the top. Our executive and extended leadership teams are committed to assessing, monitoring, and managing risk for security and vendors through a formalized risk management framework.

Our Security & Privacy Team

Finally, we have a cross-functional security and privacy team dedicated to maintaining the company's defenses against attack, monitoring our security, educating Omatic's team members on security and compliance standards, and reviewing all policies, procedures, and controls based on current and future changes to our compliance standards and business strategy.

Security Embedded Within Our Operations

Security is an integral part of our operations, not just an annual event.

CLOUD ENVIRONMENT

SECURITY CHECKS

IDENTIFY THREATS

Vulnerability Management

We actively scan for security threats using a combination of technologies, processes, and tools. Omatic leverages Microsoft Azure Security Center to secure our workloads in our cloud environment, assess compliance, scan our container images for vulnerabilities before deployment, and quickly identify threats through real-time monitoring. In addition to the Security Center, we use commercially available vulnerability scanning tools to proactively identify issues with our web endpoints. Our processes also include manual quality assurance and security checks. Since internal audits and scans are not enough, we engage with third-parties to perform external penetration tests.

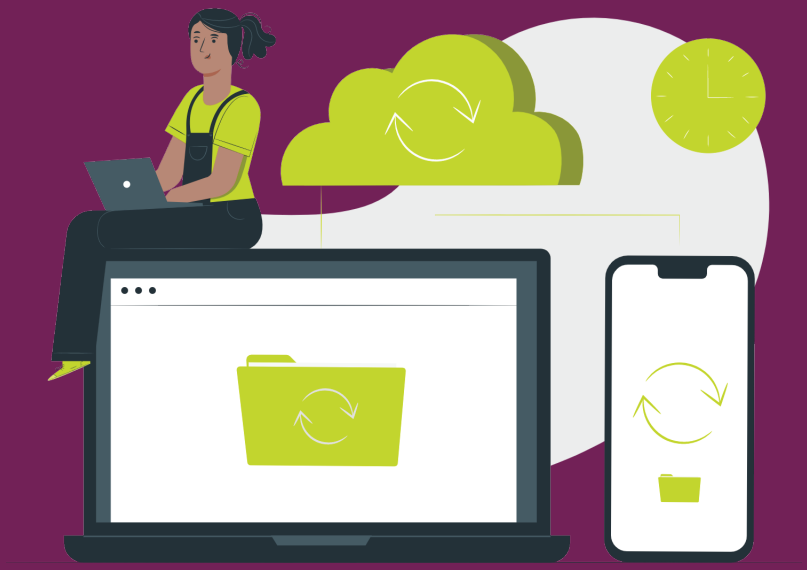
Rest assured, in the event that we should identify a vulnerability, our team will track and follow-up until we have remediated the vulnerability.

Monitoring

Omatic's security monitoring program is focused on information gathered from our internal network traffic, employee actions on systems, and outside knowledge of vulnerabilities. We consider all internal and external network data "untrusted" and inspect the data for suspicious behavior. Omatic leverages tools provided by Microsoft to detect suspicious behavior across all our systems and internal tools.

Change Movement

Omatic has developed and follows a defined process for the design, development, testing, and release of its service as part of our SDLC and change management policy. Multiple checkpoints and approvals occur to ensure separation of duties. Changes to our infrastructure are tracked through a formal process.



Incident Management

We have a robust incident management process for security events that may affect the confidentiality, integrity, or availability of your data or systems. Our incident response team will quickly assess the actual or potential impact and execute on a plan to mitigate the incident. The process includes containment to limit exposure, eradication of the root cause, recovery of key systems if affected, and documenting and enacting on lessons learned. Testing of the incident response plan occurs regularly. If an incident involves customer data, Omatic will inform the customer and support investigative efforts.

Business Continuity / Disaster Recovery

Omatic has also implemented a business continuity and disaster recovery plan for the production environment to recover and restore the system infrastructure in event of permanent or long-term loss of a data center. We test our plan annually, identify gaps, and take steps as necessary to update our plan.

Security as a Central Part of Our Technology

Omatic Cloud leverages Microsoft's Azure cloud services. Since we use Azure, Omatic operates under a shared security responsibility model, where Microsoft Azure handles the security of the underlying cloud infrastructure (i.e., physical security, host infrastructure, network controls) and Omatic secures the platform deployed in Azure (i.e., customer data, identity and access management, client and end-point protection).

High Availability

Leveraging Azure cloud services allows Omatic to focus less on managing physical hardware and securing physical environments, and focus more on managing the availability and scalability of the services. We are deployed into four different regions and can switch traffic between the east and west coast of the United States.

Data Stays in Your Country

For our Canadian and UK clients, you may need to simplify compliance with data and privacy regulations by keeping data within your country. Omatic Cloud will provision your instance so that all data transfer and storage occur within your borders.

Access to the System

Omatic Cloud also uses Auth0, an identity management platform, to manage authentication with the Omatic Cloud and enable support for Single Sign On with your organization's identity provider. This will allow you to define your password rules and use multi-factor authentication.

Securing Data in Transit and at Rest

Data is vulnerable to unauthorized access as it travels across the Internet or within networks. Securing your data is a top priority for Omatic. We support strong encryption protocols such as TLS 1.2 to secure the connection between all services and clients. We also encrypt all data storage using AES-256 through our primary database Cosmos DB. All databases and backups are encrypted, giving you end-to-end encryption.

Our Third-Party Certifications

SOC 2

We're committed to handling our user and partner data securely, so Omatic has completed our annual third-party SOC 2 Type II audit where an independent auditor has evaluated our product, infrastructure, and policies, and certifies that Omatic complies with their stringent requirements. The SOC 2 (System and Organization Controls) Type II report is a globally recognized security measure that rates a service provider's compliance with security, availability, and confidentiality best practices.

HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that establishes data privacy and security requirements for organizations that are charged with safeguarding individuals' protected health information (PHI). These organizations meet the definition of “covered entities” or “business associates” under HIPAA.

Many of our customers are subject to HIPAA and can use the Omatic Cloud by executing a Business Associate Agreement (BAA) with Omatic. We ensure that the Omatic Cloud meets the requirements under HIPAA and align with our SOC 2 report.

Our Commitment to Your Data

You own your data, not Omatic. The data you process through our system is yours, and we do not scan it for advertisements or sell it to third parties.

We only process data for the purpose to fulfill our contractual obligations with you. We only keep your data in our system if there is a business purpose.

Should you choose to stop using our services, we will delete the data from our systems within 90 days.

Conclusion

The protection of your data is a primary design consideration for the Omatic Cloud and team member operations. As a Microsoft Gold-Certified Partner, we have access to a leading-edge technology stack that offers a significant level of protection, scale, and availability. For these reasons, many social good organizations across all Mission Focuses including Healthcare, Cause and Cure, Higher Education, K-12, Arts and Culture, Faith-Based, National Organizations, Animal Welfare, and Family and Human Services put their trust in Omatic to help them leverage the best of technology and security so they can easily access current, clean and complete data driving insight to empower and amplify their missions around the world.

omatic

Turn data into connections.

Contact us to learn more.

info@omaticsoftware.com
omaticsoftware.com
888.662.8426