

PRIVACY POLICY

1. INTRODUCTION

- 1.1. Rent Pay (Pty) Ltd., trading as ACPAS (hereinafter referred to as “ACPAS”) provides you and the entity which you represent (collectively, “you/your”) with access to its Loan Management Software and Payment Gateway Services as a Third-Party Payment Provider (“TPPP”).
- 1.2. Throughout this policy the products and services made available to you, in accordance with the Service Level Agreement you have entered into with ACPAS, shall be collectively referred to as “the Products”.
- 1.3. This Privacy Policy governs the relationship between you and ACPAS, as it pertains to your personal information and the personal information which you collect from consumers in the ordinary course of business.
- 1.4. Your use of the Products is entirely dependent on the acceptance of this Privacy Policy. Should you not agree with the contents of this policy, please do not proceed to make use of the Products. Please note that you will be deemed to have accepted this policy if you click the “I agree” tick-box and continue to use the Products.
- 1.5. You will be required to accept this policy each time you access the Products, failing which access will not be granted to use the Products.

2. SCOPE

- 2.1. This policy contemplates to the Personal Information of yourself as well as the Personal Information collected, used, stored and protected in the course of ACPAS’ business, including its Products and websites.
- 2.2. This policy will also outline the choices available to you regarding our use of your Personal Information or the Personal Information collected through the utilization of the Products and how to access, update and request deletion of such information.

- 2.3. The use of Personal Information shall be limited to the purpose of providing the Services for which you have engaged ACPAS.
- 2.4. This policy is aimed at meeting the statutory privacy requirements applicable within South Africa. This policy will be continually developed and maintained in order to ensure consistent compliance with the aforementioned requirements.

3. PERSONAL INFORMATION

- 3.1. Personal Information is information or data which identifies or relates to specific individuals. In respect of this policy, such information will also relate to your customers (consumers) and includes, but is not limited to, the following information: -

- 3.1.1. Name;
- 3.1.2. Age;
- 3.1.3. Gender;
- 3.1.4. Ethnicity;
- 3.1.5. Identity Number;
- 3.1.6. Assets & Liabilities;
- 3.1.7. Income;
- 3.1.8. Payment Records;
- 3.1.9. Account Numbers;
- 3.1.10. Payment and/or Deduction dates;
- 3.1.11. Transactional History of banking accounts;
- 3.1.12. Agreements/mandates entered into;
- 3.1.13. Browsing patterns and usage;
- 3.1.14. Hardware specifications.

4. YOUR CONSENT & AGREEMENT

- 4.1. By submission of your details and/or utilization of the Products, you expressly consent to the use and disclosure of your Personal Information, in the manners which will be outlined in this Policy.
- 4.2. If you, or your customer, object to any of the potential uses of your Personal Information, as outlined in this Part, please do not continue use of the Products.

5. SECURITY & CONFIDENTIALITY

- 5.1. In order to render services to you and provide you with use of the Products, ACPAS is required to collect and disclose personal information of you and/or personal information collected by you from consumers. The aforementioned personal information will only be disclosed to specific third parties and only for the purposes of providing you with the Products and/or any services which ACPAS is required to render in respect of the Products, or as may be required or prescribed by law.
- 5.2. We understand the value of Personal Information and have therefore taken all reasonable measures to ensure that the Personal Information collected through the use of the Products is protected from loss, misuse or unauthorized access and/or alteration.
- 5.3. ACPAS has undertaken and maintains a series of IT-Security measures and protocols in respect of the Products. Although full disclosure is not required for the purposes of this Policy, such IT-Security measures may be requested from ACPAS by directing correspondence to the contact details contained in this Policy.
- 5.4. ACPAS maintains the following internal protocols to ensure the security and integrity of data and personal information: -
 - 5.4.1. Only authorized personnel have access to the data collected, processed and retained through the use of the Products and such personnel are trained and informed of their obligations and responsibilities in respect of safeguarding and protecting the data to which they have access;
 - 5.4.2. No unauthorized personnel have access to the data collected, processed and retained through the use of the Products and any such unauthorized person is aware of the consequences and actions which may be taken against them for accessing, or attempting to access, such data;

5.4.3. Internal policies and protocols provide for continuous engagement with service providers, partners, banks and integrational measures of ACPAS, to ensure that the Products are continuously afforded the latest security and privacy updates, whether internally or procured from a service provider, and that all agreements with such service providers, partners, banks and integrational measures are maintained and renewed.

6. DATA CONTROLLER & DATA SUBJECTS

6.1. ACPAS does not, under the Service Level Agreement entered into for the provision of the Products, collect, process or retain data, of its own accord or without your consent and direction. The role of ACPAS in the relationship between it and you is to make the Products available and to continuously maintain and develop the Products for your use and benefit in the conduction of your business. Therefore, without your use of the Products, no data can be collected. Yet, it is the role of ACPAS to retain the data collected by you at all relevant times.

6.2. For the reasons set out above, you are the “Data Controller”. You are the one who collects Personal Information from data subjects and directs ACPAS to retain, protect and utilize such information in the manner required to give effect to the Service Level Agreement.

6.3. The consumers who enter into credit agreements with you and provide you with their Personal Information for the purposes of loan applications, loan agreements and payment mandates are the “Data Subjects”.

6.4. Data Subjects who seek to access, correct, amend or delete data relating to their Personal Information, should address such a request to the Data Controller (you). You are then required to execute the request if: -

6.4.1. the request is reasonable;

6.4.2. executing the request is lawful and does not impede on other requirements which you are required to meet;

- 6.4.3. the request is not in pursuit of criminal activity, or will allow the Data Subject to engage in criminal activity;
 - 6.4.4. executing the request would not be against public interest and the pursuit of justice; and
 - 6.4.5. you have not received any order or direction from competent authority directing you not to execute such a requests in relation to that specific Data Subject, or a group or collective of Data Subjects which includes the Data Subject making such a request.
- 6.5. Should a request be received for access, amendment or deletion of data to which you do not have access, and ACPAS does have access to such data. The request must be sent to the Information Officer of ACPAS, who will investigate and, if appropriate, execute the request.
- 6.6. If you, or the company which you represent, seek to amend any Personal Information of yourself or of your business which is held by ACPAS and not accessible through the Products, a request should be directed to the Information Officer of ACPAS, the contact details of which are contained in the latter portion of this Policy.

7. OUR USE OF INFORMATION AND DATA COLLECTED

- 7.1. ACPAS may, as a result of the Service Level Agreement, transfer and disclose the Personal Information collected through the use of the Products, for the purposes of: -
- 7.1.1. Providing the Products to you, and complying with instructions received from you;
 - 7.1.2. Verifying your identity, or the identities of other Data Subjects, with whom you conduct business;
 - 7.1.3. Taking credit decisions;
 - 7.1.4. Compliance with Laws, Public Duties, Court Orders and Authorized Investigations;

- 7.1.5. For the purposes of security and crime prevention;
 - 7.1.6. For ACPAS' internal use, with the aim of improving the Products and services which ACPAS render in relation to the Products, and for the purposes of market analysis in order to improve the Products, its offerings or that of its associated companies;
 - 7.1.7. The conduction of market research;
 - 7.1.8. Disclosure to credit bureau for the purposes of drawing credit reports and receiving information contained therein;
 - 7.1.9. Disclosure of payment mandates to registered banks of South Africa in order to create payment instructions and/or deductions;
 - 7.1.10. Providing you with information via email, telephone, or other means in respect of ACPAS' products and/or services, from time to time.
- 7.2. Despite the use of the data and/or Personal Information utilized as described above, the Personal Information will still be utilized in a manner which compliant with the privacy and data laws of South Africa and is afforded the same level of security as data and Personal Information, not being utilized.
- 7.3. ACPAS may disclose or use your data with third parties involved in the process of providing the Products to you. These third parties have been carefully vetted and selected before a trusted relationship is established. All third-party service providers are contractually and statutorily bound to maintain the confidentiality and security of the data and Personal Information provided to them, and are restricted to only utilizing such data or Personal Information for the specific purpose to which it relates.

8. OTHER DATA COLLECTED

- 8.1. In addition to the personal information which is collected, processed and retained through the use of the Products, ACPAS is required to collect additional data relating to you, or the business which you represent, in order to provide you with the Products. This information includes, but is not limited to: -

- 8.1.1. All personal information which you (and the company) submitted to ACPAS when entering into the Service Level Agreement, or during negotiations for entering into a Service Level Agreement;
 - 8.1.2. All personal information completed in the ancillary agreements with third parties which you had to agree to or complete in order to use the Products (for example, agreements or declarations required by banks before taking payment instructions);
 - 8.1.3. The requisite financial information, as submitted to ACPAS, by you;
 - 8.1.4. All other information submitted to ACPAS, by you, as part of the onboarding process of the Products;
 - 8.1.5. Information relating to your computer, your IP address, your operating system and browser type. This information is strictly used to ensure that you are able to effectively use the Products.
 - 8.1.6. Statistical Data and browsing patterns, which do not identify any individual's personal information including general internet usage through the use of a cookie file which is stored in your computer's hard drive. Cookies enable ACPAS to improve its offerings to you, estimate audience sizes and usage patterns, store information relating to your preferences and to recognize you when you return to our website. Please note that your browser settings can be set to refuse cookies, but that this will detract from certain advantages gained when ACPAS is able to access the aforementioned data.
- 8.2. The data and Personal Information noted above are also retained and protected in accordance with the protocols and measures outlined in this policy.
 - 8.3. Please note that third parties advertise on our websites and that there are links to such third parties' websites. However, we do not have access to, or control over their websites and therefore cannot take responsibility for the information or data collected from their websites.

9. **PERSONAL IDENTIFICATION NUMBER**

- 9.1. For the purposes of using the Products, you are provided log-in details in the form of a username and password. It is your responsibility to maintain the confidentiality of these particulars and we cannot be held liable for breaches which occur as a result of sharing, disclosing and/or disseminating these particulars.

10. TRANSFERRING OF DATA TO FOREIGN TERRITORIES

- 10.1. In order to maintain the most effective levels of security for data and personal information, ACPAS may be requires to transfer the data it retains outside the borders of South Africa to secure servers in foreign territories.
- 10.2. When data or Personal Information is transferred outside South Africa, ACPAS will ensure that the data and information is held securely to standards at least as good as those required within South Africa, and that such data and information is only utilized for the purposes for which is was collected.
- 10.3. ACPAS retains the right to store personal information and data on any secure server in any territory, internationally, provided that such servers meet the data and information protection standards of South Africa.

11. DATA RETENTION PERIODS

- 11.1. ACPAS will retain the Personal Information and data collected by it for as long as your account is active, or as needed in order to provide services to you and in accordance with any legislative requirements, as may be prescribed from time to time.
- 11.2. Personal Information and data will be retained, regardless of the existence of a relationship between you and ACPAS, for as long as necessary to comply with its legal obligations, to resolve disputes, for the enforcement of its rights, or as may be directed by a competent authority.

12. DATA BREACH

- 12.1. In the event that a data breach occurs, or there are reasonable grounds to believe that a data breach has occurred and that the Personal Information of

you or of a data subject as been accessed, acquired, compromised or leaked, ACPAS will:-

- 12.1.1. As soon as practicable, take the appropriate steps to limit the breach and restore the integrity and security of the system;
- 12.1.2. As soon as reasonable, report to the affected Data Controller(s) the relevant facts and extent of the breach or compromise;
- 12.1.3. If applicable, report on the identity of the person(s), group(s) or organization(s) suspect of, or known to have, caused the breach or compromise and/or accessed the Personal Information, unless ACPAS has received an order or direction from a competent authority not to do so;
- 12.1.4. Notify you immediately, if it is necessary for you to stop use of the Products and the extent to which you are required to stop using the Products, in order to restore the integrity of it and avoid furthering the scope of the breach or compromise.

13. RIGHT TO ACCESS & AMEND

- 13.1. You have the right to access the Personal Information that is retained, relating to your use of the Products. To obtain a copy of your Personal Information, as held by ACPAS, please direct an email to the Information Officer, using the contact details listed in this policy. Should there be any amendments required to the data or Personal Information, a request may be directed to the Information Officer, in the same manner.
- 13.2. Similarly, the Data Subjects whose Personal Information is collected through the use of the Products, have the same right contemplated in the preceding paragraph, as it relates to their Personal Information. However, as the Data Controller, their request must be submitted to you, whereafter you will direct an instruction to ACPAS' Information Officer, using the contact details listed in this policy, if you do not have access to amend such personal information. Should there be any amendments required to the data or Personal Information, a request may be made in the same manner.

- 13.3. Although ACPAS takes care to ensure that all data output is true and correct, the validity of data and of reports generated using the Products, are both reliant on the accuracy of the information which you input. Therefore, ACPAS cannot be held responsible for inaccuracies of data captured by you.

14. **ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT**

- 14.1. ACPAS subscribes to the principles outlined in Section 51 of the Electronic Communications and Transactions Act, 2002 (“ECTA”), which governs your right to having your Personal Information kept private.
- 14.2. In accordance with Section 51 of ECTA, we will only collect, collate, process and store (“use”) your Personal Information, with your permission, as set out in this Policy, unless we are legally obligated to do otherwise. The information and data which we use in terms of this policy shall only be used for the lawful purpose in terms of which it is required.
- 14.3. This Policy discloses the specific purpose for which Personal Information of you and of your Data Subjects, as collected through use of the Products, is requested, used and stored.
- 14.4. No Personal Information will be utilized for any reason other than the reasons outlined in this policy, without your express consent to do so, unless ACPAS is ordered or directed to do so, by a competent authority.
- 14.5. Personal Information retained by ACPAS will be disclosed, without your consent if: -
- 14.5.1. It is are required by law to do so;
 - 14.5.2. Disclosure is in public interest; **and**
 - 14.5.3. Such disclosure will be deemed to have carried your express or implied consent.

- 14.6. You are herewith notified that you are entitled to, and understand that you may, option out of any mailing list maintained by ACPAS for commercial and marketing communications.

15. **MARKETING**

- 15.1. By acceptance of this policy and subject to privacy laws, you consent to be contacted for marketing purposes and agree to be included in marketing efforts by ACPAS. This includes telemarketing, mass distribution of mail, email and sms messages, and the sale or distribution of a marketing or customer list by ACPAS to a third party. You may option out of any such marketing campaigns or efforts by giving any written notice to ACPAS.
- 15.2. In respect of emails sent by ACPAS, you may unsubscribe from such mailing lists by using the “unsubscribe” link at the bottom of such emails. This will not affect your transaction and administration related emails in respect of the Products.
- 15.3. If you wish not to receive marketing calls, please advise the representative calling you and you will be added to our “Do Not Call” list.
- 15.4. ACPAS maintains a “Do Not Call” and “Do Not Mail” list, as legislatively prescribed.

16. **PRIVACY EXCLUSIONS**

- 16.1. As detailed in this Policy, ACPAS has taken great care in ensuring the Personal Information and data about you and of your customers are protected and confidential. However, ACPAS will not accept any liability of Personal Information is breached or compromised if: -
- 16.1.1. the breach or compromission occurred in relation to data stored directly on your hard drive;
- 16.1.2. the breach or compromission occurred as a result of your failure to keep your usernames and passwords private and confidential or distributed the aforementioned information willingly and/or allowed such information to be distributed;

- 16.1.3. You committed, or allowed to commit without intervention, the use of your usernames and passwords for the purposes of breaching or compromising data;
- 16.1.4. You engaged in any form of illegal activity, the consequences of which gave rise, directly or indirectly, to a breach or compromise of data;
- 16.1.5. The data was never in possession of ACPAS;

17. AMENDMENTS

- 17.1. ACPAS reserves the right, at its sole discretion, to update, modify, amend or replace this policy, whether in part or in whole, from time to time as may be required by it, or by law, from time to time.
- 17.2. You agree to review this policy each time you use the Products or access the ACPAS website.
- 17.3. Unless the contrary is clearly indicated in the updated policy, such updated policy shall replace and supersede all previous policies.
- 17.4. The most recent version of this Policy may be accessed, at any time, by following this link: <https://secure.acpas.co.za/Solution/Login.aspx> and selecting the ACPAS Privacy Policy document.

18. JURISDICTION

- 18.1. This policy will be governed, regulated and interpreted in accordance with the laws of South Africa and both you and ACPAS submit to the jurisdiction of the South African court with the appropriate jurisdiction.

19. CONTACT DETAILS

- 19.1. The contact details of ACPAS and of its Information Officer for all matters relating to this policy, shall be as follows:

THE INFORMATION OFFICER
RENT PAY (PTY) LTD t/a ACPAS
RENT PAY (PTY) LTD t/a ACPAS
92 Jean Avenue
Doringkloof, Centurion
info@acpas.co.za
012 665 0319

20. **WARRANTEES**

- 20.1. By agreeing to this policy and continuing to use the Products, you warrant that you are legally entitled to do so, on behalf of the entity which you represent;
- 20.2. By obtaining any services and products, or entering into any agreement with ACPAS which results in you obtaining access to the Products, you warrant that you are duly authorized to enter into such agreements and obtain access on behalf of the entity which you represent;
- 20.3. You warrant that you will not use the Products, or any of its affiliated services, or any information to which you have access, or which is sent to you by ACPAS, for any purpose which is unlawful in South Africa, in international law, or prohibited in terms of this policy.
- 20.4. You indemnify ACPAS from any damage or liability which may arise, whether directly or indirectly, as a result of your breach of any portion of this Policy.

21. **ACCEPTANCE**

- 21.1. Your acceptance of these terms and conditions is recorded by clicking "I Agree" and the details thereof are as follows: ACPAS will store a register of users and last date and time that the users accepted this policy by clicking on the "I Agree" button when logging into the ACPAS secure software platform.