Where and How Data is Stored

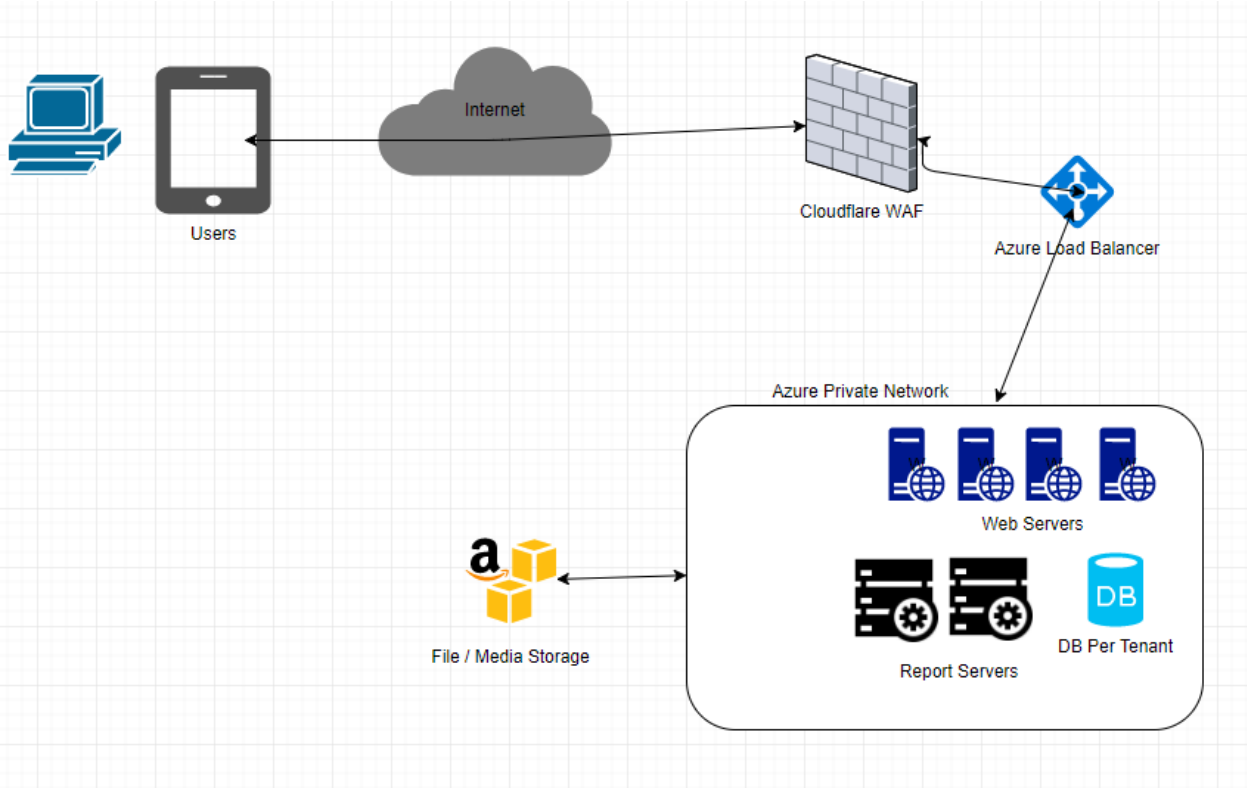
Technology

The OpenWater Platform is a proprietary system built on Microsoft .NET technologies. Its basis is 100% custom and is not derived from a popular system (e.g. DotNetNuke). As such it is not vulnerable to threat vectors often in the news (e.g. WordPress, Drupal, DotNetNuke vulnerabilities).

The basis of the platform is Microsoft ASP.NET MVC with Entity Framework and is kept up to date. The system is built to avoid common web based security threats (database injection, cross site scripting, and cookie hijacking to name a few).

The system is a Multi-tenant, Single Database per Tenant Architecture.

Diagram and Data Flow



Data Flow:

- Public Internet users access OpenWater via a Cloudflare Firewall (Tls 1.2 Encryption)
- Cloudflare routes to Azure Load Balancer (Tls 1.2 Encryption)
- Access Granted to Web Facing Servers inside Azure Private Network (Tls 1.2 Encryption)
- Web Servers and Report Servers interface with 1 DB per Tenant (Tls 1.2 Encryption)
- Database stores form field information (Encrypted at Rest)
- All media files (videos and picture uploads) are stored in Amazon S3 (Encrypted at Rest)

Storage Locations

Data is stored in Microsoft Azure Regions depending on customer origin (your organization's location). Data includes all user information including name, email, and collected forms information.

United States	US East 2
Canada	Canada East
Europe	Ireland
Australia	Australia West
All Other Countries	US East 2

All uploaded files (videos / pictures) are stored on Amazon S3 East 1 Region and are served via a point of presence as close to the end user as possible.

Who Has Access to Your Data

OpenWater processes your data. This data is only used for purposes of providing customer service and support. OpenWater will **never** sell this data to third parties, nor provide it to third parties for any reason other than law enforcement.

OpenWater staff that are not affiliated with providing service and support will **never** have access to your private data.

The following stakeholders have access to OpenWater data:

Stakeholder	**Access**
OpenWater General Staff	OpenWater General Staff including Sales, Marketing and internal operations have access to the public website of your organization. General staff are no different than the general public and can only see and view information that has been made publicly available by your organization.
OpenWater Implementation and Support Staff	The OpenWater implementation and support staff is separated into small teams of 3 to 5 individuals who work on batches of customers. You will be designated a primary support representative who is managed by a support team lead. In addition to these two individuals OpenWater may assign 1 to 2 additional members to service this team. All of these support members will be able to access your information. All staff members on these teams are from the United States or Canada and undergo background checks prior to being given access. All of their access is logged and monitored. If you opt out of customer service, no implementation or support staff member will have access to your information.
OpenWater Senior Technical Staff	OpenWater Senior Technical Staff has access to backups of your data. These backups are used to reproduce issues for remediation or to recover from a data loss event (human error or system error). All access to backup data is logged and monitored.
Your Organization Staff	Administrators designated by your organization will have the ability to access information hosted by OpenWater on behalf of your organization. The platform supports two levels of access control: **All Access** or **Designated Access** per program hosted by OpenWater.

Service Level Agreement and Monitoring

OpenWater is committed to a 99.9% Uptime Service Level Agreement per month.

The platform uptime is monitored by Pingdom and a historical record can be viewed at https://openwater.statuspage.io/

The system is monitored 24 / 7 / 365 days per year. System outages and partial outages are reported on the status page and customers can subscribe to updates.

System outages typically occur on days when many other systems across the Internet are facing issues. Notably, Amazon S3 and Microsoft Azure based solutions, which are relied on by millions of organizations, including OpenWater, will fail to operate during an outage.

The OpenWater Status Page is resilient to an outage by a single cloud provider and is the best source of up-to-the-minute information.

The historical record shows OpenWater exceeds the 99.9% uptime mark. Since tracking began in 2013, we have noticed there are typically one to two events per year that last longer than one hour, and no events that have lasted longer than 4 hours.

While we cannot control short term changes in the cloud, we are committed to providing a service level of 99.9% and have structured our system in a way that would allow us to move to another provider should our current vendor face prolonged outages or issues.

Our traffic doubles each year, and we currently service over one million users per month. Response time has remained consistent at sub-1 second per page load.

In the event of a service disruption, our priority is to first restore normal services. Credits for service are not provided, however, should OpenWater fail to meet the 99.9% service level agreement, the customer will have the right to terminate the agreement early and receive a refund for the prorated, paid portion of the license fees.

GDPR and Privacy Shield Compliance
All OpenWater customers that have end-users in the European Union must comply with General Data Protection Regulation and Privacy Shield.

OpenWater is a data processor per GDPR. Organizations that license OpenWater are data controllers. This document describes OpenWater's compliance measures as a processor.

1. Only process personal data on instructions from the controller, and inform the controller if it believes said instruction infringes on the GDPR (28.3). In other words, a data processor may not opportunistically use or mine personal data it is entrusted with for purposes not outlined by the data controller.
    a. OpenWater staff will only process data for the purpose of providing customer service or support to the organization. Data will never be transferred or mined to a third party.

2. Obtain written permission from the controller before engaging a subcontractor (28.2), and assume full liability for failures of subcontractors to meet the GDPR (28.4)
    a. Subcontractors and additional services used by OpenWater are documented by policies in our Master Services Agreement. Relevant to GDPR is OpenWater's use of Google Analytics. OpenWater uses Google Analytics strictly to observe usage of its platform. No personal demographic data is transferred to Google Analytics. Beginning May 25, 2018, customers may disable Google Analytics tracking by OpenWater. Disabling Google Analytics will reduce OpenWater's ability to diagnose issues based on server load to your website.

3. Upon request, delete or return all personal data to the controller at the end of service contract (28.3.g)
    a. OpenWater has a defined procedure for requesting data destruction and data export. The summary of this procedure is as follows: The organization may request a copy of their data within 30 days after the end of service period for no additional charge. Data will be destroyed 365 days after the end of service period, however a prompt destruction may be requested as well for no additional charge.

4. Honor End-Users "Right to be Forgotten"
    a. Your organization has full control of its end-user data and can delete personal information stored regarding your end users at any time with no limitations.

5. Enable and contribute to compliance audits conducted by the controller or a representative of the controller (28.3.h)

a. OpenWater will participate in compliance audits by the controller or representative of the controller. Burdensome compliance measures may result in additional fees which will be incurred only after approval from the customer.

6. Take reasonable steps to secure data, such as encryption and pseudonymization, stability and uptime, backup and disaster recovery, and regular security testing (32.1)
    a. Data is transmitted using TLS 1.2 encryption. Data is encrypted at rest. Microsoft Azure Key Management is used to ensure security of encryption keys.

    b. Uptime, Backup and Disaster recovery procedures are listed in the following sections of this document:
        i. **Service Level Agreement and Monitoring**
        ii. **Backup Procedures and Continuity Plan**

7. Notify data controllers without undue delay upon learning of data breaches (33.2)
    a. OpenWater will notify impacted customers within 24 hours of learning about a data breach.

8. Restrict personal data transfer to a third country only if legal safeguards are obtained (46)
    a. OpenWater is Compliant with Privacy Shield. Status and recourse mechanisms are listed on OpenWater's registration page at PrivacyShield.gov: https://www.privacyshield.gov/participant?id=a2zt0000000TRMiAAO&status=Active

<u>Additional Responsibilities for the Data Controller</u>
Your Organization should include a privacy policy that adheres to the GDPR. The following elements should be included.

1. Identify OpenWater is the Data Processor and reference our Privacy Policy: https://www.getopenwater.com/privacy-policy/
    a. Summary: Data will only be used by OpenWater to provide services to your organization. OpenWater agrees to never re-sell your data or transfer it to a third party.

2. Identify the personal data collected and stored:
    a. By default OpenWater collects the following information: First Name, Last Name, Email Address of all end-users.

    b. All other personal information you plan to collect, including but not limited to gender, race, political views, and sexual orientation must be identified and protected.

3. Ensure personal data is collected fairly and with consent.

a. Beginning May 25, 2018, OpenWater will allow you to define a Consent Message that appears when a user first accesses the OpenWater platform. If you enable this feature, all users must agree to your consent message before accessing the platform. If you choose to not use this feature, you must include a checkbox during account creation in OpenWater that requests consent to data collection. This checkbox may not default to opt-in.
b. Beginning May 25, 2018, OpenWater will allow you to list a consent message on all outgoing emails from the OpenWater platform. This message will appear in the footer of emails and include a link to allow the user to deny future contact from the OpenWater platform. OpenWater recommends use of this feature to allow for rapid consent management by the end-users.

PCI Compliance, Scanning and other Compliance (SAS-70, SOC-2)

OpenWater undergoes PCI Compliance which covers components related to its payment gateway handling. By use of the Microsoft Azure Platform, OpenWater is able to inherit security controls for many other popular audits.

Document	**How to Access**
PCI Compliance SAQ-D, AOC version 3.2	Request via your OpenWater Support Representative
PCI Compliance Daily Scan Results (Scans Provided Daily by TrustGuard)	Request via your OpenWater Support Representative
ISO 9001, ISO 20000-1:2011, ISO 22301, ISO 27001, ISO 27017, ISO 27018 FEDRAMP HIPAA SAS-70 SOC 1, SOC 2, SOC 3	Request via Microsoft Service Trust Center

Backup Procedures and Continuity Plan

OpenWater maintains backups to recover from data loss caused by human error or system error in the following manner:

Backup Type	Purpose	Retention	Time to Restore	Cost
Secondary Database Copy on an alternate Azure Region	Fail-Over in the event of prolonged outage > 8 hours	N/A	15 Minutes to Enact Failover	N/A
Nightly Backup of Database	Recovery from Human Error	365 Days	1-2 Business Days	$250 for urgent restore due to human error No charge for standard restore or if data loss occurred due to system error
Point and Time Restore of Database	Recovery from Human Error or System Issue with 1 minute granularity on data	7 Days	1 - 2 Business Days	N/A (No rush service available)
2nd Nightly Backup of Database on Alternate Data Center	Recovery from Catastrophe / Loss of Data Center	365 Days	N/A	N/A

Continuity Plan

OpenWater is designated a High Priority, but not Mission Critical System. Our continuity of operations plans fails over to a secondary environment after an 8 hour period. In the event of an outage, the end users of the platform should be asked to return after the outage to complete their applications or enter their review scores. OpenWater suggests organizations include a policy that states a deadline may be extended in the event of a prolonged system outage.

OpenWater has a strong historical record with an uptime exceeding 99.9%, with no prolonged outages, however organizations that rely on 100% uptime should request a dedicated continuity plan.

In the event of an outage, the plan is as follows:

1. An outage is detected within two minutes by Pingdom and text messages are sent to operations staff.

2. An outage exceeding four minutes will trigger self-healing operations
    a. Each server node will begin a reset until all server nodes are restarted

3. An outage exceeding five minutes will result in an alert to our Status Page

4. A prolonged outage greater than 5 minutes will include one update to our status page each hour until the problem is resolved and normal operations are resumed.

5. If no resolution has been found within 4 hours, preparation to swap to the failover environment will begin.

    a. If a resolution has been found, then the senior member of the ops team will decide to wait for resolution or to swap to the failover environment

    b. If no resolution has been found within 8 hours of the initial outage, a failover swap will occur

    c. The operations plan is to rely on the primary environment, time of outage (e.g. weekend or weekday, summer slow season vs busy fall / winter) may shift the final decision to swap to failover sooner than 8 hours or longer than 8 hours

6. In the event of a total data center loss, OpenWater will be able to restore customer databases that are up to 24 hours stale to a new data center on any popular cloud provider (Amazon Web Services, Azure, Google Cloud Platform). In the event of such a catastrophe, OpenWater will communicate publicly with all customers the prioritization plan.
    a. Customers that have been active within the last 24 hours will take priority, Up to 24 hours of data may be lost, and Up to 5 days may be required until full restoration of Operations.

Data Destruction Policy

By default OpenWater retains all backups for a period of 365 days for all customers including those that are no longer using the service.

As a customer of OpenWater you may download your data at any time to common formats including CSV, XLS and JSON. All attached media can be downloaded using our Bulk Downloader or via DropBox.

If you are no longer a customer, you may request a copy of your data within 30 days at no additional charge.

If you are no longer a customer and wish to have OpenWater destroy your data, please send a certified letter signed by an Officer or appropriate authorized representative of your organization to:

OpenWater Software Inc
Data Security Department
4401 Fairfax Drive Suite 200
Arlington, VA 22204

In this letter include a secret phrase.

OpenWater will verify your request by

1. Sending an email to the work email address of this user
2. Follow up Phone Call on a Recorded Line
3. Confirmation of Secret Phrase
4. Confirmation of additional data (e.g. method and date of payment to OpenWater)

Upon verification, OpenWater will send a confirmation email to two additional staff at your organization.

Assuming there are no concerns, OpenWater will purge all data, including backups for your organization and provide a certificate of destruction.

Data Breach

There are no known data breaches on the OpenWater Platform. In the event of a data breach OpenWater will take the following actions.

1. Request immediate assistance from the Microsoft Azure Computer Emergency Response Team

2. Notify the Appropriate Authorities

3. File a claim with Insurance, OpenWater carries $1,000,000.00 worth of cyber data breach insurance.

4. Within 72 hours, Notify the impacted customers (24 hours for those customers based within the European Union)

5. Provide an update once every 24 hours to the impacted customers until the full impact is known and a resolution is in place