oxylabs®

Oxylabs KYC Policy

Building trust in web intelligence by protecting consumers, businesses, and the internet from malicious actors.

Executive Summary

Oxylabs upholds strict Know-Your-Customer (KYC) standards throughout every part of our business, from initial service provision to continued risk assessment and monitoring. Each customer that attempts to gain access to our solutions or infrastructure is subject to one of or all of our verification processes.

Our goal, however, is not to prevent customers from accessing web intelligence solutions. Strictness of our KYC is dependent on numerous factors such as use cases, business legitimacy, cooperation with our specialists, etc. Well-meaning, globally recognized, or cooperative customers may be fast tracked throughout the process.

Oxylabs KYC is separated into several parts with varying degrees of severity. Each process has unique characteristics in addition to general questionnaires. Our Risk Assessment team will also employ technological solutions and independent third party sources to verify any statements made. Finally, in some cases ID verification or a compliance call with both parties may be required.

These strict compliance standards exist as our primary way to safeguard customers, consumers, and the internet from malicious use of our solutions while shining a light on how far the web intelligence industry has progressed since its inception. Oxylabs prides itself on being the most innovative and ethical provider in the industry, bringing web intelligence acquisition the legitimacy the industry deserves.

> Ethics, compliance, and security have helped create the Oxylabs we have today. Transparency is the way forward for the web intelligence community, so we decided to outline exact practices we employ to protect the integrity and interests of stakeholders. Our hope is that many others will follow, creating industry-level best practices for KYC verification, ultimately benefiting everyone and bringing web intelligence to limelight and shedding off the negative perception it once held.

Julius Černiauskas
Chief Executive Officer at Oxylabs

Table of Contents

Principles of Know-Your-Customer Practices

Oxylabs uses a multi-layered KYC approach that separates each customer into several distinct stages, depending on automated and manual initial assessment. There are slight differences for individuals and businesses, however, the end goal is the same – to create accountability and identify the person(s) intending to purchase our services.

Our risk questionnaire always includes contact information and details, business use case and industry, a short description of the business model, and company-related information, if purchased on behalf of an organization. All provided information is kept strictly confidential, according to our Privacy Policy.

All provided details are verified through independent sources such as business registers. Additional information may be requested if an insufficient amount of data was provided for verification. A live call or ID verification may be required for further assessment.

Additionally, our third party risk assessment tools and financial services providers evaluate customer registrations automatically and independently. Oxylabs Risk Management tech stack helps us reduce incidents of fraud and abuse and, as such, any information provided by these solutions is foundational to the final evaluation of our customers.

Failure to comply with our KYC requirements will result in a rejection of services. Identification and assignment of accountability are the primary goal of our practices, therefore, any action that may obstruct or hide the identity of the purchaser will also result in rejection.

KYC Requirements

All interested parties will be required to submit personal details that help with identification. Personal details are mandatory for our risk assessment to remove the possibility of our services being purchased under fake identities. All of the provided details are kept confidential and verified through independent sources.

Companies will also be required to submit business registration information in addition to personal data from the responsible person. Details are verified based on all established compliance procedures.

Naturally, cooperative companies, large enterprises, easily verifiable brands, and low-risk businesses go through a streamlined onboarding process. After KYC verification, our teams will engage with the company to fast forward them through the setup process, enabling them to get started with Oxylabs solutions faster.

Post-onboarding

Our Risk Management team will conduct post-onboarding processes, ranging from continued communication to ongoing due diligence. While we do not collect any operational data about our customer activities, we commit to ensuring that our solutions are being used as described.

As such, our Risk Management team will perform assessments to verify whether the use case provided and agreed upon matches the one being used in practice. If suspicions arise, our team may contact the individual or company responsible for the use, requesting an explanation.

Forbidden and Inherently Risky Use Cases

Oxylabs forbids the usage of our infrastructure or solutions for illegal and unethical use cases. These include, but are not limited to:

- Credential stuffing.
- Website traffic boosting.
- Mass email sending or spamming.
- Anything related to fraudulent or criminal activities.

Many use cases, however, are dependent upon intent, company profile, and expected result. These use cases are forbidden by default with exceptions provided only to specific industries and intents:

- **Financial use cases.** Access may be provided only to financial institutions, government entities, or cybersecurity companies with a clear, well-defined, and non-malicious goal.
- **Government websites.** Access provided only in cases such as investigative journalism or academic research with assurances and agreements provided to Oxylabs.
- **Gaming and entertainment.** Access provided only if a legitimate, non-malicious use case is provided.
- **Advertisements.** Access granted to companies and other entities that provide extensive documentation for a legitimate use case and have a strong business profile.
- **Ticket websites.** Access granted only if no items are being purchased and cybersecurity measures of websites not circumvented.

Additionally, many use cases are inherently risky as they may involve accidental or intentional procurement of personal data. Such uses may only be allowed if and only if no personal data is accessed and only publicly available information is viewed.

Any inherently risky use case will require a higher degree of verification to ensure that no abusive use of our infrastructure or solutions is performed, therefore, our Risk Management Team may request additional information as a safety precaution.

Finally, in our assessments, the company industry may be evaluated as well. Cybersecurity companies, for example, are considered to be low risk as their values and goals align with Oxylabs' stated purpose and mission. Similarly, government entities, non-profit organizations, and academic institutions may be allowed a wider array of use cases than most for-profit companies.

As such, all risk assessments are performed through a two-axis matrix that evaluates both the particular use case (e.g., accessing government websites) and the organization (e.g., an academic institution). Both aspects factor into the final decisions made by the Oxylabs Risk Management team.

Rejection of Services

Failure to comply with KYC assessment requirements will automatically result in a rejection to provide services. Oxylabs, however, reserves the right to terminate existing contracts if certain conditions apply.

Any deception on behalf of the customer's use case, identity, or any other important assessment factor may result in termination of the contract even if an initial testing phase was provided. Additionally, if the use case is intended to change, the customer should inform Oxylabs about the changes ahead of time in order to provide us time to conduct a risk assessment.

Additionally, a customer may be informed about improper use of our infrastructure if Oxylabs deems that such usage is harmful to us or any other third parties. Such actions will result in Oxylabs providing recommendations for operational changes, whenever possible. Malicious non-compliance with these recommendations, however, may result in contract termination.

Finally, Oxylabs takes any misuse of our infrastructure extremely seriously and will investigate any report about such activities. Customers, consumers, and any other parties may send in an anonymous report to our Risk Management Team to our dedicated compliance email address.

Key Takeaways

Oxylabs is committed to safeguarding the internet, consumers, and customers from abusive usage of our services. Each customer will have to go through a KYC process that may include several layers of verification.

Our process is segmented into different categories, depending on pre-assessment risk. Some requirements for each segment are identical while others may be unique to the company in question. The initial goal of the basic KYC questionnaire is to discover and verify the identity of the individual or company to ensure that proper accountability can be established.

Regardless of the results gleaned from the KYC questionnaire, some use cases are outright forbidden and are not subject to assessment or negotiations. Most, however, are evaluated on a two-axis basis wherein our Risk Management Team will assess whether the use case has any legitimate merit and whether the company intending to do so would be both within rights and reasonably able to uphold the legal and ethical requirements of such usage.

In cases where Oxylabs is contacted by legal authorities in regards to an ongoing or intended investigation, our company offers full compliance and cooperation. Third parties may also contact us with any suspicions about improper usage, which will be considered a cause for Oxylabs to conduct an independent investigation. In cases where no improper usage is detected, our company will provide a written confirmation to the third party that the reported use is legitimate.

Finally, Oxylabs always reserves the right to both refuse and terminate the provision of services. These may arise in cases when a customer does not pass KYC verification or attempts to obstruct discovery or deceive the company in regards to intended or practical usage of our services. Additionally, if some specific actions by a customer may or do harm our infrastructure or third parties, recommendations will be provided for changes that have to be implemented for continued provision of services.