CREDITJAMBO

PRIVACY, COOKIES POLICY & DATA PROTECTION

Credit Jambo Ltd:
Privacy and Cookies Policy

1. About Us

Credit Jambo Ltd is a registered financial institution under the laws of the Republic of Rwanda under registration number 120675143 (here referred to as the "company" or "we" or "us") with its registered office at MN 233 St, Muhoza Sector, Musanze District, Northern Province - Rwanda.

At Credit Jambo, we believe that Privacy is a fundamental right. This is why we designed the privacy policy below, intended to show you how we collect, use, secure, and sometimes distribute some of your personal information acquired when you visit our website.

This Privacy Policy ("Policy") explains how Credit Jambo uses the personal information that it collects from you, or that you provide us, will be processed by us, including the type of information being collected, method of such information collection, use of such information, protection of such information and sharing of such information with third parties. The Policy applies to all of the products, subscriber-based services, mobile applications ("Services"), and websites offered by Credit Jambo Ltd, its branches, or affiliated companies.

Please read the following carefully to understand our views and practices regarding your data and how We will treat it. By continuing to visit Our website (www.creditjambo.com) and other Credit Jambo customer touchpoints, you accept and consent to the practices described in this Policy. If you disagree please do not use or access our website or other Credit Jambo Services.

By using our website (www.creaditjambo.com) you agree to the terms of this privacy policy. It is therefore important that you take time to carefully read through this policy before using our website. If you disagree/accept please do not use or access our website or other Credit Jambo Services. Credit Jambo reserves the right to change this policy at any time.

If you have any questions or concerns regarding this Policy, you should contact us at hello@creditjambo.com.

2. Why Do We Collect Your Information

2.1. We collect most of the personal information directly from you when you use our website and we retain them for as long as necessary to fulfill the purposes outlined in this privacy policy unless a longer period is required or permitted by law. Data may be collected in person, by telephone, or electronically and is aimed generally at understanding our clients, and their needs and improving their experience when using our website.

2.2. The following are specific purposes for which we collect and process your information:

2.2.1. Business Projections
2.2.2. Marketing
2.2.3. KYC purposes
2.2.4. Market Intelligence
2.2.5. Service provision and improvement

3. What Information Do We Collect?

3.1. The volume and type of information we collect depends on the way you use our website as well as the information you make available to us. Depending on your privacy settings we may obtain the following information:

3.1.1. **The information you make available to us**: by using our [services/website/platform], you provide us with certain personal information which includes your [Please add all info that you collect such as name, telephone contact, and email address].

3.1.2. **Information collected automatically**: some information will be collected automatically when you use our website. This information includes your product search history, like or saved products or services, any interactions with our customer service or our clients, your IP address as well as your location as and when it is enabled on your device. Additionally, information may be collected automatically through the use of cookies from our website. Still, you have the right to make modifications to the information we are allowed to collect or you can reject the cookies wholly [Make sure you have an option to reject].

3.1.3. **Information from other persons/third parties**: we collect some information from persons with whom you have relationships or interactions such as your address or location from carrier agencies, and social media platforms; for example: Facebook, X, Linkedin, Instagram, Whatsapp to allow easy or automatic collection of data or to keep your records up to date.

4. How Do We Use Your Information?

4.1. We limit the collection and use of personal information to the minimum we believe is necessary to deliver our service to you. We can do this by using your personal information in the following ways:

4.1.1. We use the information we collect to personalize your experience when you access our website. This is made possible because the collected information enables us to have a better understanding of your needs vis a vis the services we provide.

4.1.2. We use the information to contact you regarding your account, especially in case of any problems or disputes.

4.1.3. To aid the government or government agency in its mission to identify people for a specific purpose or public interest.

4.1.4. To send you emails about our products, updates, or other information we think may be valuable.

4.1.5. We use the information to help you improve and maintain our services.

4.1.6. Additionally, we use information to create and provide new services designed to enhance your experience with us.

5. Do We Ever Disclose Your Information To Third Parties?

5.1. We do not disclose any of your personal information to third parties outside the company family, except in the following circumstances:

5.1.1. When we have your explicit consent to make any such disclosure to a third party.

5.1.2. We have a legal obligation to disclose any information which might include some of the personal information we collected.

5.2. For this provision, the company family may include our holding company, subsidiaries, or sister companies and shall not be considered a third party.

6. How Do We Keep Your Information Secure?

6.1. We are committed to ensuring that your information is secure. To prevent unauthorized access or disclosure we have put in place suitable physical, electronic, and managerial procedures to safeguard and secure the information we collect.

6.2. The safety measures in place are as follows:

6.2.1. We use sophisticated codified language methods, such hashing, to convert sensitive data into keys or shorter, fixed-length values. Hashing makes sure that the original material is safeguarded even in the event of illegal access. By adding an extra layer of protection, this cryptographic technique makes it very difficult for any possible bad actors to interpret or exploit your data.

6.2.2. Our dedication to data security extends to our online presence. SSL Certificates are used on our website and platform. SSL is a security protocol that creates an encrypted connection between the user's web browser and our servers. This encryption guarantees that all information sent between you and our platform is confidential and safe.

6.2.3. We are also planning to partner with some companies including but not limited to technological developers which will help us in protecting our customers' data. In such circumstances, our partners enter confidentiality arrangements with us.

7. Do We Use Your Information In Communication?

We may use your personal information to contact you with promotional materials, product and company updates. You may at any time revoke or unsubscribe to their promotional materials by clicking the unsubscribe button at the bottom of the materials.

8. What Happens In Case Of Data Breach?

8.1. We have designed our website to ensure the safety of your information at all times. However, we recognize that there is a need to have clear safety measures in place to be followed in case of any security breaches which have become increasingly common in our industry with the growth of the internet.

8.2. We shall have a duty to inform you within a reasonable time of any data breach as and when it may arise.

8.3. We shall also provide you with clear options available to you depending on the nature of the breach to ensure the safe recovery of your data and account with the least inconvenience to you.

9. What Are Your Rights Regarding The Personal Information Collected?

9.1. Under this policy, you have the following rights:

9.1.1. Right to access your personal information to be able to make changes, update, and even delete any information.

9.1.2. Right not to provide certain information even though it may be necessary for you to use our website.

9.1.3. Where you do not wish to receive emails or notifications from us or want to stop receiving them.

9.1.4. Right to freely opt out at any point in time by notifying us of your intention to do so.

9.1.5. Right to delete your account along with your personal information at any time when you no longer feel interested in our services.

9.1.6. Right to request a copy of your information that we keep.

9.1.7. Right to request us to stop processing the personal information that we collected.

9.1.8. Right to us to rectify; complete or erasure your information.

9.1.9. Right to appeal to the supervisory authority in the country.

10. Does Our Website Contains Links To Third-Party Websites?

Our website may contain links to third-party websites. We are not responsible for the privacy policy practices or content of these websites. We encourage you to review the privacy policies of any third-party websites you visit.

11. Children's Privacy

Our website is not intended for individuals under the age of 16. We do not knowingly collect personal information from children. If we become aware that we have inadvertently collected personal information from a child under the age of 16, we will take steps to delete such information.

12. Collection Of Sensitive Data

Upon your explicit consent separate from the consent to this privacy policy, we may collect your sensitive personal information related to your health, racial, ethnic, origin, religious or philosophical beliefs, genetic or biometric data, sexual life or family details, and political opinion.

We emphasize the protection of your sensitive personal data when the firm gathers and handles it. Our dedication to protecting your privacy includes the deployment of strong security measures, such as:

1. **Data Encryption:** Sensitive personal data is encrypted during transmission and storage to preserve its secrecy.
2. **Secured Infrastructures**: Our systems and infrastructures are built with security in mind, using industry best practices to prevent unwanted access and breaches.
3. **Roles Management:** To guarantee that permissions are properly issued and managed, we use role-based access restrictions. This helps to ensure that only authorized people have access to sensitive personal data categories.

These security measures, including the previously stated tokenization, work together to minimize third-party access to and recognition of your sensitive personal data. We are committed to maintaining the highest data security standards and are always accessing and updating our policies to reflect changing threats and technology.

13. Data Protection: Safeguards, Security Measures and Mechanisms

To protect personal data, both technical and organizational measures have been put in place. These measures aim to ensure confidentiality, integrity, and availability of the data while complying with relevant data protection regulations such as GDPR (General Data Protection Regulation). Here's a comprehensive list of such measures:

13.1. Technical Measures:

13.1.1. **Encryption**: Encrypt data at rest and in transit using strong encryption algorithms to prevent unauthorized access.

13.1.2. **Access Controls**: Implement role-based access controls (RBAC) and least privilege principles to restrict access to personal data based on job roles and responsibilities.

13.1.3. **Multi-factor Authentication (MFA)**: Require additional authentication factors (e.g., SMS codes, biometrics) besides passwords to access sensitive data.

13.1.4. **Firewalls and Intrusion Detection/Prevention Systems**: Deploy firewalls to monitor and control incoming and outgoing network traffic. Intrusion detection/prevention systems can help identify and mitigate potential threats.

13.1.5. **Data Masking/Anonymization**: Mask or anonymize personal data in non-production environments to reduce the risk of unauthorized access.

13.1.6. **Data Loss Prevention (DLP)**: Implement DLP solutions to monitor and prevent unauthorized transfer or leakage of sensitive data.

13.1.7. **Regular Security Patching**: Keep software, operating systems, and applications up-to-date with the latest security patches to address vulnerabilities.

13.1.8. **Secure Development Practices**: Follow secure coding standards and conduct regular security reviews to identify and mitigate security flaws in applications.

13.1.9. **Logging and Monitoring**: Maintain logs of system activities and regularly monitor for suspicious behavior or unauthorized access attempts.

13.1.10. **Endpoint Security**: Use endpoint security solutions such as antivirus software, endpoint detection and response (EDR) tools, and mobile device management (MDM) to protect devices accessing personal data.

13.2. Organizational Measures:

13.3. **Data Protection Policies and Procedures**: Develop and enforce clear policies and procedures for handling personal data, including data classification, access control, and incident response.

13.4. **Employee Training and Awareness**: Provide regular training to employees on data protection best practices, including phishing awareness, password hygiene, and incident reporting.

13.5. **Privacy by Design/Default**: Incorporate privacy considerations into the design and development of systems and processes from the outset.

13.6. **Data Minimization**: Collect and retain only the minimum amount of personal data necessary for the intended purpose.

13.7. **Vendor Management**: Assess the security practices of third-party vendors and service providers handling personal data and ensure they comply with relevant data protection standards.

13.8. **Incident Response Plan:** Develop and regularly test an incident response plan to effectively respond to data breaches and security incidents.

13.9. **Data Impact Assessments (DPIA)**: Conduct DPIAs to identify and mitigate privacy risks associated with processing personal data.

13.10. **Data Retention and Disposal**: Define data retention periods and securely dispose of personal data when it is no longer needed for its original purpose.

13.11. **Privacy Governance Framework**: Establish a privacy governance framework with clear accountability and oversight of data protection responsibilities.

13.12. **Regular Audits and Compliance Checks**: Conduct regular audits and compliance checks to ensure adherence to data protection regulations and internal policies.

Detailed procedure on how we deal with data breaches and cyber security incidents can be found in the CreditJambo_INCIDENT RESPONSE PLAN