Power Privacy Policy

1. About this policy and your privacy.

This policy explains how we can collect, use, hold and disclose your personal information, as well as ensuring the quality, integrity and security of your personal information under applicable Privacy Laws.

Frictionless Enterprises Limited (FEL), which includes its successors-in-title, legal representatives and assigns, provider of the Power Marketplace Platform and hereinafter referred to as Power™. As the data collector, Power™ ("we" “us” “our”) recognize the importance of privacy and security and are committed to protecting and respecting your privacy and personal information.

This policy outlines how personal data we collect from you, or that you provide to us, will be handled by us.

Please read the following carefully to understand our how your personal data will be treated.

The collection and processing of your personal data is in accordance with the Data Protection Act 2019 (the “Act”), and any other laws or regulations passed pursuant to the said Act

2. Definitions

2.1 "Anonymisation" means the removal of personal identifiers from personal data so that the data subject is no longer identifiable;

2.2 “Applicable Data Protection Laws” means the DPA;

2.3 “Authorized Persons” means:

i. authorized employees; and

ii. service providers, agents, outsourcers and auditors;

who have a need to know or otherwise access Data and information to enable the Contractor to perform its obligations under this contract and who are bound in writing by confidentiality obligations sufficient to protect the Data and information in accordance with the terms and conditions of this Contract.

2.4 "consent" means any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject;

2.5 "data" means information which —

(a) is processed by means of equipment operating automatically in response to instructions given for that purpose;

(b) is recorded with intention that it should be processed by means of such equipment;

(c) is recorded as part of a relevant filing system;

2.6 "data controller" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data;

2.7 "data processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller;

2.8 "data subject" means an identified or identifiable natural person who is the subject of personal data;

2.9 “DPA” means Kenya Data Protection Act,2019 and any other laws or regulations passed pursuant to the said Act (hereinafter “DPA”);

2.10 "encryption" means the process of converting the content of any readable data using technical means into coded form;

2.11 "filing system" means any structured set of personal data which is readily accessible by reference to a data subject or according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

2.12 "identifiable natural person" means a person who can be identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or social identity;

2.13 "personal data" means any information relating to an identified or identifiable natural person;

2.14 "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

2.15 "processing" means any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means, such as

(a) collection, recording, organisation, structuring;

(b) storage, adaptation or alteration;

(c) retrieval, consultation or use;

(d) disclosure by transmission, dissemination, or otherwise making available; or

(e) alignment or combination, restriction, erasure or destruction.

2.16 "profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's race, sex, pregnancy, marital status, health status, ethnic social origin, colour, age, disability, religion, conscience, belief, culture, dress, language or birth; personal preferences, interests, behaviour, location or movements;

2.17 "pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, and such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person;

2.18 "restriction of processing" means the marking of stored personal data with the aim of limiting their processing in the future;

2.19 "sensitive personal data" means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject; and

2.20 "third Party" means natural or legal person, public authority, agency or other body, other than the data subject, data controller, data processor or persons who, under the direct authority of the data controller or data processor, are authorised to process personal data.

3. What is personal information?

3.1. When you use Power Marketplace on your mobile, we may collect your personal information to provide you with Power Marketplace services and to verify your activity for security purposes.

3.2. Power™ has a general duty of confidentiality towards you, except in the following circumstances:

- where disclosure is compelled by a relevant regulation or law;
- where disclosure is made with your express or implied consent.

3.3. Personal information includes any information about an identified individual or an individual who can be reasonably identified from that information.

3.4. The information will still be personal information whether it is true or not and regardless of whether we have kept a record of it.

Some examples of personal information may include your:

- name;
- mailing or residential address details;
- contact details such as telephone numbers, email address, social media platform user name;
- government issued identifiers such as National ID, Alien Card, Passport or KRA PIN;
- bank account and Mobile Money account details;
- credit history, credit capacity, ability to be provided with credit or credit worthiness;
- photograph, video or audio recording; and
- sensitive information such as information relating to your health, biometric data.
- your location

4. Technical and other information.

4.1. We may also collect technical information to help us detect security threats and for fraud analysis and prevention. Such technical information may include information about your device or computer such as operating system version, how your device or computer connects to our services, and your web browser settings.

4.2. This information may also be used or stored in combination with your personal information for these purposes, including to enable us to contact you if we detect a security threat.

5. Use and Disclosure.

5.1. We may use your information to comply with legislative or regulatory requirements in any jurisdiction, prevent fraud, crime or other activity that may cause harm in relation to our products or services and help us run our business.

5.2. Based on your express or implied consent we may also disclose your personal information to anyone we engage to do something on our behalf, and other organisations that assist us with our business.

5.3. As a provider of financial services, we have legal obligations to disclose some personal information to government agencies and regulators or agencies authorized by within applicable laws and regulations. e.g. Licensed Credit Bureaus

6. What kinds of personal information do we collect and hold?

6.1. The personal information that we collect about you will depend on the products or services that you apply for, or enquire about.

6.2. If you do not allow us to collect all of the personal information we reasonably request, we may not be able to deliver those products or services to you.

6.3. Throughout the life of your product or service, we may also collect and hold additional personal information about you.

6.3.1 This could include transaction information or making a record of queries or complaints you make and, if you make an insurance claim, collecting additional information to assess the claim.

6.4. Our collection of 'sensitive information', personal information under Privacy Laws, is further restricted to circumstances where we have obtained your express consent and to certain other permitted situations.

6.5. Generally, we will only collect this information if it is reasonably necessary to provide you with a specific product or service and you expressly consent to our collection.

6.6. When we collect information we will disclose the specific purpose for which we use, request and store your personal information.

This privacy policy was last updated on 8th March 2022.

6.7. We will also keep a record of that personal information and the purpose for which we collected it.

6.8. We will not use your personal information for any other purpose, other than which we disclosed to you unless you provide your express consent or unless we are permitted to do so by law.

For example, we may collect voice biometric information to verify your identity or authorise transactions.

6.9. When you use Power Marketplace on your Mobile Device, we may also collect, store and retain information from your device, including your device ID, your location information and information about apps installed on your device to verify that you are using a trusted device, your use of the Power Marketplace App including transactions, or to monitor your device for security purposes.

6.10. Location information is also used to customize the look and feel of the Power Marketplace App.

6.11. To access some services within this App, we may need to request access to certain features on your device.

6.11.1 We will always ask for your permission before we access anything stored on your device.

6.11.2 If you do not provide us permission, we may not be able to provide the service you requested.

6.11.3 We may access a range of features on your Mobile Device but we do not store or retain this information including:

- information about the device used such as device IDs; and
- IP addresses. Your IP Address is a number that is automatically assigned to the device that you are using by your Internet Service Provider (ISP).
- contact information stored on your device to make a payment or to send a payment notification (e.g. a phone number):
- your Camera for Liveness identity verification: we will request your permission to access camera, media and location to complete the Identity verification process.
  Identity verification increases your affordability and access to services provided by Power™.
- Credit Status Verification: we will request your permission to access to your Contacts, Media and calendar to determine your credit eligibility.
  - Contacts
  - Total number of contact
    - Contacts added in last week or last month
    - Frequency of adding a contact

    Note: We do not read or save your contact names or numbers
  - Media
    - Total no of media
    - Average size of media

    Note: We do not save the pictures or videos in your mobile device.
  - Calendar
    - number of events or meetings in your calendar.

    Note: Power™ does not access the list of participants or the content of the meeting or events including pictures or videos on your mobile device.

6.12. We may also collect general statistics in relation to your activity.

This privacy policy was last updated on 8th March 2022.

6.12.1 This data is made anonymous and used to improve your experience on this App and our Products and Services.

6.13. We collect information using cookies when you use our websites, or mobile application. Cookies are small pieces of information stored on your hard drive or in memory.

6.13.1 One of the reasons for using cookies is to offer you increased security.

6.13.2 They can also record information about your visit to our website, allowing us to remember you the next time you visit and provide a more meaningful experience.

6.14. We may also collect information from third party websites, applications or platforms containing our interactive content or that interface with our own websites and applications.

7. How do we collect personal information?

7.1. We collect most personal information directly from you whether in person, on the phone or electronically, for example when you interact with FEL to:

- apply for, register your interest in, or enquire about a product or service;
- provide us with feedback or make a complaint;
- visit our websites, or use our mobile application; and
- talk to us, or do business with us.

7.2. From time to time we collect personal information about you from third parties or organisations.

7.3. This may arise in circumstances where you have given your consent to do so, such as when you apply for credit or an insurance product

For example, we may collect personal information about you from:

- publicly available sources of information, such as public registers;
- your nominated representatives;
- your employer (for example, where you utilize Pay services;
- other organisations, who jointly with us, provide products or services to you or with whom we partner to provide products or services to you;
- service providers, such as companies that provide fraud prevention reports;
- insurers, lenders mortgage insurers, re-insurers and health care providers; and
- credit reporting bodies.

8. For what purposes do we collect, hold, use and disclose personal information?

8.1. The main reason we collect, use, hold and disclose personal information is to provide you with products and services (including where applicable, third party products and services) and to help us run our business.

This includes:

- checking whether you are eligible for the product or service;
- assisting you where online applications are not completed;
- providing the product or service;
- helping manage the product or service;
- helping us develop insights and conduct data analysis to improve the delivery of products, services, enhance our customer relationships and to effectively manage risks;
- understanding your interests and preferences so we can tailor digital content; and

8.2. We may also make your personal information anonymous which we have collected for the purposes described in this Privacy Policy.

8.3. As a result, this Privacy Policy will generally not apply to our use of anonymous information. However, we will continue to safeguard this anonymous information.

This privacy policy was last updated on 8th March 2022.

8.4. Where we use anonymous information together with other information (including personal information) and in doing so, we are able to identify you, that information will be treated as personal information in accordance with this Privacy Policy and applicable Privacy Laws.

8.5. We may use or disclose your information to comply with our legislative or regulatory requirements in any jurisdiction and to prevent fraud, criminal or other activity that may cause you, us or others harm including in relation to products or services.

9. How do we hold and protect your personal information?

9.1. Much of the information we hold about you will be stored electronically.

9.2. We store some of your information in secure data centres and with our contracted service providers (including cloud storage providers), and some of these data centres may be located outside Kenya.

9.3. We use a range of physical, electronic and other security measures to protect the security, confidentiality and integrity of the personal information we hold.

For example:

- access to our information systems is controlled through identity and access management controls;
- employees and our contracted service providers are bound by internal information security policies and are required to keep information secure;
- all employees are required to complete training about privacy and information security; and
- we regularly monitor and review our compliance with internal policies and industry best practice. Unfortunately, no data transmission over the Internet or data storage system can be guaranteed to be 100% secure.

9.4. If you have reason to believe that your interaction with us is no longer secure for example, if you feel that the security of any account you have with us has been compromised, please immediately contact us.

10. Who do we disclose your personal data to, and why?

10.1. We may share your personal data with our partners and third parties, including outsourced data processing undertaken on our behalf (some of which are located outside of Kenya), that we engage to provide products and services to you .

10.2. We information is shared, we require our service providers to keep such information under strict privacy regulations and prohibit them from disclosing such information to anyone for any other purpose

10.3. We do not share or disclose any non-public personal information about you to any other companies except as permitted by or required by law or for the purpose of marketing their products to you

10.4. By accepting these terms and conditions you are providing your explicit consent to share your information to these third party partners, some of which may be outside your local jurisdiction, if necessary for legitimate business purposes as defined in this policy.

10.5. As a digital credit provider we shall disclose any positive or negative information of yours to credit reference bureaus licensed and approved by Central Bank of Kenya.

10.6. By clicking and consenting to complete registration to the Power Marketplace **you are providing your explicit consent** to submission of positive & negative information for a Power™ to Pay, Borrow or Protect transaction.

10.7. To protect personal information, we enter into contracts with our service providers and other third parties that require them to comply with applicable Privacy Laws and and standards relating to data protection and information security.

10.8. These contracts, amongst other things, require our service providers to only use the personal information we disclose to them for the specific role we ask them to perform.

10.9. Generally, we use contracted service providers to help us in our business activities. For example, they may help us provide you with products and services, provide us with insurance, deliver technology or other support for our business systems, refer us to new customers, or assist us with marketing and data analysis.

These organisations may include:

- our agents, contractors and contracted service providers (for example, mailing houses, technology service providers and cloud storage providers);
- authorised representatives and credit representatives who sell or arrange products and services on our behalf;
- insurers, and health care providers;
- payment systems operators (for example, merchants receiving card payments);
- other organisations, who jointly with us, provide products or services to you, or with whom we partner to provide products and services to you;
- other financial services organisations, including banks, CMA custodians, and contracted service providers;
- debt collectors;
- professional advisors such as our financial advisers, legal advisers and auditors;
- fraud bureaus or other organisations to identify, investigate or prevent fraud or other misconduct;
- regulatory bodies, government agencies and law enforcement bodies in any jurisdiction; and
- credit reporting bodies:
- where we are required or authorised by law or where we have a public duty to do so;
- you may have expressly consented to the disclosure or your consent may be reasonably inferred from the circumstances; or
- we are otherwise permitted to disclose the information under applicable Privacy Laws.

11. Third Party Information

11.1. Power™ reserves the right to share aggregate loan and account information with third parties.

11.1.1 Customer Consent:

- In connection with your Power™ to Pay and/or maintaining a Power™ to Borrow credit facility with Power™, you authorise Power™ to carry out credit checks with, or obtain your credit information from a credit reference bureau. In the event of the account going into default, you consent to your name, transaction and default details being forwarded to a credit reference bureau as defined in the Digital Credit Provider Regulations 2021, and / or as amended.
- You acknowledge that this information may be used by banking institutions and other credit grantors in assessing any application for credit submitted by you.

11.1.2 Disclosure of information:

- You agree that Power™ may disclose details relating to your account to any third-party including credit reference bureaus, where disclosure requirements are as defined in the Digital Credit Provider Regulations 2021, and or as amended for the purposes of evaluating creditworthiness or any transaction with or credit application made with the Lender or for any other lawful purpose.
- ii. You agree that the Lender may disclose details relating to your account including details of your default in servicing financial obligations on your account to any third party including credit reference bureaus for the purpose of evaluating your credit worthiness or for any other lawful purpose.

This privacy policy was last updated on 8th March 2022.

12. Our Data Security

12.1. We have appropriate security measures in place to prevent personal information from being accidentally lost, used or accessed in an unauthorised way.

12.2. The following security procedures, and technical and organisational measures to safeguard your personal information have been put in place:

- In cases where personal data is being processed in third countries or third parties, a rigorous data protection impact assessment is being performed to ensure that your data is always secured.
- Our application platform is hosted in ISO 27001 certified secure data centres.
- Firewalls, intrusion detection and prevention, anti-virus and anti-malware and backup and disaster recovery is in place to prevent data loss or deletion.
- Our applications are engineered by following industry standards to minimise security vulnerabilities and updates on a regular basis.
- Intrusion detection and prevention secures the network traffic to the servers and applications.
- Anti-malware and anti-virus software is deployed to all of our servers and regularly scan and update with the latest anti-malware and virus signatures.
- We regularly apply critical, security patches and firmware updates to operating systems and physical hardware to minimise the risk of vulnerabilities
- Our employees undergo background screening and selection processes, with a restricted list of employees having access to secure areas of the applications, databases and physical infrastructure. Access to the secure areas are logged and auditable.
- We will use all reasonable efforts to safeguard your personal information. However, you should be aware that the use of the Internet is not entirely secure and for this reason we cannot guarantee the security or integrity of any personal information which is transferred from you or to you via the Internet.
- We limit access to your personal information to those who have a genuine business need to know it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

13. Breach Notification

13.1. In the event of a data security breach being identified we will Notify the Data Commissioner within seventy-two hours of becoming aware of a breach and to the data subject in writing within a reasonably practical period.

14. Your Data

14.1 Data Retention

- We keep most of your personal data for as long as your account is active. We retain the personal data you provide while your account is in existence or as needed to provide you with our services in line with data retention laws and regulations applicable in your local jurisdiction.

14.2 Rights to Access and Control Your Personal Data

- You can access your personal data from our services when you follow our procedures on data subject requests. You can always modify or update your personal data using the applicable menus in the app.
- When you wish to deactivate yourself from this mobile app, you are required to send a request to us and we shall contact you to validate the request for processing.

This privacy policy was last updated on 8th March 2022.

- A de-activated account may still have transactional history kept on our systems in accordance with applicable financial laws and data retention regulations or policies in your local jurisdiction.

14.3 Account Closure

- We retain your personal data even after you have closed your account if reasonably necessary to comply with our legal obligations (including law enforcement requests), meet regulatory requirements, resolve disputes, maintain security and prevent fraud.