Version 1.0 | Feb 2018

Security Policy

Open Social

Index

Open Social Security

Open Social, as all software products should, has taken a no-compromise approach towards security. Protecting and securing our customer's data is of utmost importance to us.

We have multiple layers of defense to protect data from leakage, deletion, and theft. We also strive to protect the integrity, confidentiality, and availability of our customer's data. Our practices and software ensure a high level of security for all projects.

Our key objectives are:

- Ensuring customer data protection and trust.
- Minimizing security risks and vulnerabilities threatening the data.
- Compliance with international and industry standards.

This page provides an overview of our security measures and practices. If you have any questions, please contact security@getopensocial.com.

Your Data is Kept Safe

Open Social has elaborate and certified hosting platforms, deployments, and backups that protect both your own data and your customers' data.

Certified Hosting

Open Social uses cloud hosting rather than on-premise hosting. Security responsibilities are shared between the company, Open Social, and the cloud service provider. **This means that our hosting platforms, Platform.sh and Amazon Web Services, are responsible for securing the underlying infrastructure of Open Social.** And Open Social is responsible for any security measures on top of that. This shared security responsibility model provides your data with a secure default security.

Hosting your data with Open Social has the following benefits:

- **You can choose from three different hosting platforms.** We have hosting services from Amazon Web Services, Platform.sh, and Microsoft's Sovereign Cloud.
- **Your data can be hosted in both the EU and US.** This ensures that our customers comply with regulations and laws of a specific country (read more about it here).
- **Your data is protected by multiple layers of security.** Each hosting platforms comes with various advantages and secure infrastructure. Continue reading for more information.

Platform.sh

Open Social receives hosting services from Platform.sh, a continuous deployment cloud hosting solution for web applications. Here's an overview of how the Platform.sh security measures for Drupal 8 keep your data safe:

- **Service isolation.** Each service is deployed in an isolated LXC container that is protected by network firewalls.
- **Read-only file system.** Application code is deployed on a read-only file system and safeguards against attacks on PHP files.
- **Protective block.** This block identifies and prevents application vulnerabilities. It restricts access to websites with security vulnerabilities.
- **Environmental variable management.** Open Social has a high degree of control over the build process and runtime environment of their platforms.

Deployment

Open Social is hosted on Amazon Web Services (AWS), a platform that maintains a rigid security program and has a world-class facility infrastructure. It deploys a comprehensive security architecture for Open Social:

- **Network security.** AWS provides services to increase the privacy and control of network access.
- **Inventory and configuration management.** The tools provided by AWS comply with organizational standards and best practices.
- **State of the art data centers.** AWS data centers are built using innovative architectural and engineering processes.
- **Data encryption.** AWS adds a layer of security to your data with various encryption features, such as EBS, S3, Glacier, Oracle RDS, SQL Server RDS, and Redshift.
- **Access control.** Open Social deploys AWS access controls for backups, which define, enforce, and manage user access policies.
- **Monitoring and lagging.** AWS has tools that help Open Social see what's happening in their AWS environment.

The data stored in the AWS data centers are housed in nondescript facilities, and have the following characteristics to keep your data as safe as possible:

- **Controlled physical access:** access is controlled with video surveillance, intrusion detection systems, professional security staff , and two-factor authentication.
- **Fire detection and suppression:** automatic fire detection and suppression equipment.
- **Power:** electrical power systems are fully redundant and maintainable 24 hours, 7 days a week.
- **Climate and temperature:** climate and temperature are constantly controlled.
- **Management:** preventive maintenance and electrical, mechanical, and life support maintenance.

Backups

Open Social has multiple environments for back ups to keep your data safe from loss or deletion. Platform.sh backups consist of snapshots that are stored on Platform.sh servers and have a retention of 7 days. This serves as a backup feature for clients. It consists of all the relevant files including: application, site-specific, and database. Data only backups are stored off-site in an external data-center. All backups contain the data needed to restore the site on any given hosting provider.

Additionally, we have an automated process that creates, stores, and encrypts copies of all Open Social platforms. This provides additional assurance that no information will be lost. We can also restore data quickly! Backups are stored off-site at the AWS S3 EU Frankfurt location. Each client has their own folder and cannot access the backups of other clients.

Customer Data Protection

Open Social has a user-centered design, in which user privacy and freedom of choice have been at the forefront of our activities. We are well aware of the General Data Privacy Regulation (GDPR) that will become operative on the 25th of May, 2018. The GDPR is an upcoming EU legislation that serves to enhance the protection of the personal and private data of EU citizens. Although Open Social is naturally compliant with most of the GDPR, in the upcoming months we will ensure that Open Social has full compliance. Read about our progress here.

Protected Against All Known Vulnerabilities

Open Social is designed to protect all information by ensuring the maintenance of our software, adhering to strict security advisory policies, and patching against all known vulnerabilities.

Our Security Practices

Open Social employs a number of security practices to ensure that every project and its data is secured. These practices are summarized below.

Limited Access to Data

There are only a small handful of people that can access the production data and update the website. Access to the website is carried out using secure connections only.

We also have role-based restrictions on the community platform, for example the administrator user cannot be edited by anyone, normal users do not have access to site management features (e.g. viewing, editing, or deleting users), and site managers do not have access to features they don't need access to.

Updating Third Party Code

We have weekly security update window with Drupal that ensures regular monitoring of our code. There is a team ready if any security fixes need to be implemented.

Code Reviews

Open Social conducts peer reviews of code to ensure that none of the code is deployed without at least two people looking at it first. On top of that there are automated reviews that regularly check for common security pitfalls and a process that prevents the addition of dependencies that have known security vulnerabilities in it.

HTTPS Connections

Open Social uses HTTPS connections. A SSL certificate is provided for every installation at no extra cost for our customers.

Update Processes

Open Social has a secure server that can automate the deployment of new releases. Moreover, we regularly update and maintain Drupal modules to ensure security.

Password Security

Administrative accounts use strong passwords only and are only available to a handful of people.

Experienced Team

Open Social has an experienced team to ensure that all security process and practices are running smoothly. The team has experience with large scale projects that involve over hundreds of thousands of users. They understand and implement common security measures. The Open Social team also develops and/or reviews code that runs on the Open Social platforms themselves.

Software Maintenance

Open Social is hosted on Drupal, one of the most popular open source content management systems. Drupal has a mature framework for application security, providing the following security benefits for Open Social:

A network of support

Open Social benefits from the security support provided by the Drupal security team and thousands of developers worldwide. Open collaboration from the Drupal community ensures that potential vulnerabilities and design flaws are flagged way quicker than programs built on proprietary software.

Security clearance

Open Social has security clearance from the Drupal security team. This means the following has been conducted on Open Social's code: an automated test for security implications, a manual review by the Drupal community, and a final check by the Drupal security team.

Security updates

Open Social and Drupal security updates always go through without prior customer approval. This is to ensure that the application and hosting environments are not at risk.

Drupal 8 Security

Open Social is built on Drupal 8 (the newest version of Drupal), which implements multiple measures to protect your data against attacks such as SQL injection, CSRF, and XSS. All developers are encouraged to avoid vulnerabilities by using a set of secure APIs, which minimizes the exposure to these attacks. See below for a list of Drupal 8 security measures that apply to Open Social.

- Avoids exploitation of XSS attacks.
- Executing server side code is practically impossible.
- SQL Injection vulnerabilities are avoided.
- Session hijacking is impossible with Drupal's HTTPS connection.
- The Twig theme engine avoids bad practices and ensures security in the front-end.
- Trusted host patterns are used to avoid hijacking of the HTTP host directive.
- Improved user passwords by stretching the passwords.
- Users are encouraged to serve their website on an HTTPS-only connection and the mixed mode SSL was removed.

Drupal Security Advisory

Drupal has a mature process in place to detect vulnerabilities in the Drupal core or contributed projects. A private issue is created and reported to the Drupal security teams for

any found vulnerabilities. The impact of this vulnerability is reviewed and evaluated. If it poses a threat, the security team and any associated maintainers update a new release that fixes the security vulnerability. Finally, a security advisory is issued so that site owners can address issues quickly.

Meet Compliance Requirements

Your data is stored in both the cloud and in physical locations in the U.S. and Europe. These different locations enable you to comply with the relevant security and data protection laws of your country.

Local Compliance Standards

All Open Social data is hosted in secluded servers rooms in AWS data centers located in the U.S. (US-Amazon) and Europe (EU-1 Amazon). Our customers can choose to store their data in one of these clouds, ensuring that their data complies with the relevant and local legislation, for example in the field of security, data protection, privacy, personal data, reporting obligation data leaks, and the like.

Europe

In Europe, our customers' data adheres to the EU Data Protection laws and any upcoming regulations that fall under the GDPR. View the EU Data Protection website from AWS to learn about how AWS ensures its own and contributes to our compliance with the local EU data requirements.

Open Social also offers Sovereign Cloud Hosting through Platform.sh due to their cooperation with Microsoft. These sovereign clouds ensure that customers meet the data requirements and necessary certificates of a specific country. For example, the Microsoft Cloud Germany offers data centers and strict data protection measures that are in line with both German data laws and regulations and international standards.

United States

In the U.S., there is no single, comprehensive law regulating the use and collection of personal data, however there are guidelines and frameworks that are considered 'best practices'. AWS ensures that your data is handled and stored in alignment with these best practices and IT security standards.

All data will comply with the following American and European regulations and alignments:

- CISPE
- EU MODEL Clauses
- FERPA
- GLBA
- IRS 1075
- U.K. DPA
- EU Data Protection Directive

AWS Compliance Program

AWS has a compliance program in place to maintain security and data protection in the cloud. These are the security certifications that apply to Open Social:

- C5
- Cyber Essentials Plus
- DoD SRG
- FedRAMP
- FIPS
- ISO 9001
- ISO 27001
- ISO 27017
- ISO 27018
- PCI DSS Level 1
- SOC 1
- SOC 2
- SOC 3

Read more about AWS certifications on the AWS compliance site.

Scope and Use

Open Social values transparency in our services and solutions for customers. This page has been created with transparency in mind. We are continuously improving security measures and data protection, therefore this page will be updated regularly to communicate updates and changes.

If you have any questions, then please contact security@getopensocial.com.

Additional Reading

- Embracing Open Source Security with Drupal
- Keep Your Community Safe with Backups
- Drupal Security Advisory
- Amazon AWS Security Policies
- Platform.sh Protective Block