PRIVACY POLICY OF AN ONLINE SERVICE

RENDERBUZZ.COM

§ 1 General provisions

1. Definitions. What do the terms used in this document mean?

As used in this Policy, the following terms shall have the meanings set forth below:

a. **Client** – a person who registers for the Service and creates an account in order to use offered services;

b. **GDPR** - the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

c. **Service** – the website under domain www.renderbuzz.com;

d. **User** – each person browsing the web pages of the Service, also those who do not intend to register for it or use offered services;

2. Who is the Data Controller? Who handles your personal data?

The Data Controller of the data collected by the means of the Service **Monika Kopczyńska 3DMEDIA limited partnership** with registered seat in Bąblinek (64-607 Kiszewo), ul. Bąblinek 4A, KRS (National Court Register number= 0000452857 (Court: Sąd Rejonowy Poznań-Nowe Miasto i Wilda w Poznaniu, IX Wydział Gospodarczy), NIP (tax identification number) 6060092150, REGON (National Official Business Register) 302369020, email address: support@renderbuzz.com – hereafter referred to as **Controller.**

3. What legal regulations do we apply regarding processing your data?

Personal data of Client and User shall be processed according to the GDPR and state regulations of common law concerning personal data protection, as well as the act on Providing Services by Electronic Means of July 18th 2002 (Journal of Laws 2002 No 144, item 1204 with later amendments).

4. What principles do we observe while processing your data?

Controller shall exercise due diligence to protect the interest of persons whom the data concerns, and in particular to ensure that the data is:

a. processed lawfully, fairly and in a transparent manner in relation to the data subject („lawfulness, fairness and transparency");
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes („purpose limitation");
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed („data minimization");
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay („accuracy");
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed („storage limitation");

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures („integrity and confidentiality").

5. Personal Data Protection Inspector

The Controller did not appoint a Personal Data Protection Inspector.

§ 2 The manner of data collection on the website.

1. Data collection by the means of forms in Service

Personal data OF Clients are collected in Service when they are freely provided during registration of an account or any update of the data at a later time. The extent of personal data, divided into mandatory and non-mandatory data is presented in the table below:

Mandatory data	Non-mandatory data
- username (of the account) - first name - last name - name of the company - primary address - city - post code - country	- phone number - secondary address - tax identification number (NIP) - other additional data provided by Client (Clients may freely provide additional information)

Providing mandatory data is necessary to gaining access to services offered in the Service. There is no legal obligation to provide the data, however refusal to give consent to do so entails lack of access to the services.

Client may (but does not have to) provide non-mandatory data for easier communication (phone number, secondary address) or in order to enable issuing a VAT invoice (tax identification number). Such data should only be provided if Client consents to this data being processed for those purposes.

2. Collecting data from Cookies files

Information on Users and Clients are also collected through cookies files stored on devices used by Clients and Users. Detailed information is included in §5.

§ 3 Information on the extent of personal data processing

1. What data, for what purposes and on what legal basis will be processed?

Information on the type of collected data of Clients and Users, purposes for what it will be processed and legal basis is summarized in the table below:

Type of data	**The purposes of the processing**	**Legal basis**
Username (of the account) first name last name name of the	Preparing contracts of providing rendering services and taking steps at the request of the data subject prior to entering into a contract such as: - establishing and maintaining an account in	Article 6 section 1 letter b GDPR (Performance of a contract)

company primary address city Post code country Tax identification number	Service used to purchase points, order services and communicate with Controller; - providing services; - complaint handling; - issuing bills.	
	Fulfilling legal obligations, including tax ones, imposed on Controller.	Article 6 section 1 letter c GDPR (Legal obligation)
	Investigation, defense or recognition of claims.	Article 6 section 1 lit f GDPR (The legitimate interest of the Controller).
Phone number Secondary address	Establishing easy communication with Client in matters related to performance of contracts of performing rendering services.	Article 6 section 1 letter a GDPR (Consent)
Email address	Direct marketing in the form of sending trade information.	Article 6 section 1 letter a GDPR (Consent)
All data stored in the computer system of Controller	Making and storing backup copies, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.	Article 32 section 1 point b) and c) GDPR

2. Recipients of the data – who apart from the Controller may have access to your data?

Personal data of Users and Clients may be made available to the following types of recipients:

a. payment intermediaries;
b. providers of cloud-based software systems (SaaS) used by Controller;
c. providers of IT or programming services, webpage maintenance services, as well as services, tools and scripts used in Service;
d. subcontractors;
e. Google Inc. (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA) – within the extent of the Google Analytics service;
f. Entities authorized by the law (courts, public prosecutor, police, tax office).

3. For how long will your data be processed?

Personal data of Users and Clients shall be processed for the period necessary to complete a given purpose, including:

a. until limitation periods of claims arising from conclude contracts expire – in the case of data processing for the purpose of performing contracts, investigation or defense of claims;
b. until the end of the period of storing tax documentation required by the law;
c. until User exercises the right to exclude their personal data from processing for the purposes of direct marketing, including the moment of expressing objection or withdrawing consent – in the case of processing for marketing purposes.

4. How can you influence the extent of processing of your data?

User and Client can influence the purpose, extent and recipients of the data processed by Controller, in particular by the means of providing or refusing to provide data, which is not mandatory in forms in Service.

5. Information on transferring data to third countries (outside the EU and EEA)

Personal data of Users and Clients may be transferred to a third country – The United States of America, due to the fact that Controller uses services provided by Google Inc. (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA).

The transfer is carried out under the decision of the European Commission (so called Privacy Shield) which provides that companies with registered offices in the United States of America, which joined the Privacy Shield program have an adequate level of personal data security. You have the right to obtain a copy of your personal data transferred to the third country.

§ 4 Rights of data subjects

1. What rights do you have in regard to processing your personal data?

Each person whose personal data is processed by Controller has rights summarized in the table below and in further provisions of this Policy.

Right of access	Article 15 GDPR. The essence of the law: The data subject shall have the right to obtain from the Controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and information listed in the document.
Right to rectification	Article 16 GDPR The essence of the law: The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
Right to erasure	Article 17 GDPR The essence of the law: The data subject shall have the right to obtain from the Controller the erasure of personal data concerning him or her without undue delay and the Controller shall have the obligation to erase personal data without undue delay where one of the grounds listed in the regulation applies.
Right to restriction of processing	Article 18 GDPR The essence of the law: Restriction of processing means marking stored personal data in order to limit its processing in the future. After data has been marked like this, processing it, apart from storing, may happen inly based on consent or for purposes specified by the regulation. Restriction can be demanded in cases specified in the regulation.

Right to data portability	Article 20 GDPR The essence of the law: The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another Controller without hindrance from the controller to which the personal data have been provided.

2. Right to withdraw consent

If Controller processes personal data of User or Client based on consent, it can be withdrawn at any time, regardless of the legitimacy of data processing before the consent has been withdrawn.

3. Right to object to processing data for marketing purposes

If Controller intents to process or processes personal data for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, including profiling.

Controller does not process personal data of Users and Clients for marketing purposes, apart from short notices sent to Clients' email address, if Clients expressed consent to such action. Controller does not store data for profiling purposes, namely to creating profiles of Users or Clients in order to adjust personalized offers.

4. How can you exercise the abovementioned rights?

In order to exercise the rights described above, one may contact Controller through traditional or electronic mail using Controller's contact data included at the beginning of this Policy.

5. Right to make a complaint to data protection supervisory authorities

In the case of personal data being processed unlawfully, User and Client may make a complaint to the General Inspector for Personal Data Protection (GIODO) (the position shall be renamed as the Head of the Personal Data Protection Office).

§ 5 Cookies and performance data

1. Cookie files are small fragments of text information stored as text files saved on hard drives of PCs, laptops or the memory of a smartphone or other device used for browsing the Web. More information on what Cookie files are can be found e.g. here: https://en.wikipedia.org/wiki/HTTP_cookie.

2. Controller may process data stored in Cookie files while Users use Service for the following purposes:

a. identifying logged Users and indicating they are logged in;
b. remembering login details to Service;
c. adjusting the Service content to individual preferences of Users (e.g. displayed colors, text size, layout) and optimization of using Service;
d. conducting anonymous statistical analysis on the usage of Service.

3. Most Web browsers on the market accepts saving cookie files as standard procedure. Each user may specify the conditions of using Cookie files in the settings of their Web browser. It

means that saving Cookie files can be e.g. partially (e.g. temporarily) or fully disabled – in the latter situation, however, it may influence some functionalities of the Service.

4. Web browser settings concerning Cookie files is very important in terms of consent to Cookie files being used by Service. According to the law such consent may be also given through browser settings. In case of the lack of such consent Web browser Cookie files settings should be adjusted accordingly.

5. Detailed information on changing Cookie files settings and deleting them manually in most popular browsers are available in help sections of the browsers and in articles linked below (click on the relevant link):

- in Chrome browser
- in Firefox browser
- in Internet Explorer browser
- in Opera browser
- in Safari browser

6. Controller processes also anonymized performance data relevant to the use of Service (IP address, domain) for statistical purposes, facilitating Service administration. This data is collective and anonymous, so it does not contain information identifying individual Users.

§ 6 Final provisions

1. Service may contain links to external websites administered by entities other than Controller. It is recommended to familiarize oneself with privacy policies of each such visited website.

2. Controller uses technical or organizational measures ensuring protection of processed data adequate to existing threats and category of data under protection, and in particular protects it from becoming available to unauthorized persons, processing in breach of the law, as well as modification, loss or damage.

3. Controller provides adequate technical or organizational measures preventing unauthorized persons from obtaining and modifying personal data sent via email. This includes protecting the collected data from unauthorized access and only allows access to Account after providing valid login and password.