# PRIVACY POLICY

## INTRODUCTION

When you register and use carclub-rentals.com ("**this website**"), you gain access to the enhanced websites, services and other content from Berggruen Car Rentals Private Limited, India and its affiliates (collectively known as **"Berggruen"**). When you register and use this website, you provide personally identifiable information. This Privacy Policy (**"Policy"**) explains the information practices that apply to your personally identifiable information. Berggruen has implemented this privacy policy to explain to you how it uses and protects personally identifiable information that may be collected from you through this website.

## APPLICABILITY

By accessing and using this website, your use indicates your agreement to the terms of this Policy. **If you do not agree to the terms of this Policy, please do not use this website.**

This Policy applies only to information that Berggruen collects about you as a user of this website. This Policy does not apply to information about you, collected by Berggruen's affiliated providers, or third party websites and offering linked to or otherwise accessible from this website. The information collected or received by Berggruen's affiliated providers and these third parties is subject to their own privacy policies.

## PERSONAL INFORMATION PROVIDED BY YOU

As per the format of the website, you will not be required to provide personally identifiable information as a condition of browsing this website. However, Berggruen may collect personal information for facilitating transactions with you. **By providing**
**Berggruen, personally identifiable information through this website, you acknowledge and consent to the collection, use and disclosure of personally identifiable information of the type and for the limited purposes described in this Policy.** The personally identifiable information that Berggruen may collect includes, but is not limited to your:

- Name
- Address
- Telephone numbers
- Email address
- Driver's license number
- Date of birth
- Credit card number
- User name and password
- Any other information provided by you

Berggruen may also receive information about you from credit reporting agencies and other third parties. Berggruen would not collect any sensitive information about you (i.e. personal information specifying racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information pertaining to personal or intimate details of an individual's life).

## Physical Security

1. **How is the data center protected from unauthorized users? Please list details.**

   Visitors have to complete following formalities to get access in to Reliance IDC:

   I. Send an email for Work permit request to IDC Tech desk through Authorized person for accessing the Data center
   II. The case ID is created by IDC Tech desk and the visitor has to quote the same to the Security personnel while entering the Data center.
   III. The Visitor is required to make an entry into the Visitor register kept at the reception
   IV. Access card is issued to the Visitor post verification of case id by the Security Control room
   V. Access to the visitor is provided only for the required areas in which he would be accessing
   VI. There is CCTV surveillance across the Data center
   VII. There are Security personnel deployed at strategic locations

2. **Are visitors and housekeeping escorted by authorized personnel?**

   Yes

3. **What type of physical access control is used for entering the company campus?**

   Biometric Access system with pin and finger scan

4. **Are the physical security systems monitored 24/7?**

   The Security control room is manned 24X7 for monitoring the Physical security systems

5. **Are photo IDs issued for employees?**

   Yes. Photo ID based access cards are issued to employees

6. **Provide detail on third-party security audits (e.g. SSAE16 SOC2, ISO, etc.) you have had performed. Include copies of these audits if possible.**

   I. At what level are you certified?
   II. Date of first certification?
   III. Date of last certification?

***ISO 27001:2013*** *- Date of first certification: 30-May-2008, Date of last certification: 30-May-2017*
***ISO 9001:2015*** *- Date of first certification: 26-Feb-2005, Date of last certification: 15-Mar-2017*
***ISO 20000-1:2011*** *- Date of first certification: 11-Dec-2008, Date of last certification: 11-Dec-2017*

## Disaster Recovery

1. **Emergency power capabilities installed?**

   Yes. UPS systems and Diesel Generators are installed for emergency power requirements

2. **Do you have documented Emergency escalation plans?**

   Yes

## Intrusion Protection

1. **Are externally facing servers OS hardened?**

   Yes. OS hardening reviews are carried, and accordingly hardening process is initiated

2. **Are externally facing web servers using Web Application Firewalls?**

   No (Not part of subscribe service)

3. **Are your web applications subject to Web vulnerability assessments?**

   No (Not part of subscribe service)

4. **Are firewalls used between external and internal services?**

   Yes

5. **Are you using OS vulnerability assessment tools such as Nessus?**

   No

6. **Are you using Intrusion Detection appliances in your external environment?**

   Yes

7. **Is Anti-virus installed on all servers/clients?**

   Anti-virus services not being provided for clients

8. **Has the system undergone security analysis or penetration testing, either by TI personnel or third-party firm? If so, please provide review date and summary of findings.**

   No

## Data Protection

1. **How is customer data segregated, by server, database, etc.? Can we request fully dedicated resources?**

   Customer data segregation is carried out via dedicated hosting services. Fully dedicated resources may be requested for

2. **Describe your processes or procedures in place for protecting TI's data against loss not due to a disaster, including, but not limited to data loss from laptop theft, hot-site files mishandled, backup tapes lost, etc.**

   I. Access Control maintained in laptops / PC's that are password protected by individual users.
   II. Physical security is maintained on a 24X7 basis via Security personnel and CCTV cameras installed at strategic locations.
   III. Routine checkup and regular maintenance carried out for the hardware's by Central IT team. Calls are logged with IT Helpdesk for hardware / software support.
   IV. Data is stored on the Central server. Backup of data on central server is taken by the Backup team through defined backup policies.
   V. Records of all physical data transfer is maintained.

3. **Provide details on location and physical security of your data center. Is your data center hosted by a 3rd party or is it wholly owned and managed by you?**

   Reliance IDC's Site location is carried out on the basis of following guidelines

   I. Necessities like Electricity, Water, Telephone lines and Networking Infrastructure support is available.
   II. The facility is not located in a flood, earthquake, hurricane, or tornado prone area.
   III. The facility is away from any Nuclear Plants, Military Bases, Embassies and other Government Buildings.
   IV. Facility is closer to emergency services like Police, Fire brigade and Hospitals.

4. **Describe the physical security provided for all TI data that is taken off-site.**

   Reliance IDC maintains a list of the material in the form of Material Movement registers for material which enters into the Reliance IDC premises and moves out of the premises. It is required to be sent only after necessary consent and approvals from appropriate authority of the respective IDC Leads

# Personnel and Training

1. **Do you perform criminal background checks on employees?**

   Yes. Reference checks are carried out

2. **Is contract labor used for administrative duties or application development?**

   No. Administrative duties are handled only by employees. No application development services are rendered to customers

3. **Are your developers and Admins trained in security best practices? Code reviews held?**

   Yes. They are trained on the Security aspects

# Policies

1. **Do you have a documented patch policy for servers?**

   Yes

2. **Do you have a documented customer data handling policy?**

   Yes. Information has varying degrees of sensitivity to the Reliance IDC. The level of security and the types of protective controls and measures used to secure information are depends on the sensitivity of information. Certain information needs an additional level of protection due to its criticality.
   In Reliance IDC one of the fundamental principles of information security is the "need to know" and "least privilege". This principle holds that information should be disclosed only to those people who have a legitimate business need for the information. The data classification scheme has been designed to support the "need to know" policy so that information will be protected from unauthorized disclosure, use, modification, and deletion. Data classification is followed for handling customer data

3. **Do you have a documented customer data classification policy?**

   Yes. Classification Levels are as below:

   i. **CONFIDENTIAL**

      CONFIDENTIAL information is that which is to be shared only with a very limited group and the unauthorized disclosure of which could be reasonably expected to cause damage to the business or its security.

   ii. **PRIVATE**

      While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impact IDC its employees / customers, business partners can be classified as PRIVATE.

iii. **INTERNAL**

The information which is generated for/ by Reliance IDC employees and can be shared with Reliance IDC or Reliance ADAG group companies and can be shared or transferred to only identified external customers or any out of Reliance entity is classified as INTERNAL.

iv. **PUBLIC**

By definition, there is no such thing as unauthorized disclosure of this information and it may be freely disseminated without potential harm.

4. **Do you have a documented customer data destruction policy?**

I. For media like floppy and CDs are broken.
II. For Hard Disk and Tape storage media, the media is formatted before leaving the Reliance IDC.
III. For equipment like switches, routers, firewall etc. all the configuration files are deleted, and the device is set to factory default condition.
IV. For decommissioned servers hard disk drives are formatted prior to sending the server to the stores.
V. Any PC leaving the IDC premises, the user of the PC formats the hard disk drive before handing over the PC to the Central IT.

5. **What is the process for notification of customers in case of a security breach? How/When?**

It is done via email by IDC Tech desk. An incident case is generated by IDC Tech desk and notification is sent to the Customer.

## Application Access and Authorization

1. **How do users access the application? Examples: Web access, console, command line interface**

Not Applicable - Services not Managed by IDC

2. **What authentication is used for client access to application? Are you compatible with Federated ID SAML 2.0 standards?**

Complexity enabled Password

3. **Describe the various roles assigned in the application to TI users. For example, some roles might include: Data Entry, Data Review, Approval, User Management, Data Correction, Super User, IT Support, and Administrator**

There are 3 types of Access for the users:

I. Administrative/Super user Rights
II. Normal User Rights,
III. Read only

4. **Does the application have an administrator or other privileged account that may have permissions greater than those of the typical user?**

   Yes. There is an Administrative/Super user Right

5. **Do administrators use named credentials when accessing systems or use root/administrator?**

   Named credentials are used for accessing the systems

6. **Are administrative activities logged and archived?**

   Yes

7. **Is system access logged? If so, please note the current retention period of system access logs. As part of an investigation would TI be allowed to access these logs?**

   Administrative activities are logged but not archived. Logs will be overwritten once it reaches 20 MB size limit, Any Change on system will be carried out with service request raised by customer or by IDC.

8. **Are any additional application and server logs archived? How long are they retained? As part of an investigation would TI be allowed to access these logs?**

   Incident logs are retained for 3 months for investigation purpose. In case of incidents, the logs may be shared with TI

9. **Does the application lock an account after repeated failed login attempts?**

   System User Accounts will be locked after 3 invalid attempts & will be unlocked after 30 Minutes of time

## Separation of Duties

1. **Do any business processes supported by this application require "Separation of Duties (SoD)" or other safeguards to prevent a single user from abusing the system**?

   There is a "Segregation of duties" logic followed. Accesses to systems and applications are given only as per the role requirement

2. **Have the roles and assignments been reviewed to ensure SoD conflicts do not exist?**

   Yes.

## Account Provisioning

1. **Who provides new users with access to the system?**

   As customer & IDC both have Administrative privileges we both can create/provide.

2. **Who provides existing users escalated privileges if needed?**

   As customer & IDC both have Administrative privileges we both can create/provide.

3. **How are users removed from the system after termination or job change?**

   As customer & IDC both have Administrative privileges we both can create/provide.

4. **Are there established approval and review processes for the above? If so, please describe.**

   IDC create users only if we receive request from customer to do so.

## Password Compliance

1. **Are account passwords maintained in accordance with a Security Policy governing complexity rules, length, expiration, etc.? If so, please provide details.**

   Yes. All infra servers are supposed to be aligned with the following password management controls:

   I. Maximum Password age - 60 days
   II. Account lockout threshold - 5 attempts
   III. Complex password

## Data Approval

1. **Is someone responsible for reviewing and/or approving the output of this application? If so, please identify the responsible individual(s) and describe the review process**

   I. User access right review responsibility is assigned to the asset owners and they are instructed to review the current access rights verses valid access request forms every month.
   II. Asset owners disable the unwanted or expired user accounts if account holders do not reply after expiry date intimation mail.
   III. Whenever any employee resigns the job or gets transferred to other departments, the respective department head sends e-mail to all asset owners to disable his/her user accounts.

# OTHER INFORMATION

Our Web servers may automatically procure certain general non-personal information from your computer. This information includes your IP address. Our Web-server automatically recognizes each visitor's domain name or IP address, wherever possible. In addition, it may collect your browser type and operating system. However, it would not collect the visitor's email address.

While it is not its practice to link IP addresses to your personally identifiable information, Berggruen reserves the right to use IP addresses to identify a user when it is felt that it necessary to protect the compelling interests of

Berggruen, our website, customers or others, or to comply with laws, court orders, or laws enforcement requests.

**1. HOW IS THE INFORMATION TO BE USED?**

Berggruen uses the information collected for the following purposes:

- To assist you with reserving, renting, purchasing and leasing motor vehicles;
- To provide information concerning car sales, ride- sharing and fleet management;
- To conduct other transactions that you request;
- To operate and improve the website, services and offerings available through this website;
- To personalize the content and advertisements provided to you;
- To fulfill your requests for products, programs and services;
- To communicate with you and respond to you inquires;
- To conduct research about your use of this website; and
- To help offer you other products, programs, or services that may be of interest.

Your personally identifiable information will not be shared with third parties unless it is necessary to fulfill a transaction you have requested, in other circumstances in which you have consented to the sharing of your personally identifiable information, or except as described in this Policy. Berggruen may use your personally identifiable information to present offers to you on behalf of business partners and advertisers.

Data collected online may also be merged and combined with information you provide to us by means other than through this website as part of the standard business operations of Berggruen, provided, however, this Policy applies only to data collected online. If the same information about you is gathered from this website and also from other sources with different privacy policies, Berggruen may elect, in its sole discretion, to treat such information in accordance with the privacy policy that least restricts our use and disclosure of such information.

## USAGE OF COOKIES

From time to time, information may be placed on your computer to improve this site and Berggruen's services for you. This information is commonly known as "cookies" and many web sites use them. Cookies are pieces of data stored on your computer's hard drive or browser, and not on this website. They typically enable collection of certain information about your computer, including your internet protocol address, your computer's operating system, your browser type and the address of any referring sites.

The use of cookies provides benefits to you, such as eliminating the need for you to enter your password frequently during a session, or where applicable re-enter items you place in a shopping cart from visit to visit if you do not finish a transaction on an earlier visit. By showing how and when our visitors use this site or other Berggruen sites, the use of cookies allows Berggruen to continue to improve them. If you do not wish to receive cookies, or want to be notified of when they are placed, you may set your web browser to do so, if your browser so permits. Please understand that if cookies are turned off, you may not be able to view certain parts of this site that may enhance your visit. Some of our business partners whose content is linked to or from this site may also use cookies. However, we have no access to or control over these cookies.

## WITH WHOM THE INFORMATION MAY BE SHARED

Berggruen cannot ensure that all of your private communications and other personally identifiable information will never be disclosed in ways not otherwise described in this Privacy Policy.

By way of example (without limiting the foregoing), Berggruen may be required to disclose information to the government or third parties under certain circumstances, or third parties may unlawfully intercept or access transmissions or private communications.

Berggruen can (and you authorize us to) disclose any information about you to governmental and legal authorities as it, in its sole discretion, believes necessary or appropriate, in connection with an investigation of fraud, intellectual property infringements, or other activity that is illegal or may expose us to legal liability.

Therefore, although Berggruen uses industry standard practices to protect your privacy, Berggruen does not promise, and you should not expect, that your personally identifiable information or private communications would remain private. As a general proposition, Berggruen does not sell or rent any personally identifiable information about you to any third party.

In the event that ownership of Berggruen was to change as a result of a merger, acquisition or transfer to another company, your personally identifiable information may be transferred.

Berggruen will share much of our data, including personally identifiable information about you, with its subsidiaries and other websites so that you gain greater value addition from the services and information provided by them. To the extent that these entities are getting access to your information, they will treat it at least as protectively as they treat information they obtain from their other users.

## USAGE OF SUBCONTRACTORS

Berggruen may use subcontractors to provide some products or services to you. Berggruen also may need to share your personal data with these subcontractors so that they can provide services to it. Berggruen's subcontractors are not allowed to use such personal data for any other purposes and Berggruen imposes confidentiality requirements on their services.

## EXTERNAL LINKS

This site may contain links to other sites. Please note that Berggruen is not responsible for the privacy practices or contents of any other sites. Berggruen recommends that you read the privacy policies of such sites.

## CHOICES YOU CAN MAKE ABOUT YOUR INFORMATION

Berggruen gives you a number of choices about the collection, use and distribution of your information. For example, you must affirmatively request to receive e-mail from Berggruen and/or business partners concerning information about special offers, promotions and new features, products and services. Every Berggruen e-mail will provide you with the opportunity to remove yourself from the e-mail list.

## ACCURACY OF COLLECTED DATA

Berggruen will on its own initiative or at your request, free of charge, replenish, rectify or erase any incomplete, inaccurate or outdated personal data retained by it in connection with the operation of this site. Please consult the contact information posted below on this page, if any, or elsewhere on this site to determine how best to contact Berggruen to update and/or review your personal data and/or opt-out of receiving marketing communications from Berggruen.

## SECURITY PROVIDED BY BERGGRUEN

Berggruen has established safeguards to help prevent unauthorized access to or misuse of your personally identifiable information, but cannot guarantee that your personally identifiable information will never be disclosed in a manner inconsistent with this Policy (for example, as a result of unauthorized acts by third parties that violate applicable law or the policies of the service and its affiliated providers). To protect your privacy and security, Berggruen uses passwords to help verify your identity before granting access or making corrections to any of your personally identifiable information.

## CHANGE IN TERMS

Berggruen may update this Privacy Policy from time to time, and so you should review this Policy periodically. If there are significant changes to Berggruen's information practices, you will be provided with appropriate online notice. You may be provided other privacy-related information in connection with your use of offerings from Berggruen, as well as for special features and services not described in this Policy that may be introduced in the future.

Except as otherwise expressly discussed in this Privacy Policy, this document only addresses the use and disclosure of information that Berggruen collects from you.