ObservePoint

OBSERVEPOINT SECURITY

ObservePoint Security Overview

What does ObservePoint do?

ObservePoint provides its customers with a license to use its hosted enterprise-class data governance platform.

ObservePoint users go to our website to log in to our platform to conduct audits of their digital marketing tags across all of their own publicly facing webpages and apps for accuracy. These audits help customers validate data collection from analytics, advertising, tag management systems and other data collectors. Our platform can also be used to run simulations to interact with focused, high-value publicly facing web content on a customer's webpage or app to simulate a human user. Simulations can confirm site functionality and detect tagging errors. In addition, ObservePoint can also run scans to help ensure privacy compliance by validating that cookie banners are in place and functioning as expected and that third parties are not collecting data they shouldn't. ObservePoint's platform is designed and continually upgraded and maintained to help our customers confirm data quality and identify gaps or weaknesses in implementation of their tags on their websites and apps.

What data does ObservePoint collect?

Our customers designate which of the webpages and apps they would like to scan with the ObservePoint platform when they log into our website and start using the product. ObservePoint does not collect any personally identifiable information and does not access any systems or data that is not explicitly defined by the customer. This is usually websites and apps that are available to the general public. That means that we do not collect or have access to any user or customer's data, credit card information, personally identifiable information, or connect to any of your internal systems. If the average person browsing the internet cannot get to the page without logging in or creating an account, our product cannot scan that information. Our customer service team will work with your security team to have you create an administrative dummy account (that cannot access customer information) for the purposes of testing your tags. The data accessed and collected here is still not personally identifiable in any way.

What if my company is about to launch a new website and I want to scan non-public web pages in my development environment?

Our product does have the ability to scan your website code in a preproduction environment through the creation of a virtual private network (VPN) tunnel, or via network access list allowing ObservePoint's servers to browse the preproduction sites. We recommend NEVER using real accounts for testing. Our customer service team will work with your security team to have you create an administrative dummy account that cannot access customer information for the purposes of testing your tags and pages in preproduction environments. As with production systems, ObservePoint will only have access to any data associated with the active browser session, and if applicable, the test account which is being used for login. The data accessed and collected here is still not personally identifiable in any way.

Even though we're not accessing your company's private information or any of your customer data, we safeguard our customers by following industry best practices:

- Shield principles and supplemental principles located at **https://www.privacyshield.gov/EU-US-Framework**;
- ObservePoint has appointed a single individual, our Operations Manager, to establish, direct, monitor and communicate information security requirements and controls;
- We carry out appropriate pre-employment checks on all personnel to ensure the security and confidentiality of customer data being accessed by our personnel;
- ObservePoint conducts on-going security training and awareness activities to our staff to ensure that they are familiar with the company's information security policies and best practices to protect our own and our customers' information;
- We take special pains to configure all systems and devices that store, process or transmit data in line with good industry practice to reduce the level of inherent vulnerabilities, including keeping such systems updated and installing the latest security patches;
- ObservePoint protects all systems that are accessible via the internet against malware infections through the use of appropriate malware protection solutions;

- We protect information, applications and systems within our own internal net works against unauthorised access and disclosure by using appropriate measures including, but not limited to: firewalls, internet gateways, or equivalent network devices;

- On our systems that store, process, or transmit data, we assign user accounts—particularly those with special access privileges (e.g. administrative accounts)—only to authorised individuals, and provide only the minimum level of access to applications systems and networks necessary for each employee to perform his or her role;

- We secure information in transit (including back-ups) using industry good practices including, but not limited to: encryption, tokenisation, and hashing to preserve the confidentiality of the data;

- We DO NOT utilize removable media and any other portable storage devices to store information, with all laptops and mobile devices using full disk encryption;

- ObservePoint maintains appropriate system, security, and audit logs that identify user and administrative activities and review for anomalies on a regular basis;

- We have established appropriate monitoring measures to identify and detect anomalies and potential breaches in a timely manner;

- We segregate the systems and processes used for test and development activities from production systems and ensure a change control process is implemented for the promotion of code to the production environment;

- We ensure customer production data is not used for testing unless prior written approval is obtained from that customer;

- In order to ensure ongoing stability and security, we conduct quarterly vulnerability assessments. If the results of these quarterly vulnerability assessments present any critical or high risk vulnerabilities, we remedy all critical and high issues; and

- We take every precaution to make sure our customers' data is protected against loss, destruction and damage, and against unauthorised or accidental access, processing, erasure, transfer, use, modification, disclosure or other misuse. We also ensure that only authorised personnel have access to customer data. Your data is backed up every 6 hours to our private cloud, currently provided by AWS.