Privacy Policy (PP)

Shine Servers LLP takes great care in handling the personal data of her customers to guarantee customer privacy. Personal data is carefully converted and secured. In this process, we follow the requirements of the so-called European Union General Data Protection Regulation (GDPR) and other laws protecting information about you at our company. To know more please carefully read this Privacy Policy.
ShineServers.Com values the privacy and security of the information that you share with us. This Privacy Statement applies to information collected through www.shineservers.com (the "website"). This Privacy Statement also applies to other information Shine Servers receives in the United States from Europe. This Statement describes how Shine Servers collects, uses, shares, protects, or otherwise processes your personal information. **By using this website, you agree to the terms of this Privacy Statement.**

Collection and Use of Information

Shine Servers LLP collects personal information to set up and manage accounts for our ecommerce services and to handle orders of goods and services from Shine Servers LLP.

You may need to provide Shine Servers LLP with personal information such as:

names; phone numbers; mailing, billing, shipping, and email addresses;
bank account information; credit and debit card information; dates of birth; and identification documents.

- Shine Servers LLP uses such information for sending server details, contacting customer if necessary, processing payments and refunds;
- Providing customer service; providing dispute resolution, chargebacks, refunds, or related issues;
- Marketing and surveys; sending service update notices;
- Recovering debt and collections; detecting and preventing fraud; detecting and preventing violations of our legal agreements;
- Measuring, improving, and customizing our services; and
- Fulfilling other technical, logistical, financial, tax, legal, compliance, administrative, or back office functions.

Shine Servers LLP may also collect background information and credit checks from third parties to verify your identity; deter, detect, and prevent fraud and illegal activity; make business decisions; and as a part of our legal obligations. Shine Servers LLP retains such information for as long as reasonably required for business purposes or as reasonably required to comply with our legal obligations.

Community Information

Shine Servers LLP collects information from you to post entries to our community website or forums. Such information may include your email address, Internet Protocol address, user name, date and time of signup, and date and time of posts to the forum.

Shine Servers LLP uses this information for the secure and efficient functioning of our website, to provide you with access to our community site, to detect and prevent violations of our legal agreements, and as part of any legal obligations related to our community website.

Transaction Information

Shine Servers LLP collects information on each transaction conducted through our website. Such information may include the amount of the transaction; the goods purchased; the identity of the seller, affiliate, and customer; payment type; currency; location; Internet Protocol address; and websites visited.

Shine Servers LLP uses such information for refunds, for customer service, for website optimization, or for other administrative or business purposes. Shine Servers LLP may share information related to the transactions you conduct through our website with sellers, affiliates, or customers for the purposes disclosed in this Privacy Statement. Shine Servers LLP retains transaction information for as long as reasonably required for business purposes or as reasonably required to comply with our legal obligations.

Customer Service Correspondence

Shine Servers LLP also collects information involving customer service correspondence. This information may include emails, internet chats, faxes, or telephone calls directed to our customer service centers. Shine Servers LLP processes this information to provide customer service, handle complaints or disputes, measure and improve our customer service, detect and prevent fraud, and detect and prevent violations of our legal agreements. Shine Servers LLP retains customer service information for as long as reasonably required for business purposes or as reasonably required to comply with our legal obligations.

Google AdWords

Shine Servers LLP uses Google AdWords, a web analytics and search engine advertising campaign management service. Google AdWords uses cookies, web beacons, and other means to help Shine Servers LLP analyze how users use the site. You may find Google's Privacy Statement at http://www.google.com/intl/en/privacypolicy.html.

Google Analytics

Shine Servers LLP uses Google Analytics, a web analytics service. Google Analytics uses cookies, web beacons, and other means to help Shine Servers LLP analyze how users use the site. You may find Google's Privacy Policy at http://www.export.gov/safeharbor/.

Your rights

At any moment you are allowed to request Shine Servers to reveal which personal data is being kept in your customer profile, and if necessary we can correct or delete this. You can send in a ticket or simply by e-mail with the reference of your name and address to our helpdesk at legal@shineservers.com .

Security data

Shine Servers uses security procedures to keep unauthorized people from obtaining access to personal data.

Visiting data

On our website, we keep a general history of the pages that are visited on our site, to know which page(s) are visited most. The purpose of this system is to improve the setup of our website, so Shine Servers can further optimize their services; the information is not used for any other purposes.

Data Processing Agreement

This Data Processing Agreement is an integral part of the agreements between the Customer and SHINE SERVERS LLP. ShineServers.Com is the Processor of the personal data and the Customer is the Controller with regard to the personal data.

1. Purposes of data processing operations

1.1 The Processor commits to processing personal data on the instructions of the Controller, subject to the conditions of this Data Processing Agreement. The data will only be processed for the purpose of storing data of the Controller in the 'cloud', the related online services, colocation and those purposes that can be reasonably associated with it or will be determined by mutual agreement.
1.2 The Controller will decide which types of personal data it requires the Processor to process and therefore also to which (categories of) data subjects the personal data relate. The Processor exerts no influence on this decision. This relates in any case to personal data of customers of the Controller, and staff of the Controller, that are stored by the Customer at the Processor. The Processor will refrain from using the personal data for any purpose other than that determined by the Controller. The Controller will inform the Processor of the purposes of the processing where these are not already stated in this Data Processing Agreement.
1.3 The personal data to be processed on the instruction of the Controller will remain the property of the Controller and/or the data subjects concerned.

2. Obligations of the Processor

2.1 In respect of the processing referred to in Article 1, the Processor will ensure compliance with applicable legislation and regulations, including in any event the legislation and regulations in the field of the protection of personal data, such as the General Data Protection Regulation.
2.2 The Processor will inform the Controller, upon the latter's first request, of the measures it has taken to meet its obligations under this Data Processing Agreement.
2.3 The Processor's obligations arising from this Data Processing Agreement also apply to any party processing personal data under the authority of the Processor, including, but not confined to, employees, in the broadest sense.
2.4 The Processor will notify the Controller if it feels that an instruction provided by the Controller violates the legislation referred to in paragraph 1.

3. Transfer of personal data

3.1 The Processor is allowed to process the personal data in European Union member states. In addition, the Processor is allowed to transfer the personal data to a country outside the European Union, provided the Processor ensures an adequate level of protection and it complies with the other obligations to which it is subject pursuant to this Data Processing Agreement and the General Data Protection Regulation.
3.2 Upon request, the Processor will inform the Controller of the country or countries involved.
3.3 In particular, the Processor will, in determining an adequate level of protection, take account of the duration of the intended processing, the country of origin and the country of final destination, the general and sectorial rules of law that apply in the country concerned, as well as the professional rules and the security measures complied with in those countries.

4. Division of responsibility

It is preferable that a report is only made once it is likely that the notifier and the content provider will be unable to reach an agreement. The notifier is responsible for ensuring reports are correct and complete.
4.1 The Processor will make ICT means available for the processing that can be used by the Controller for the purposes stated above. The Processor will itself only perform processing on the basis of separate agreements.
4.2 The Processor is solely responsible for the processing of the personal data under this Data Processing Agreement, in accordance with the instructions of the Controller and under the express (ultimate) responsibility of the Controller. The Processor is expressly not responsible for any other processing operations involving personal data, including in any event, but not confined to, the collection of personal data by the Controller, processing for purposes that the Controller has not notified to the Processor and processing by third parties and/or for other purposes.:
4.3 The Controller warrants that the content, the use and the instructions for the processing of personal data as referred to in the Agreement are not unlawful and do not infringe any third-party right.

5. Engagement of third parties or sub-contractors (sub-processors)

5.1 The Processor engages third parties, which are available on request and for which the Controller hereby provides authorisation. In the case of new third parties, the Processor will inform the Controller thereof. If the Controller has well-founded objections to the engagement of the third party, a suitable solution must be sought in consultation. If the parties are unable to reach a suitable solution, the Controller may give notice to terminate the Agreement if the use of a specific third party of which it has been notified is unacceptable to it.
5.2 The Processor will in any case ensure that these third parties assume similar obligations in writing as those agreed between the Controller and Processor.
5.3 The Processor warrants correct compliance with the obligations in this Data Processing Agreement by such third parties and, in the event of errors committed by such third parties, is liable itself for any and all damage or loss as if it had committed the error(s) itself.

6. Security

6.1 The Processor will endeavour to take sufficient technical and organisational measures against loss or any form of unlawful processing (such as unauthorised disclosure, interference, alteration or provision of personal data) in connection with the processing of personal data to be performed.
6.2 The Processor does not guarantee that the security is effective in all circumstances. If the Agreement does not include explicitly defined security, the Processor will endeavour to ensure that the security provided shall meet a standard that is not unreasonable, taking into account the state of the art, the sensitivity of the personal data and the costs associated with implementing the security measures.

7. Notification obligation

7.1 The Controller is at all times responsible for reporting data leaks (which includes a breach of the security of personal data that leads to a risk of negative consequences, or has negative consequences, for the protection of personal data) to the supervisory authority and/or data subjects. In order to enable the Controller to meet this legal obligation, the Processor must inform the Controller without delay of a data leak after it has detected one and if the leak relates to the personal data that are processed by the Processor on behalf of the Controller.
7.2 The notification obligation shall in any case include reporting that a leak has occurred, as well as:

- the supposed or known cause of the leak;
- the consequences (that are currently known and/or are to be expected);
- the solution or proposed solution.

8. Handling requests from data subjects

In the event that a data subject submits a request to exercise their statutory right of inspection or their statutory right to improvement, addition, amendment, blocking, erasure of data or data portability to the Processor, the Processor shall forward the request to the Controller and the Controller will handle the request. The Processor may inform the data subject about this.

9. Privacy and confidentiality

9.1 All personal data the Processor receives from the Controller and/or collects itself within the framework of this Data Processing Agreement is subject to a duty of confidentiality towards third parties. The Processor will not use this information for any purpose other than that for which it was provided.
9.2 This duty of confidentiality does not apply insofar as the Controller has expressly granted permission to provide the information to third parties, if providing the information to third parties is logically required in view of the nature of the work assigned and the performance of this Data Processing Agreement or if there is a statutory obligation to provide the information to a third party.

10. Audit

10.1 The Controller may have an audit conducted at the Processor by an independent 'Register EDP Auditor' who is bound by a duty of confidentiality in order to verify compliance with the agreements under this Data Processing Agreement concerning the protection of the personal data processed by the Processor on behalf of the Controller.
10.2 This audit will only take place where there is a specific and well-founded suspicion of misuse of personal data, and only after the Controller has requested and assessed similar existing reports from the Processor, and has made reasonable arguments to justify an audit being initiated by the Controller. Such an audit is justified if the similar reports that the Processor has available provide an insufficient or inconclusive answer regarding compliance with this Data Processing Agreement by the Processor. The Controller will notify the Processor of the audit in advance, giving at least two weeks' notice.
10.3 The Parties will jointly assess the findings of the audit that has been conducted and will determine on that basis whether or not those findings will be implemented by one of the Parties or by both Parties jointly.
10.4 Insofar as possible and reasonable, the Processor will cooperate with the Controller in carrying out a data protection impact assessment.
10.5 The costs of the audit described in paragraphs 1 and 4 above will be borne by the Controller.

11. Duration and termination

11.1 This Data Processing Agreement will enter into effect once it has been signed by the Parties, on the date of the second signature.
11.2 This Data Processing Agreement has been entered into for the term specified in the Agreement between the Parties, in the absence of which it will at least apply for the duration of the collaboration.
11.3 Upon termination of the services by the Processor, the Controller is itself responsible for making copies of, exporting or otherwise returning, in good time, the personal data that the Processor processes on behalf of the Controller. After the end of the term of the Agreement, the Processor will remove or destroy the (personal) data of the Controller.
11.4 The Processor is entitled to revise this agreement from time to time. It will inform the Controller of the changes at least three (3) months in advance. The Controller may lodge a notice of objection by the end of these three (3) months if it does not agree to the changes. If the Processor does not receive a notice of objection within this period, the changes will be deemed to have been accepted by the Controller.

12. Applicable law and settlement of disputes

12.1 The Data Processing Agreement and its execution are governed by Dutch law.
12.2 Any disputes that may arise between the Parties in connection with the Data Processing Agreement will be submitted to the competent court in Rotterdam.

Modifications

Shine Servers has the right to make changes to this Privacy Statement. Therefore, please check this page regularly. If you have any questions, please contact us.

This document was last revised: May 25, 2018 at 03:59AM GMT.