Power Privacy Policy

This Privacy Policy ("Policy") was last updated in **May 2026.**

Contents

1. About this Policy..... 1
2. Definitions..... 1
3. Data Protection Principles..... 3
4. What kinds of Personal Data do we collect and hold?..... 4
5. Use and Disclosure..... 6
6. How do we collect Personal Data?..... 6
7. For what purposes do we collect, hold, use, and disclose Personal Data?..... 7
8. How do we hold and protect your Personal Data?..... 8
9. Who do we disclose your Personal Data to, and why?..... 8
10. Transfer of Personal Data outside Kenya..... 10
11. Credit Information Sharing..... 10
12. Our Data Security..... 10
13. Marketing Communications..... 11
14. Your rights as a Data Subject..... 11
15. Complaint Handling..... 12
16. Personal Data Breach Notification..... 13
17. Data Retention..... 13
18. Account Management, Deactivation, and Closure..... 13
19. Disclosure of Personal Data in Specific Circumstances..... 13
20. Children's Personal Data..... 14
21. Non-compliance..... 14
22. Contact information..... 14

1. About this Policy.

This Policy applies to all users of the Power Platform, prospective customers, existing customers, suppliers, merchants, agents, partners, visitors of our premises, and any other persons who interact with FEL or access our products and services through any channel. The Power Platform is operated by Frictionless Enterprises Limited ("FEL"), a company incorporated in Kenya and licensed by the Central Bank of Kenya as a Digital Credit Provider (Non-Deposit Taking Credit Provider). FEL is a wholly owned subsidiary of Power Financial Wellness Inc., a company incorporated in the United States, which is the ultimate holding company of the Power group. FEL trades as Power Financial Wellness and is the legal entity responsible for deploying and operating the Power mobile application on application stores and all other channels through which the Power Platform is made available. References to "Power", "we", "us", and "our" in this Privacy Policy are references to Frictionless Enterprises Limited. FEL is registered with the Office of the Data Protection Commissioner (ODPC) as both a Data Controller and a Data Processor in Kenya with identification number **332-972A-E36D**. References to "you", "your", "yours", "yourself", and "Data Subject" are references to the natural person whose Personal Data is collected and processed by us. The collection and processing of your Personal Data is in accordance with the Applicable Law. You are encouraged to read this Policy carefully to understand how we process your Personal Data. By accepting our terms and conditions or using our services, you acknowledge and agree to the practices described in this Policy. We may revise this Privacy Policy from time to time to reflect changes in our data processing practices or to comply with legal and regulatory developments. Where appropriate, we will notify you of material updates. This Policy should be read alongside our Terms and Conditions and any additional privacy notices or statements that we may provide at the point of data collection or processing. Such notices supplement this Policy and do not replace it.

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 Law"** means the Constitution of Kenya, the Data Protection Act, 2019 (the "DPA"), the DPA Regulations, and all other legislation, regulations, guidelines, and codes of practice applicable to the processing of Personal Data in Kenya, as amended from time to time;

2.3 **"Biometric Data"** means Personal Data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person that allows or confirms the unique identification of that person, including facial recognition data, selfie photographs processed for identity matching, fingerprint data, and liveness verification data. Biometric Data is Sensitive Personal Data;

2.4 **"Children"** means persons under the age of eighteen (18) years;

2.5 **"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;

2.6 **"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 the intention that it should be processed by means of such equipment;

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

2.7 **"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. For the purposes of this Privacy Policy, Power is the Controller unless otherwise stated;

2.8 **"data processor"** means a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of the data controller;

2.9 **"Data Protection Officer" or "DPO"** means the officer designated by Power pursuant to the DPA, responsible for overseeing Power's data protection strategy and compliance with the DPA and the Regulations;

2.10 **"Data Subject"** means an identified or identifiable natural person who is the subject of Personal Data;

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

2.12 **"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;

2.13 **"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 identity;

2.14 **"Personal Data"** means any information relating to an identified or identifiable natural person;

2.15 **"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;

2.16 **"Platform" or "Power Platform"** means the Power mobile application, any related website, and all digital services, products, and channels through which Power provides financial wellness products and services to users;

2.17 **"processing"** means any operation or set of operations that 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;

2.18 **"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;

2.19 **"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;

2.20 **"restriction of processing"** means the marking of stored Personal Data to limit their processing in the future;

2.21 **"Sensitive Personal Data"** means data revealing the natural person's race, health status, ethnic or 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;

2.22 **"Sub-processor"** means a natural or legal person, public authority, agency, or other body engaged by a Processor to carry out specific Processing activities on behalf of that Processor and/or the Controller; and

2.23 **"third Party"** means a 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.

In this Policy, unless the context requires otherwise: (i) the singular includes the plural and vice versa; (ii) a reference to any gender includes all genders; and (iii) headings and sub-headings are for convenience only and are not to be taken into account in interpretation.

3. Data Protection Principles

3.1. Power processes Personal Data in accordance with the data protection principles set out in the DPA. In particular, Power shall ensure that Personal Data is:

3.1.1. processed lawfully, fairly, and in a transparent manner in relation to the Data Subject (lawfulness, fairness, and transparency);

3.1.2. collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes (purpose limitation);

3.1.3. adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed (data minimisation);

3.1.4. accurate and, where necessary, kept up to date; every reasonable step shall be taken to ensure that inaccurate Personal Data is erased or rectified without delay (accuracy);

3.1.5. kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which it is processed (storage limitation);

3.1.6. processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful Processing and against accidental loss, destruction, or damage, using appropriate technical and organisational measures (integrity and confidentiality); and

3.1.7. processed in compliance with the rights of Data Subjects, and Power shall remain accountable for and demonstrate compliance with the foregoing principles (accountability).

4. What kinds of Personal Data do we collect and hold?

4.1. When you use Power on your mobile, we may collect your Personal Data to provide you with Power services and to verify your activity for security purposes.

4.2. The Personal Data that we collect about you will depend on the products or services that you apply for, or enquire about.

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

4.4. The information will still be Personal Data, whether it is true or not, and regardless of whether we have kept a record of it.

4.5. Some examples of Personal Data may include your:

(a) **Identity Data:** includes your name, username or similar identifier, national identity card or passport number, foreign national certificate (alien card), KRA PIN, photograph, date of birth, age, gender, marital status, title, nationality, and any other similar identifier.
(b) **Contact Data:** includes your postal address, physical address, email address, telephone numbers, and call data records.
(c) **Financial Data:** includes bank account details, mobile money account details, card payment details, and other payment information.
(d) **Transaction Data:** includes details of payments to and from you, loan disbursements, repayments, and other details of products and services you have acquired from us.
(e) **Credit History:** credit capacity, ability to be provided with credit, or creditworthiness.
(f) **Technical Data:** includes internet protocol (IP) address, login information, browser type and version, time zone setting and location, device information, operating system and platform, and other technology data from the devices you use to access our Platform.
(g) **Profile Data:** includes your account information, product and service preferences, feedback, survey responses, and interests.
(h) **Usage Data:** includes information about how you use our Platform, products, and services.
(i) **Communications Data:** includes your preferences for receiving marketing and other communications from us and Third Parties, and your communication preferences generally.
(j) **Biometric Data:** includes your voice, fingerprint, or selfie photograph captured for liveness detection and identity verification purposes.
(k) **Location Data:** includes geolocation information collected via the Platform where you have consented to location services, used to provide and improve location-relevant features.
(l) **Employment and Income Data:** includes information about your employer, income, and earned wages, collected in connection with earned wage access and salary advance services.
(m) **Device Data:** 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 app, including transactions, or to monitor your device for security purposes.
(n) **Sensitive Personal Data:** such as information relating to your health, and biometric data.

4.6. Throughout the life of your product or service, we may also collect and hold additional Personal Data about you. 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.

4.7. Our collection of 'Sensitive Personal Data' is further restricted to circumstances where we have obtained your express consent and to certain other permitted situations. 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.

4.8. When we collect information, we will disclose the specific purpose for which we use, request, and store your Personal Data. We will not use your Personal Data for any purpose other than the one for which we disclosed it to you unless you provide your express consent or unless we are permitted to do so by law. For example, we may collect facial biometric information to verify your identity or authorise transactions.

4.9. To access some services within this App, we may need to request access to certain features on your device. We will always ask for your permission before we access anything stored on your device. If you do not provide us permission, we may not be able to provide the service you requested.

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

(a) information about the device used, such as device IDs;
(b) 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);
(c) contact information stored on your device to make a payment or to send a payment notification (e.g., a phone number); and
(d) Your Camera for Liveness identity verification: We will request your permission to access the camera, media, and location to complete the Identity verification process.

4.11. On Apple iOS devices, we use ARKit to capture face 3D spatial orientation and facial expressions. We use this data to ensure the selfie being taken is of a live user for authentication and fraud reduction purposes. The ARKit information is processed entirely locally, and the spatial orientation/facial expression data is not submitted to any third (or first) parties. Identity verification increases your affordability and access to services provided by Power.

4.12. From time to time, we derive aggregated or anonymised data from Personal Data we hold, for example, analysing Platform usage patterns across our user base to understand which features are most accessed, or producing statistical reporting for internal planning and regulatory purposes. Data in this form does not identify any individual, directly or indirectly, and is therefore not Personal Data. Where, however, we combine aggregated data with other information in a manner that renders any individual identifiable, whether directly or by reference to an identifier, the resulting data constitutes Personal Data and will be handled in accordance with this Privacy Policy.

4.13. We collect information using cookies when you use our websites or mobile applications. Cookies are small pieces of information stored on your hard drive or in memory. We use cookies for the following purposes:

(a) to offer you increased security.
(b) to maintain your session and remember your preferences;
(c) to personalise content and offers based on your previous activity on the Platform;
(d) to analyse visitor behaviour and improve the performance and usability of our Platform; and
(e) to support security features, including fraud detection.

4.14. Third-party service providers and business partners may also place cookies on your device in connection with the Platform. We do not control these third-party cookies and are not responsible for their content or operation.

4.15. Most web browsers accept cookies by default. You may adjust your browser settings to refuse cookies or to alert you when a cookie is placed on your device. Please note that refusing cookies may affect the functionality and availability of certain features of our Platform.

4.16. 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.

4.17. 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, internet protocol (IP) address, your login identity data, browser type and version, device information, operating system and platform, time zone setting and location, browser plug-in types and versions, how your device or computer connects to our services, your web browser settings, and other technology on the devices you use to access our systems. This information may also be used or stored in combination with your Personal Data for these purposes, including to enable us to contact you if we detect a security threat.

4.18. We also collect Personal Data through closed-circuit television (CCTV) surveillance systems installed at our premises. CCTV devices are positioned at designated locations within Power's premises for the purposes of maintaining safety and security, and deterring and detecting crime.

4.19. Minor's Personal Data is not collected/processed unless they are accompanied by a legal guardian or parent.

5. Use and Disclosure.

5.1. We will only use your Personal Data for the purposes for which we collected it as indicated in this Privacy Policy, or for reasons we give you during the collection of the data. If we need to use your Personal Data for an unrelated purpose, we will notify you and seek your consent where necessary. Please note that we may process your Personal Data without your knowledge or consent if this is required or permitted by law.

5.2. 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.

5.3. We may also disclose your Personal Data to anyone we engage to do something on our behalf, and other organisations that assist us with our business.

5.4. As a provider of financial services, we have legal obligations to disclose some Personal Data to government agencies and regulators or agencies authorized by Applicable Law and regulations. e.g., Licensed Credit Bureaus.

5.5. If you fail to provide Personal Data that we require in order to provide a product or service, we may be unable to perform the contract we have with you, or may be unable to enter into a contract with you. We will notify you if this is the case at the relevant time.

6. How do we collect Personal Data?

6.1. We collect most Personal Data directly from you, whether in person, on the phone or electronically, for example, when you interact with Power to:

(a) apply for, register your interest in, or enquire about a product or service;
(b) open or operate an account on the Platform;
(c) complete an identity verification or KYC process;
(d) provide us with feedback or make a complaint;
(e) request marketing communications or other information;
(f) complete a survey or participate in a promotion;
(g) visit our websites, or use our mobile application;
(h) complete a survey or participate in a promotion, or do business with us; and
(i) pay using our services

6.2. From time to time, we collect Personal Data about you from third parties or organisations.

6.3. When you use the Platform, we automatically collect Technical Data, Usage Data, and Location Data (where permitted) through cookies, server logs, and similar technologies. 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

6.4. We may collect Personal Data about you from:

(a) publicly available sources of information, such as public registers, for example, i. the Integrated Population Registration Service (IPRS), Kenya Revenue Authority (KRA), National Transport and Safety Authority (NTSA), the Companies Registry, and other government registries;
(b) social media platforms, to the extent you have made your profile publicly accessible;

(c) your nominated representatives;
(d) your employer (for example, where you utilize Pay services;
(e) other organisations, who jointly with us, provide products or services to you, or with whom we partner to provide products or services to you, and/or with whom we have data sharing arrangements, and/or who have obtained your consent to share your data with us;
(f) service providers, such as companies that provide fraud prevention reports;
(g) insurers, lenders, mortgage insurers, re-insurers, and health care providers; and
(h) credit reporting bodies.

6.5. Where our Platform includes links to third-party websites or applications, those third parties may collect data about you independently. We do not control those third-party platforms, do not influence the data they collect, and are not responsible for their privacy policies. When you leave our Platform, we encourage you to read the Privacy Policy of every website or application you visit and to understand your rights in respect of that platform.

6.6. The Personal Data we hold about you must be accurate and current. Please keep us informed if your Personal Data changes during your relationship with us.

7. For what purposes do we collect, hold, use, and disclose Personal Data?

7.1. The main reason we collect, use, hold, and disclose Personal Data 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:

(a) checking whether you are eligible for the product or service;
(b) assisting you where online applications are not completed;
(c) providing the product or service;
(d) helping manage the product or service;
(e) helping us develop insights and conduct data analysis to improve the delivery of products, services, enhance our customer relationships, and to effectively manage risks;
(f) To carry out identity verification and Know Your Customer (KYC) checks, including liveness verification;
(g) To manage risk, detect and prevent fraud, money laundering, and other financial crime, and to comply with AML/CFT obligations;
(h) To administer and protect the Platform, ensure business continuity, and manage complaints and queries;
(i) To use data analytics and research to understand credit risk, improve our Platform, and personalise our products and services;
(j) To enforce our rights under any agreement with you, including debt recovery;
(k) To send you marketing communications about our products and services (subject to your opt-out right); and
(l) understanding your interests and preferences so we can tailor digital content;

7.2. For KYC and identity verification, we may review political affiliations to identify politically exposed persons, and may process criminal records data for fraud and money laundering prevention purposes.

7.3. We may also make your Personal Data anonymous, which we have collected for the purposes described in this Privacy Policy.

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

7.5. We will only use your Personal Data where we have a lawful basis to do so. The lawful bases for Processing under the DPA include: (i) your consent; (ii) performance of a contract to which you are a party; (iii) compliance with a legal obligation; (iv) protection of vital interests; and (v) our legitimate interests, where not overridden by your rights and interests.

7.6. 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.

8. How do we hold and protect your Personal Data?

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

8.2. 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.

8.3. We use a range of physical, electronic, and other security measures to protect the security, confidentiality, and integrity of the Personal Data we hold. For example:

(a) access to our information systems is controlled through identity and access management controls;
(b) employees and our contracted service providers are bound by internal information security policies and are required to keep information secure;
(c) data processing agreements with all Processors and Sub-processors
(d) data sharing agreements with third parties
(e) all employees are required to complete training about privacy and information security; and
(f) 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.

8.4. 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 at customersupport@power.io

9. Who do we disclose your Personal Data to, and why?

9.1. 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.

9.2. When 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

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

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

9.5. As a digital credit provider, we shall disclose any positive or negative information about you to credit reference bureaus licensed and approved by the Central Bank of Kenya.

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

9.7. These contracts, amongst other things, require our service providers to only use the Personal Data we disclose to them for the specific role we ask them to perform.

9.8. 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.

9.9. These organisations may include:

(a) our agents, Sub-processors, contractors, and contracted service providers (for example, mailing houses, technology service providers, identity verification providers, and cloud storage providers);
(b) authorised representatives and credit representatives who sell or arrange products and services on our behalf;
(c) third parties with legal standing: including trustees, executors, persons holding a power of attorney, and joint account holders, where applicable.
(d) insurers, and health care providers;
(e) payment systems operators (for example, merchants receiving card payments);
(f) other organisations, who jointly with us, provide products or services to you, or with whom we partner to provide products and services to you;
(g) other financial services organisations, including banks, CMA custodians, and contracted service providers;
(h) debt collectors;
(i) professional advisors such as our financial advisers, legal advisers, and auditors;
(j) fraud bureaus or other organisations to identify, investigate, or prevent fraud or other misconduct;
(k) regulatory bodies, government agencies, and law enforcement bodies in any jurisdiction;
(l) credit reporting bodies;
(m) where we are required or authorised by law, or where we have a public duty to do so;
(n) Where you may have expressly consented to the disclosure, or your consent may be reasonably inferred from the circumstances; or
(o) emergency and welfare services: where disclosure is necessary to protect your vital interests or those of another person.

9.10. We share your Personal Data with our Group entities, including affiliates and related entities within the Power Financial Wellness Inc. group, for legitimate business purposes consistent with this Privacy Policy.

9.11. In the event of a merger, acquisition, restructuring, or sale of assets, Personal Data may be transferred to the acquiring entity, subject to equivalent privacy protections.

10. Transfer of Personal Data outside Kenya

10.1. We may transfer your Personal Data to, or store and process it in, countries outside Kenya in the following circumstances:

(a) Where you have consented to the transfer;
(b) where we engage Processors or Sub-processors whose operations are conducted from outside Kenya;
(c) where a cross-border transfer is necessary to fulfil a legal obligation or to perform a contract with you; or
(d) where a transfer is necessary for the establishment, exercise, or defence of legal claims.

10.2. Where your information is transferred to affiliates of Power in other countries, we ensure that your Personal Data is protected by requiring that they follow the same rules when processing your Personal Data.

10.3. When we, or our permitted third parties, transfer or store information outside Kenya, they or we will ensure that it is lawful and that it has an appropriate level of protection, including transfer to jurisdictions that have established data protection laws, and entering legally binding agreements to ensure the security of your Personal Data.

10.4. Where your Personal Data is transferred to a country that does not provide an equivalent level of protection as Kenyan law, we will implement appropriate safeguards, which may include:

(a) a written Data Processing Agreement incorporating standard data protection clauses;
(b) binding corporate rules; or
(c) such other mechanism as may be recognised as adequate under Applicable Law from time to time.

11. Credit Information Sharing

11.1. We may 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. You acknowledge that this information may be used by banking institutions and other credit grantors in assessing any application for credit submitted by you.

11.2. We may disclose details relating to your account to any third party, including credit reference bureaus, where disclosure requirements are as defined under Applicable Law, 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.

11.3. We 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 creditworthiness or for any other lawful purpose.

12. Our Data Security

12.1. We have appropriate security measures in place to prevent Personal Data 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 Data have been put in place:

(a) Pseudonymisation, encryption, and anonymisation of Personal Data in transit and at rest.

(b) 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.

(c) Our application Platform is hosted in ISO 27001-certified secure data centres.

(d) Firewalls, intrusion detection and prevention, anti-virus and anti-malware, and backup and disaster recovery are in place to prevent data loss or deletion.

(e) Our applications are engineered by following industry standards to minimise security vulnerabilities and are updated on a regular basis.

(f) Intrusion detection and prevention secures the network traffic to the servers and applications.

(g) Anti-malware and anti-virus software is deployed to all of our servers and regularly scans and updates with the latest anti-malware and virus signatures.

(h) We regularly apply critical security patches and firmware updates to operating systems and physical hardware to minimise the risk of vulnerabilities

(i) 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 is logged and auditable.

(j) We will use all reasonable efforts to safeguard your Personal Data. 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 Data that is transferred from you or to you via the Internet.

(k) We limit access to your Personal Data 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.

12.3. We have procedures to detect, investigate, and respond to a suspected Personal Data Breach.

12.4. Where we have provided you with a password or PIN to access certain parts of our Platform, you are responsible for keeping that credential confidential and for not sharing it with any Third Party.

13. Marketing Communications

13.1. We strive to provide you with choices regarding the use of your Personal Data for marketing purposes. We may use your Identity Data, Contact Data, Technical Data, Usage Data, and Profile Data to determine what products, services, and offers may be of interest to you.

13.2. You will receive marketing communications from us if you have requested information from us or used our products and services, and you have not opted out. We will not use your Personal Data for marketing purposes where you have requested that we do not.

13.3. We will not share your Personal Data with Third Parties for marketing purposes without your Explicit Consent. Where you have given consent, you may withdraw it at any time.

13.4. You may opt out of receiving marketing communications from us at any time by:

(a) following the unsubscribe link in any marketing message sent to you;

(b) adjusting your notification preferences in the Platform settings;

(c) asking third parties to stop sending you marketing messages anytime by contacting them and following their opt-out process; or

(d) writing to us at customersupport@power.io.

13.5. Opting out of marketing communications does not affect Personal Data provided to us in connection with your use of our products and services, which we will continue to process on other lawful bases.

14. Your rights as a Data Subject

14.1. Subject to the conditions and exceptions provided under Applicable Law, you have the following rights in relation to your Personal Data:

(a) **Right to be informed:** the right to be informed about the collection, use, and processing of your Personal Data, including the identity and contact details of the Controller, the purposes of processing, the categories of data processed, and Third Parties with whom your data is shared.

(b) **Right of access:** the right to obtain confirmation as to whether Personal Data concerning you is being processed and, if so, to receive a copy of that data.

(c) **Right to rectification:** the right to request that inaccurate or incomplete Personal Data about you be corrected or completed without undue delay.

(d) **Right to be forgotten (erasure/ deletion):** the right to request the deletion of your Personal Data where it is no longer necessary for the purposes for which it was collected, where you have withdrawn consent, and there is no other lawful basis for processing, or where the data has been unlawfully processed, subject to any overriding legal or regulatory retention obligation. Contact us at customersupport@power.io to request deletion, noting that we may continue to retain your information if we are entitled to do so or obliged by law.

(e) **Right to restriction of processing:** the right to request that the Processing of your Personal Data be restricted in certain circumstances, such as where you contest the accuracy of the data or where you have objected to Processing pending verification. This includes the right not to be subject to a decision based solely on automated Processing, including profiling, that produces legal or similarly significant effects, except where such Processing is necessary for a contract, authorised by law, or based on your Explicit Consent.

(f) **Right to receive your Personal Data** in a structured, commonly used, and machine-readable format, and to request transmission of that data to another controller where technically feasible.

(g) **Right to object:** the right to object to the Processing of your Personal Data where Processing is based on our legitimate interests or is carried out for direct marketing purposes. We will cease such Processing unless we can demonstrate compelling legitimate grounds that override your interests, rights, and freedoms.

(h) **Right to withdraw consent:** where Processing is based on your consent or Explicit Consent, you have the right to withdraw that consent at any time without affecting the lawfulness of Processing carried out prior to withdrawal.

14.2. Before processing any request to exercise your rights under the DPA, we may ask you to verify your identity. This is a necessary safeguard: it protects you by ensuring that Personal Data is neither disclosed to nor acted upon at the request of a person who is not the Data Subject or their duly authorised representative. We may also request clarification of the scope of your request, where this is necessary to locate the relevant Personal Data or to determine the appropriate response.

14.3. We will respond to all valid requests within thirty (30) days of receipt, in accordance with regulation 10 of the Regulations. Where a request is unusually complex, involves the exercise of multiple rights simultaneously, or requires coordination with a Processor, we may extend this period by up to two further months. We will notify you of any such extension, and the reasons for it, within the initial thirty-day period, and will keep you informed of progress until the matter is resolved.

15. Complaint Handling

If you have a complaint about how we have collected, used, or otherwise processed your Personal Data, you should contact our Data Protection Officer (DPO) using the contact details provided in this Policy in the first instance. Upon receiving your complaint, our DPO will initiate an internal review process to investigate and resolve the issue. We will respond to your questions or concerns within fourteen (14) days of receipt. More complex queries may take time to resolve, and we will keep you informed if this is the case with your query.

16. Personal Data Breach Notification

We will report any Personal Data Breach to both the applicable regulatory bodies and the individuals or companies involved, as stipulated in the Applicable Law. If you want to report any concerns about our privacy practices or if you suspect any breach regarding your personal information, kindly notify us by sending an email to customersupport@power.io.

17. Data Retention

17.1. We will only retain your Personal Data for as long as reasonably necessary to fulfill the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your Personal Data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

17.2. In determining the appropriate retention period, we consider the following factors:

(a) the amount, nature, and sensitivity of the Personal Data;

(b) the potential risk of harm from unauthorised use or disclosure;

(c) the purposes for which we process the data and whether those purposes can be achieved by other means; and

(d) applicable legal, regulatory, tax, accounting, and other requirements.

17.3. By law, we have to keep basic information about our customers (including contact, identity, financial, and transaction data) for a minimum of seven (7) years after they cease being customers.

17.4. We may retain your Personal Data for a longer period than stated where: (a) there is a complaint, pending claim, or litigation reasonably anticipated; (b) a regulatory investigation or audit is underway; or (c) Applicable Law requires a longer retention period.

17.5. In some circumstances, we will anonymize your Personal Data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

18. Account Management, Deactivation, and Closure

18.1. You can access your Personal Data from our services when you follow our procedures for Data Subject requests. You can always modify or update your Personal Data using the applicable menus in the App.

18.2. 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.

18.3. A deactivated 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.

18.4. 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.

19. Disclosure of Personal Data in Specific Circumstances

19.1. We may disclose your Personal Data without your prior consent or knowledge in the following circumstances, to the extent required or permitted by Applicable Law:

(a) where required by a court order, subpoena, or other lawful legal process;
(b) where required by a regulatory authority, law enforcement agency, or government body with jurisdiction over us, including for AML/CFT reporting obligations;
(c) where disclosure is necessary in connection with national security, the prevention or detection of unlawful activity, or money laundering;
(d) where disclosure is necessary to protect the vital interests, health, or safety of any person; or
(e) where disclosure is necessary for the establishment, exercise, or defence of legal claims.

19.2. We will, to the extent permitted by law, notify you of any such disclosure where we are able to do so.

20. Children's Personal Data

20.1. Our Platform and services are not directed at Children. We do not knowingly collect Personal Data from any person under the age of 18 years.

20.2. Where the applicable age of majority in a relevant jurisdiction is higher than 18 years, the higher age threshold applies for the purposes of this section.

20.3. If a parent or legal guardian believes that a Child has provided Personal Data to us without appropriate consent, they should contact us at customersupport@power.io immediately. We will take steps to delete such data as promptly as practicable.

20.4. Where a product or service requires verification of age, and we have reason to believe a user is a Child, we will suspend or terminate access to that product or service pending verification.

21. Non-compliance

We reserve the right to end the contract with you for non-fulfillment of the conditions of this Policy and deny any request for information conflicting with this Policy.

22. Contact information

You may direct any queries, complaints, or requests relating to the processing of your Personal Data, including requests to exercise your Data Subject rights under the Data Protection Act, 2019, to us at the address below:

Power House, Kyuna Road, Westlands,
P.O. Box 77708—00508,
Nairobi, Kenya,
Tel: 254 (0)711082222,
Email: customersupport@power.io
Data Protection Officer (DPO): edwin@m-power.io