



West Park Towers | 6th Floor | Mpesi Lane | Westlands | C: +254 712 517 910 | W: www.senti.com

SENTI DATA PRIVACY POLICY AND PROCEDURES





West Park Towers | 6th Floor | Mpesi Lane | Westlands | C: +254 712 517 910 | W: www.senti.com

COPYRIGHT INFORMATION

COPYRIGHT 2022

ALL RIGHTS RESERVED. THIS MATERIAL IS CONFIDENTIAL TO SENTI LIMITED HEREINAFTER REFERRED TO AS SENTI AND IS INTENDED TO SERVE AS A REFERENCE FOR SENTI. NO PART OF THIS MATERIAL SHOULD BE REPRODUCED / PUBLISHED IN ANY FORM BY ANY MEANS, ELECTRONIC OR PHYSICAL INCLUDING PHOTOCOPY OR ANY INFORMATION STORAGE OR RETRIEVAL SYSTEM NOR SHOULD THE MATERIAL BE DISCLOSED TO THIRD PARTIES WITHOUT THE WRITTEN AUTHORIZATION OF SENTI.

ALL TRADEMARKS ARE OWNED BY THEIR RESPECTIVE OWNERS.





Effective Date: 1st August 2023.

The website (<https://senti.co.ke/>) is operated and provided by Senti Capital Limited ("SENTI", "we", "us", "our") having its registered office at West Park Towers, 6th Floor, Mpesi Lane, Nairobi Kenya. If You reside in a country where we provide our services to You and are a user of our website ("our site"), we are a data controller for the purpose of Data Protection Legislation (as defined below).

In this Privacy Policy, references to "You" and "Your" are references to a user of our website.

1. Introduction

We are committed to protecting and respecting Your privacy and handling Your information in an open and transparent manner.

This policy ("**Privacy Policy**") explains what information we collect from You, or You provide to us, what we will use it for and with whom we share that information. The Privacy Policy also sets out Your rights and who You can contact for more information. Please read the following carefully to understand our practices regarding Your personal data and how we will treat it.

In this Privacy Policy the term "Data Protection Legislation" means the Kenya Data Protection Act 2019; together with all other applicable legislation relating to privacy and data protection.

2. What Information We Collect About You

We may collect, record and use information about You in physical and electronic form and will hold, use and otherwise process the data in accordance with the Data Protection Act and as set out in this Privacy Policy. We are guided by Section 25 of the Data Protection Act on Data minimisation and particularly, ensure that the Data we collect from you is necessary for the performance of our services. The personal data we collect and process includes:

- Your name;
- Your contact information such as Your email address and telephone number;
- Your demographic information such as date of birth,
- Evidence of Your identity (for example passport or national identity card information);
- Geolocation data such as your country and city of residence
- unique identifiers such as username;
- information about Your visit to our website, including the full Uniform Resource Locators (URL), clickstream to, through and from our site (including date and time), length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs) and methods used to browse away from the page.

We also collect from You information in relation to other people (e.g., details of the recipients of Your money transfers), where You provide us with such information. By providing us with such information You confirm that You have obtained any necessary permissions from such persons to the reasonable use of their information for such purposes in accordance with this notice, or are otherwise permitted to give us this information on their behalf. Please also ensure that those other people are aware of this notice and that the provisions of this notice are clearly communicated to them.

Data Protection Principles

In the processing of your personal data, we are guided by the following principles, which are set out in Section 25 of Kenya's Data Protection Act as follows;

2.1. Fairness and lawfulness

When processing personal data, the individual rights of the data subjects must be protected. Personal data must be collected and processed in a legal and fair manner.

2.2. Restriction to a specific purpose

Personal data can be processed only for the purpose that was defined before the data was collected. Subsequent changes to the purpose are only possible to a limited extent and require substantiation and consent, where necessary.

2.3. Transparency

The data subject must be informed of how his/her data is being handled. In general, personal data must be collected directly from the individual concerned. When the data is collected, the data subject must either be aware of, or informed of:

2.3.1. The identity of the Data Controller

2.3.2. The purpose of data processing

2.3.3 Third parties or categories of third parties to whom the data might be transmitted, if any

2.4. Data reduction and data economy

Before processing personal data, you must determine whether and to what extent the processing of personal data is necessary in order to achieve the purpose for which it is undertaken. Where the purpose allows and where the expense involved is in proportion with the goal being pursued, anonymized or statistical data must be used. Personal data may not be collected in advance and stored for potential future purposes unless required or permitted by national law.

2.5. Deletion

Personal data that is no longer needed after the expiration of legal or business process-related periods must be deleted. There may be an indication of interests that merit protection or the historical significance of this data in individual cases. If so, the data must remain on file until the interests that merit protection have been clarified legally, or the corporate archive has evaluated the data to determine whether it must be retained for historical purposes.

2.6. Factual accuracy; up-to-date data

Personal data on file must be correct, complete, and – if necessary – kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, supplemented or updated.

2.7. Confidentiality and data security

Personal data is subject to data secrecy. It must be treated as confidential on a personal level and secured with suitable organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification, or destruction.

3. How we Collect Information about You

- **Information You give to us when You use our services.** If You use our services You will need to provide certain information including Your name, address, as well as the name and other details of the recipients of the money transfers that you instruct us to carry out.
- **Other information You give to us.** This is information about You that You give us by filling in forms on our site (e.g.: the 'contact us' section) or by corresponding with us by phone, e-mail or otherwise. It includes, for example, information You provide when You register on the site for us to contact You, and when You report a problem with our site. The information You give us may include, among other data, Your name and email address.
- **Social Media.** Depending on Your settings or the privacy policies for social media and messaging services such as Facebook, LinkedIn and Instagram, You may give us permission to access information from those accounts or services.
- **Information we collect about You**
 - **Cookies** - like most websites, we use "cookies" to help us make our site – and the way You use it – better. Cookies mean that a website will remember You. They're small text files that sites transfer to Your computer (or phone / tablet). They improve website use and speed – for example by automatically filling Your name and address in text fields.
 - **Log Files** - In addition, with regard to each of Your visits to our site, we will automatically collect certain information (e.g.: browser type, internet service provider (ISP), referring/exit pages, operating system, date/time stamp, and/or clickstream data). We may combine this automatically-collected log information with other information we collect about You.

- **Social Media Widgets** - Our website includes Social Media Widgets or Features, such as the Facebook Like button and Twitter button which are interactive mini-programs that run on our site to provide specific services from another company (e.g.: displaying the news, opinions, music, etc). Personal information, such as Your email address, may be collected through the Widget. Cookies may also be set by the Widget to enable it to function properly. Information collected by this Widget is governed by the privacy policy of the company that created it.

4. **How we use Your Information**

We collected your personal data for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes as guided by Section 25 of the Data Protection Act.

Our primary purpose in collecting user information is to provide you with a safe, smooth, efficient and customized experience and to provide the services You have requested from us. We may also use the information that You have provided to ensure that the content on our site is presented in the most effective manner for You and Your device.

We use Your information for the following specific purposes: -

- to carry out our obligations arising from any contracts entered into between You and us or from applicable law, and to provide You with the services in accordance with our terms and conditions and with this Privacy Policy;
- to register You with a Senti account;
- to fulfill Your Transaction / (Airtime Top Up) Request;
- to send You confirmations;
- to notify You about changes to our services;
- to prevent fraud;
- to ensure that content from our site is presented in the most effective manner for You and for Your device;
- to send You marketing communications, provided that You have given us Your consent.
- to administer our site and for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes;
- as part of our efforts to keep our site and our services safe and secure;
- to measure or understand the effectiveness of advertising we serve to You and others, and to deliver relevant advertising to You;
- to make suggestions and recommendations to You and other users of our site about services that may interest You or them; and
- to display personal testimonials of satisfied customers on our website in addition to other endorsements, where You have agreed with a third-party review site that we may do so. If You wish to update or delete Your testimonial, You can contact us using this form.

We are committed to providing data subjects with genuine choices when it comes to their personal data. We will not process personal data without a lawful basis for doing so, and we will obtain explicit consent from data subjects where required. We will provide clear and concise information to data subjects about the purposes of processing their personal data, and will provide them with clear options to opt-out where applicable.

5. **Legal Grounds for Using Your Personal Information**

We process your personal data lawfully, transparently and fairly as guided by Section 25 of the Data Protection Act. The processing of your personal Data is necessary for the legitimate interests of the organization, regulatory compliance and for fulfilling the contractual obligations between you and the organization. We process your personal data:-

- to run and administer our business;
- to prevent fraud;
- to provide You with our services;
- to evaluate, develop or improve our services;
- to keep You informed about relevant products and services You are using;
- to discharge our legal obligations to store and disclose information where necessary; and/or
- to provide You with an efficient and smooth customer experience;
- necessary for the performance of our contract with You to provide You with our services;
- necessary in order to comply with a legal obligation to which we are subject; or
- permitted by You, because You have given us consent.

5 (a) **Privacy First Approach**

We are committed to implementing a privacy-first approach to all our organizational structures, systems, and applications. This means that privacy will be considered at the outset of any project or system design, and that default settings will prioritize privacy by default. We will conduct privacy impact assessments on all new projects and will review existing projects on a regular basis to ensure ongoing compliance with data protection regulations."

6. **Sharing Your Information**

The following categories of recipients may receive Your personal information and process it for the purposes outlined in this Privacy Policy. The legal basis for sharing your personal data is for our legitimate interest in carrying out our loan disbursement and debt recovery activities, compliance with regulatory bodies as well as for our contractual obligations with the third parties. This is in accordance with Section 30 of the Kenya Data Protection Act.

- We may disclose data to provide our services, to respond to legal requirements, enforce our policies, liaise with judicial or regulatory authorities where required under applicable law, and to protect our rights and property.

- The personal information You provide to us may also be shared with third party companies, agents, contractors, service providers or related companies, including without limitation:
 - with credit reference agencies to verify Your identity or recipients of the money transferred through the Service, if this is necessary to provide You with our services, respond to Your enquiries or for any other related purposes, and
 - with fraud prevention agencies who may use it to prevent fraud and money-laundering and to verify Your identity (please note that those who commit fraud will be denied from further accessing Senti services.
 - Banks, payment card processors and other service providers that process bank transfers, credit and debit card payments or otherwise provide financial infrastructure services to enable us to provide our services;
 - Our service providers, including those who provide data hosting services, fraud prevention services, technology services, and technology tools that allow us to monitor, test and improve our services, sites and Mobile Apps. Our data hosting services are facilitated by Africa Data Centre in Nairobi, Kenya.. We also ensure that the data transferred is encrypted and anonymized.
 - with regulators or public authorities in order to fulfill regulatory, legal or professional obligations.
- We may also share Your personal information with:
 - other companies we have instructed to provide services to or for us;
 - other third parties for those purposes that may be reasonably ascertained from the circumstances in which the information was submitted;
 - other business entities, should we plan to merge with, or be acquired by, or be invested in by that business entity, or if we undergo a corporate reorganization;
 - any successor in interest, in the event of a liquidation or administration of Senti Capital Limited; and
 - to any other third party, but only subject to Your prior consent.

Safeguards

When we do disclose personal information to third parties, we will ensure that appropriate safeguards are in place to protect the confidentiality and integrity of the personal data. These safeguards may include contractual provisions requiring the third party to comply with all relevant data protection regulations and to implement appropriate technical and organizational measures to protect the personal data.

7. Links to Other Sites

Our website may contain links to other sites, including via our social media buttons. While we try to link only to websites that share our high standards and respect for privacy, we are not

responsible for the content, security, or privacy practices employed by other websites and a link does not constitute an endorsement of that website.

Once You link to another website from our website You are subject to the terms and conditions of that website, including, but not limited to, its internet privacy policy and practices. Please check these policies before You submit any data to these websites.

8. **How we protect Your Information**

Senti implements an Information Security Management System to maintain the confidentiality, integrity, and availability of Senti's information resources, in keeping with industry standard and global best practices.

- 8.1. Physical locations are protected from unauthorized access, threats, and damage.
- 8.2. Data is encrypted in accordance with the data classification and handling requirements. Backup practices of critical information resources are performed, tested, and maintained.
- 8.3. Data retention, decommissioning, and disposal requirements are aligned with contractual, legal, environmental, and business requirements.
- 8.4. Endpoints are protected by security hardening, malware protection, and host-based monitoring.
- 8.5. Access is restricted by access control, user access management, privileged access (principle of least privilege), access review, multi-factor authentication, and passwords, where applicable.
- 8.6. Information resource logs are managed, and security events monitored.
- 8.7. Network access is protected through a secure network infrastructure, network access controls, and information transfer requirements.
- 8.8. Information security risks associated with third parties that access Senti information resources are identified, assessed, and managed. Contracts with third-party vendors and processors contain information security and confidentiality clauses. Information security reviews of third party vendors and processors are regularly performed.
- 8.9. Procedures are in place to recruit competent and qualified individuals as employees. A formal disciplinary process is established and implemented for non-compliance with information security policies, standards, and procedures.
- 8.10. Information resources are maintained by identifying and remediating associated vulnerabilities.
- 8.11. Formal change management requirements are followed when introducing or modifying information resources.
- 8.12. Information security incidents are managed, including detection, analysis, resolution, and lessons learned. Incident responses include preparation, identification, containment, eradication, recovery, and lessons learned.
- 8.13. Compliance requirements are established based on legislative, statutory, regulator, or contractual obligations, and are subject to independent review.

8.14. A risk assessment process and framework is established to identify and remediate information security risks.

8.15. Requirements are implemented to ensure information security controls are verified at regular intervals to assess their validity and effectiveness during adverse situations.

Information resources are managed by identification, inventorying, maintenance, and protection controls.

9. Data Breach Management

The transmission of information via the internet (including by email) is not completely secure. Although we will do our best to protect Your personal data, we cannot guarantee the security of Your data transmitted to our site; any transmission is at Your own risk. However, we have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator when we are legally required to do so under Section 43 of the Data Protection Act.

10. How Long we keep Your Information

We will only keep the information we collect about You for as long as required in line with the retention requirements set by legal, tax, AML regulations and the need to comply with our internal policies. We will retain or store personal information only for so long as is necessary to fulfill the purposes set out in this Policy and for such time as may be necessary in order to comply with any legal obligation. The details of these retention periods are available in our Data Retention Policy which you can request by contacting us via email at info@senti.co.ke/support@senti.co.ke.

We will periodically conduct audits to ensure that we only retain personal data for as long as is required and when the period lapses, the data will either be disposed of in a secure manner, anonymized or pseudonymized (so it can longer be associated with you).

You can also ask us to delete your information as set out in Your Rights (13) below for further guidance

11. Data Storage

Data that You submit via our site is stored on secure servers owned by Africa Data Centres in Nairobi, Kenya. Such transfers are made in order to operate the service, improve our site, or to assist in our security or fraud protection activities. The legal basis for sharing your personal data is for our legitimate interest in carrying out our loan disbursement and debt recovery activities, as well as for our contractual obligations with the third parties as outlined in Section 30 of the Kenya Data Protection Act.

12. Opting Out

You will be given a choice when You provide us with Your personal information to opt in or opt out of receiving marketing communications, in accordance with Part III of the Kenya Data Protection Guidelines 2021.

You have the option of "unsubscribing" from receiving direct marketing communications from us by writing to us at info@senti.co.ke/support@senti.co.ke and/or using the unsubscribe instructions in any sms/email communications sent to you.

Once we receive notification of withdrawal of consent, we will action without delay.

13. Your Rights

The Kenya Data Protection Act, under section 26 provides You with the following rights as it relates to the processing of your personal data;

- to be informed about the processing of Your personal data (i.e. to request access to or a copy of any personal data which we hold about You;
- to rectification of Your personal data, if You consider that it is inaccurate or not up-to-date; we reserve a right to verify the accuracy of the information.
- to ask us to delete Your personal data; We may not always be able to action this request for legal reasons which will be communicated to you at the time of your request
- to withdraw consent to our processing of Your personal data (to the extent such processing is based on previously obtained consent) i.e. marketing messages
- to restrict processing of Your personal data; In some instances, we may demonstrate that we have compelling legitimate grounds to process your information which will be communicated at the time of your request.
- to object to Your personal data being processed in certain circumstances. We may need to verify whether we have compelling grounds to process your information which will be communicated at the time of your request.

You can exercise any of these rights at any time by contacting us via email at support@senti.com and we will endeavor to respond within a reasonable period and in any event within one month (three months for complex or numerous requests). We reserve the right to charge a reasonable fee (reflecting the costs of providing the information) or to refuse to respond where requests are manifestly unfounded or excessive: in this case, that will be communicated to you without undue delay.

14. Changes to this Privacy Policy

Any changes we make to our Privacy Policy in the future will be posted on this page and, where appropriate, notified to You by email. Please check back frequently to see any updates or changes to our Privacy Policy.

15. Complaints Handling Procedure



West Park Towers | 6th Floor | Mpesi Lane | Westlands | C: +254 712 517 910 | W: www.senti.com

You have a right to make a complaint by any reasonable means. You can send your complaint to us on info@senti.co.ke/support@senti.co.ke. We undertake to respond within 1 business day from receipt of the complaint. Depending on the nature of the complaint, we aim to resolve the same within 5 business days for a material complaint and 1 business day for a non-material complaint.

Questions, comments, and requests regarding this Privacy Policy are welcomed and should be addressed to:

Senti Capital Ltd,
Westpark Towers,
6th Floor, Mpesi Lane,
Nairobi, Kenya
Email: info@senti.co.ke/support@senti.co.ke

You may also use these contact details if You wish to make a complaint to us relating to Your privacy.

