

Rancard Privacy and Data Protection Policy

1. Policy Scope

The Policy is designed to regulate the collection, maintenance and use of Consumer Personal Information generated as a result of contractual relations between Rancard, the Operator and the Content Provider or Developer in all aspects relating to the publication and use of APIs, Network Capacities, Software Development Kits (SDKs) and Other Services for development through the Developer Platform, as well as all matters relating to the loading/use of Contributions and Applications and/or marketing of the Applications by the Developer albeit in the Operators' Applications Stores, or through any other channel for the use of Consumers.

2. Consumer Data Protection

Rancard is entrusted with the confidentiality of millions of peoples' communications and for managing volumes of personal information. We continue to foster the trust and confidence of customers and employees in the way we handle their personal information and provide services.

This Policy concerns the handling of customer personal information, which includes the collection, storage, access, use, updating, disclosure, disposal, destruction or any other processing of such information. It is intended to provide a comprehensive set of rules for the management of customer personal information throughout the customer lifecycle, including

Rancard may collect and maintain information on individual Consumers reasonably required for its business purposes. Consumers may provide their personal information when they access, use or sign up to Rancard's Services or its Products and Information contained thereof, either on Rancard's Platforms or Third Party Platforms supported by Rancard's Products/Platforms. Information may include but not limited to name, email address, postal address, telephone or mobile number or date of birth, depending on the activity the Consumer engages in. By submitting their details, Consumers enable Rancard (and where applicable its contractors and affiliates) to provide Consumers with the services, activities or online content they select.

It is the policy of Rancard that;, the collection and maintenance of information on individual Consumers shall be—

- (a) fairly and lawfully collected and processed;
- (b) processed for limited and identified purposes such as serving recommendations to the consumer
- (c) relevant and not excessive ;
- (d) accurate ;
- (e) not kept longer than necessary ;
- (f) processed in accordance with the Consumer's other rights ;
- (g) protected against improper or accidental disclosure ; and
- (h) not transferred to any party except as permitted by any terms and conditions agreed with the Consumer, as permitted or required by applicable laws or regulations.

Rancard shall meet generally accepted fair information principles including:

- (a) providing notice as to that individual Consumer information they collect, and its use or disclosure ;
- (b) the choices Consumers have with regard to the collection, use and, disclosure of that information ;
- (c) the access Consumers have to that information, including to ensure its accuracy ; and
- (d) the security measures taken to protect the information, and the enforcement and redress mechanisms that are in place to remedy any failure to observe these measures.

These rules apply to individual Consumer information whether initially provided verbally or in written form, so long as that information is retained by Rancard in any recorded form.

3. Third Party Actions

3.1 API's that can allow third parties to access personal user data generally requires an extension to normal data privacy terms. For example for APIs that allow third parties to develop applications which users of the service will use to access their own data, their data will most likely pass through the Third party's servers or code.

3.2 The Management of the Third party shall be committed to implement and adhere to the privacy and data protection policy of Rancard.

3.3 The Third party shall sign a Non-Disclosure Agreement or an Agreement with a confidentiality clause which mandates that the Third party shall not disclose any information related to Rancard which is identified as 'Restricted', 'Confidential' or 'Internal' to Rancard. The Third party shall ensure that they read, accept and sign the Non-Disclosure Agreement/Agreement with the relevant confidentiality clause provided by Rancard.

3.4 Controls shall be in place so that information assets or information processing environment used for providing services to Rancard/Consumers are physically/logically segregated from other customers.

3.5 This is true even if authentication patterns such as openAuth are used. OpenAuth simply means username/password credentials do not need to be shared with third parties, but – once authorized – applications may still access user data and hence privacy guidelines need to strictly apply to API usage.

4. Changes to the Privacy Policy

Rancard may amend this Privacy Policy from time to time. Use of information we collect now is subject to the Privacy Policy in effect at the time such information is used. If we make major changes in the way we collect or use information, we will notify you by posting an announcement on the Website or sending you an email. In any case, you can track all changes via the Terms of Service Tracker. A user is bound by any changes to the Privacy Policy when he or she uses the Services after such changes have been first posted.

