Introduction

At Youverify Inc. ("Youverify" or "We"), we're all about empowering people with their identity by enabling identity attestation, risk assessment, and identity risk scoring in a secured manner. The data we collect, and use helps us with that objective and nothing more. No surprises.

At Youverify, when we verify an identity or carry out a verification related to an identity (our "**Verification services**", we respect your privacy and are committed to protecting it through our compliance with this policy. This Privacy Policy is designed to help you understand how we use the information we collect to deliver our verification services and build trust in our system.

This policy applies to information we collect:

- On the Website, which is any web page or webservice located under the domain or subdomain of "Youverify.co" .
- In email, text, web service and other electronic messages between you and the Website.

It does not apply to information collected by:

- Us offline or through any other means, including on any other website operated by any third party (including our affiliates); or
- Any third party (including our affiliates and subsidiaries), including through any application or content (including advertising) that may link to or be accessible from or on the Website.

Please read this policy carefully to understand our policies and practices regarding your information and how we will treat it. If you do not agree with our policies and practices, your choice is not to use our Website. By accessing or using this Website, you agree to this privacy policy. This policy may change from time to time (see **Changes to Our Privacy Policy**). Your continued use of this Website after we make changes is deemed to be acceptance of those changes, so please check the policy periodically for updates.

Children Under the Age of 18

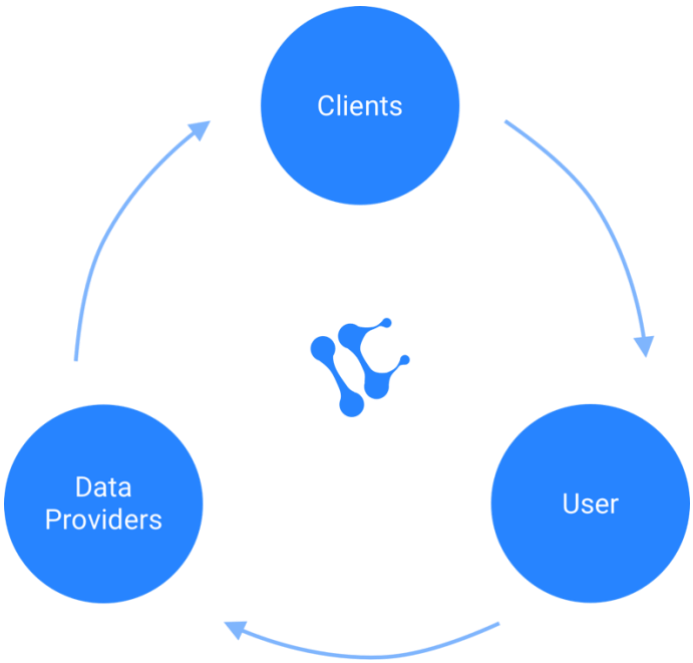
Our Website is not intended for children under 18 years of age. No one under age 18 may provide any information to or on the Website. We do not knowingly collect personal information from children under 18. If you are under 18, do not use or provide any information on this Website or through any of its features, use any of the interactive features of this Website, or provide any information about yourself to us, including your name, address, telephone number, or email address. If we learn we have collected or received personal information from a child under 18 without verification of parental consent, we will delete that information. If you believe we might have any information from or about a child under 18, please contact us at privacy@youverify.co.

Information We Collect About You and How We Collect It

To deliver our Verification Services, we need to collect some specific information about users. The particular information needed is dependent on the type of verification that's being carried out. For example, when verifying the identity of a user through Identity Document verification, we'll ask for the unique identification number of the user ("**subject**") ID, the user's date of birth, the user's first name and last name. We will then verify whether the identity document provided is authentic by matching it against existing data with our data providers. We can also ask you to provide a picture or video of your face, where we'll then verify whether the person in the photo or video is likely the same person pictured in the identity document. If yes to either of the identity document and facial verification, Youverify's client will likely consider the user to have proven their identity. Another example, when we are verifying an address through our address verification, we'll ask for the user's first name, user's last name and the user's physical address. In some scenarios, the user's physical address can be that of the user's guarantor or business premise. We will then verify whether the user's physical address exist at the location and if the user is available at the address by matching the information against existing data with our data providers and when this is not possible, we dispatch a field agent to locate, validate the address and the availability of the user at the address. If we are able to validate the information provided by the user, Youverify's client will likely consider the user to have provided a verified address.

To enable us to provide the Verification Service, the user must provide consent to our client which is enforced through our contract with the client and in scenarios where the user is engaging Youverify directly, consent are secured through the use through checkboxes and clearly labelled buttons with descriptive preceding text for which the consent covers.

The Youverify Data Lifecycle below shows you how we collect that information



1. The Client

Clients ("**business customers**") are organisations that have contracted and asked Youverify to verify an identity or verify an address or carry out verifications related to that identity. Once we have verified an identity or completed the requested verification or check, we share the results

("**report**") with the client in a Youverify Report, as described further below. The client then decides how they want to proceed with the user based on the results. In some cases, the client might ask for additional information before making a decision. Also, some clients only ask us to carry out a check if a previous check was marked as verified or not verified. This ensures we only do the minimum number of verifications needed.

2. The User

Users are individuals whose identities or personal information we verify or otherwise validate on behalf of our clients. We collect users' information from our clients or directly from the users themselves. This information might include the name of the user, the unique identification number and image of the user's identity document (e.g. passport, driver's license, biometric verification number, permanent voter's card, national ID), photos (at times, taken in quick succession for anti-fraud purposes) or a video of the user, the biometric facial identifiers in those images, and the user's date of birth (this is collected to ensure that the client or the user have enough information about the subject before requesting Youverify to verify an identity). This enables us to help the client verify that the user is the true owner of the identity document and has not shown signs of identity fraud. In some cases, the information requested might include the user's physical address, the user's guarantors' identity information, the user's employment information, and the user's education record. This enables us to help the client verify that the user information as part of our client compliance due diligence and confirm that the information is true. In some circumstances, we may also collect device identifiers and IP addresses to help us understand whether a device has previously been used in relation to suspected fraudulent activity and whether Youverify is permitted to provide Verification Services in the country in which the user is located. To further combat fraud, we also collect identity information that has been leaked or otherwise made available on the internet.

3. The Data providers

Data providers are used to provide additional information to carry out specific checks. For example, if we need to verify a national identification number ("**NIN**"), we'll match the information provided by the user with the National Identity Management Commission ("NIMC"). Another example, if we need to verify the user's right to drive, we might ask the appropriate government driving body to verify that user's information. When our client asks us to verify an address, we ask our field agents to verify the information, in this case they are our data provider for the verification request.

We also keep logs of how our clients, users, and data providers interact with our Verification Services. This might include timestamps and location information of when the information was submitted to Youverify, and information about the device used to submit that information. Sometimes, we receive information we don't need to provide our Verification Services. For example, instead of a picture of a person, a user might upload a completely unrelated image. When this happens, we seek to delete this data.

We use information to deliver and maintain our Verification Services on behalf of clients on the basis that the user has **consented** to the processing or otherwise requested Verification Services, the client has a legitimate or lawful reason for requesting Verification Services, or the processing is necessary to carry out a task in the public interest or for reasons of substantial public interest.

We also use information to further develop our Verification Services on the basis that the processing is necessary in the legitimate interest of the client or Youverify, the processing is necessary to carry out a task in the public interest or for reasons of substantial public interest, the processing is necessary for scientific research purposes, or the user has provided their consent.

Youverify Reports and Verification Classification

When we verify an identity or carry out a verification on behalf of a client, we provide a Youverify Report to that client. This Youverify Report details our recommendation and the reasoning behind it. The reasons are generated from the different machine learning models, human powered processes and the data from our data providers, that are used to verify an identity or perform a verification. As these machine learning models, human powered and data driven processes are under constant development, it is difficult to maintain a list of them in this Privacy Policy. But you can find an accurate and up to date list in our Technical Documentation, usually used by clients that have integrated or will be integrating with us. By providing our clients with these detailed Youverify Reports, our aim is to empower our clients to make informed decisions about users and to provide specific help to users that are having trouble in passing a Youverify verification.

Sharing Information Outside Youverify

As well as sharing information with clients, users, and data providers (as described above), Youverify also shares information with external parties that are performing tasks on our behalf (including our affiliates) and with other companies, organizations, government bodies, and individuals outside Youverify where we have a legitimate legal reason for doing so (for example, in connection with any merger or acquisition) or where we have been instructed to share the information on behalf of our clients.

For example, if a client as part of an investigation of a transaction related to the user, the client can instruct us to share the information and report regarding the user with appropriate authorities as part of the investigation for example, the police authority or a lawful investigation agency.

As part of our commitment to bringing legal identities online safely, we are partnering with universities and researchers active in the field of machine learning and artificial intelligence. Where appropriate, consented by the user and only where permitted under applicable law, we'll share user information with them for scientific research purposes.

Whenever legally possible, we seek to protect the information we share by imposing contractual privacy and security safeguards on the recipient of the information. In some cases, however, it's not possible for us to do so — for example, when we have a legal obligation to disclose information to a government authority and that government authority isn't willing to enter into such contractual safeguards.

Information Security

Youverify takes appropriate administrative, physical, technical and organizational measures designed to help protect information about users from loss, theft, misuse and unauthorized access, disclosure, alteration and destruction.

The safety and security of your information also depends on you. Where we have given you (or where you have chosen) a means to access certain parts of our Website, you are responsible for keeping this confidential. We ask you not to share your security details with anyone.

Unfortunately, the transmission of information via the internet is not completely secure. Although we do our best to protect your personal information, we cannot guarantee the security of your personal information transmitted to our Website. Any transmission of personal information is at your own risk. We are not responsible for circumvention of any privacy settings or security measures contained on the Website.

Youverify do not use cookies and we do not track our users and client web preferences (DNT) on our website, we ensure that all data collected and stored by Youverify is encrypted in transit and at rest for example; after authentication of our users and clients we generate a JSON Web Token (JWT) to authenticate our users and we use the JWT to make a subsequent request to our website.

In event of a data breach, which includes the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data, it also means that a breach is more than just about losing personal data. In each case of a data breach; we would carry out an investigation, quickly inform regulators, client and users of the breach, and be specific with respect to what data was impacted and how the issue will be addressed moving forward, within 72 hours of identifying the breach. If we fail to do that, we would share reasonable justification for the delay.

For more information about information security at Youverify, you can request for a copy of our information security policy at security@youverify.co . If you think you have identified a security vulnerability or bug in our Verification Services, please report it to the Youverify security team at security@youverify.co

Data Storage

We perform our Verification Services on behalf of our clients for a variety of different reasons. Those reasons are identified by our clients, and we rely on them to tell us when they no longer need us to store the information we've collected on their behalf. Once instructed, either through our agreement with the client or through an ad hoc request, we delete the information we have collected about users when performing the requested Verification Services.

If you, as a user, would like to make a specific request to have your information deleted, please make that request directly to the client that carried out your related check. For more information about how to do this, please see below under "Your Rights".

To deliver our verification services as a data processor (when we are acting on behalf of our client) and as a data controller (when we engage users directly on behalf of our client), we store and process data in a secure and encrypted manner at data centres located in countries with strict data privacy laws similar to the National Information Technology Development Agency ("**NITDA**")'s Nigeria Data Protection Regulation ("**NDPR**") of 2019. Presently, we use data centres in European Union ("**EU**") where data privacy is governed by the General Data Protection Regulation ("**GDPR**"), visit https://gdpr.eu/faq/ for more information on the EU regulation. In scenarios where we have to process

and store highly sensitive government data, we only store the data on premises of the government agency or an approved local data centre.

Where we have a legitimate legal reason, we may also store information for longer than described above – for example, where we are under a binding legal order not to destroy information.

Your Rights

You have the right to withdraw your consent to the processing of your Personal Data at any time, without affecting the lawfulness of processing based on consent before its withdrawal.
If you would like to access a copy of your information, have your information deleted, or otherwise exercise control over how your information is used, please contact Youverify at privacy@youverify.co , or the postal address below. Please be aware, some requests may require us to notify the relevant client (as described above in the Youverify Data Lifecycle) so the client may fulfil the request instead (and not Youverify). This is necessary where Youverify is acting on the client's behalf.

Other Applicable Laws

Youverify is headquartered in the Nigeria and our website is primarily directed to visitors who are located in Nigeria. Our use of personal information is subject to applicable Nigeria privacy laws.

We comply with the NDPR as set forth by the NITDA regarding the collection, use, and retention of personal information of Nigerians and natural persons residing in Nigeria.

In compliance with the NDPR, we commit to resolve complaints about your privacy and our collection or use of your personal information within 10 working days. Nigerian citizens with inquiries or complaints regarding our Privacy policy should first contact us at: privacy@youverify.co.

Changes to Our Privacy Policy

It is our policy to post any changes we make to our privacy policy on this page. If we make material changes to how we treat our users' personal information, we will notify you through a notice on the website home page and we will share the policy with all our client through email. The date the privacy policy was last revised is identified at the top of the page. You are responsible for ensuring we have an up-to-date active and deliverable email address for you, and for periodically visiting our Website and this privacy policy to check for any changes.

Contact Youverify

If you would like more information about how Youverify collects and uses information, or if you would like to contact the Youverify data protection officer, please contact Youverify at privacy@youverify.co or at:

Attention: Privacy Office
Youverify Inc.
13b, Bishop Street
Ilupeju, Lagos
Nigeria

If you would like to raise a concern with our Privacy Supervisory Authority, you can contact NITDA https://nitda.gov.ng/nit/contact-us/