DDOS-GUARD

IQWeb FZ-LLC
DDoS Protection Company

Privacy policy

Table of contents

Revision date and effective date – 15.02.2024

1. General terms

1.1. This Privacy Policy (hereinafter – as the "Privacy Policy") of IQWeb FZ-LLC (hereinafter — as the «Provider») describes how the Provider processes the personal data of the Clients or website users (hereinafter — as the "Data subject").

1.2. By using the Servises or the website of the Provider, the Data subject agrees unconditionaly with the terms of this Privacy Policy.

1.3. This Privacy Policy is an integral part of the Service Level Agreement avaliable at – https://ddos-guard.net/file/sladdg_en.pdf.

2. Processing purposes

2.1. The Provider assembles the personal data for the following purposes:

- conclusion and provision of the contract between the Data subject and the Provider;
- provision the access to the website
- provision of the access to the Client area;
- provision of the Services;
- provision the answers to the requests about the services and other information;
- Improvement of the website and the Services;
- marketing and informational purposes.

2.2. The the sourses of personal data and the ways of its usage:

How can it be used?	What is processing?
Provision information about the Provider, the Services information and news materials; providing answers to requests; participation of the data subject in contests and events held by the Provider; for conducting advertising and marketing campaigns and research	Data that is filled in in electronic forms, including surname, first name, e-mail address, contact phone number, data contained in attached documents.
Conclusion or/and provision of contract between the data subject and the	Personal data that the Data subjects provides when registering the Client

Provider, including the creation of the Client Area Account and identification at the entrance to it, communication, sending notifications, settlement of payments in the performance of contractual obligations; to account for concluded contracts.	Area Account, such as last name, first name, phone number, email address, address (country) of location, internal identifiers of services, expiration date of the bank card and other payment information required for payment, data obtained during authorization in Client Area via third-party platforms (for example, ID-number and other data provided by a third-party service), IP-address and other log-data, technical data and cookie information, data that is transmitted by the device with which the data subject is logged into the Client Area; information provided by the data subject in requests
Improving the quality of the Provider's website and the Client Area (including accounting for statistics of its visits); to assist the data subject with the Provider's website; to evaluate the effectiveness of marketing campaigns.	Technical data and information of cookies, data that is transmitted by the device with which the data subject enters the Provider's website or Personal Account

2.3. The Data subject is obliged to enter his own correct data and is independently responsible for their accuracy.

2.4. If the Data subject is not an adult or other legal requirements are imposed on his consent, consent must be given in accordance with the procedure established by law. The use of the Provider's website, Personal Account or the Provider's services/services in the absence of such consent is prohibited.

2.5. The Provider processes personal data (collection, systematization, buffering, storing, refining (updating, change), blocking, personal data termination).

2.6. The Data subject is not allowed to indicate the personal data of third parties on the Provider's website. The Data subject is responsible for the data fidelity he/she provides.

2.7 The Provider does not collect or process any special categories such as: biometric data, information about political or religious beliefs, previous convictions, health condition, or other similar information.

2.8. All credit/debit card details and personal identifiable information will NOT be stored, sold, rented or leased to any third parties.

2.9. The Provider website uses cookie data. Cookie are used to improve the Provider website (for example, to authenticate the website user, statistics on website visits, keeping website user preferences) Cookie Policy is available at https://ddos-guard.net/file/cookie_en.pdf. Note that the Data subject can disable cookie in his/her browser settings at any time.

2.10. The website and the Client area may contain links to other websites. The Provider is not responsible for this services and encourages the Data Subject to read the privacy policy and terms of use of any linked websites, as their policies may differ from this Privacy Policy.

3. Personal data transfer

3.1. The Provider can use personal data to fulfill obligations to the Data subject described in clause 2.2. of the Agreement.

3.2. The Provider does not distribute or disclose personal data to third parties without obtaining the confirmation of the Data subject or in cases where such obligation is explicitly stated by law or is aimed at meeting obligations under the agreement with the Data subject, does not place personal data in publicly available sources.

3.3. The Provider has the right to provide the processed personal data to the third parties when it is necessary to fullfil the obligations with the Data subject.

Such third parties receive the strictly limited data, for example, that is needed to the provision of Services. Provider takes possible measures to guarantee confidentiality of data transfer.

The third parties may include:

1) Service providers if it is necessary to peform a contract;
2) Affiliated companies of the Provider (for example DDOS-GUARD LLC located in Russian Federation);
3) Web analytics partners: Yandex.Metrika, Google Analytics, JivoChat, Firebase Google, Tune, Amplitude, Segmento.

3.4. In the case of entrusting personal data processing to a third party, the processing is carried out after the conclusion of an agreement between the Provider and the third party. Such party must observe the principles and rules of personal data processing set by the applicable legislation regarding personal data protection.

At this time, the Provider’s commit determines the actions (operations) with personal data to be performed by such a third-party and the purpose of personal data processing. It is establishing the obligation of the Party to comply with the

confidentiality of personal data during its processing and the responsibility to meet the requirements for the protection of processed personal data.

3.5 Personal data may be transferred to, and stored at, a destination outside the European Economic Area (”EEA”), to the countries that dont provide the sane level of data protection as EEA if cross-border transfer is necessary for the performance of the contract to which the Data subject is a party. By submitting personal data, the Data subject acknowledges that his/her personal data may be transferred outside of the EEA. In accordance with the clauses 45-49 of the GDPR, the Data subject located in the European Union it is informed about the possible risks of such transfer of personal data in connection with other data protection standards established by laws on the territory of other countries. Prior to such consent, the Data subject must also be informed that without his/her consent, the Provider will not be able to provide the Service.

4. Period of storing and termination

4.1. Personal data of the Data subject shall be stored until the objectives of personal data processing are achieved unless a different period is required by the law.

4.2. Processing of personal data ends when:

- achieving the purpose of personal data processing;
- in the case of withdrawal of consent to personal data processing, if there are no other grounds for personal data processing provided for by the apllicable legislation;
- expiration of the consent to personal data processing or, in other cases, provided for by law.

4.3. Personal data shall be terminated after the extinction of contractual relations and the performing of all responsibilities assumed by the Parties, in the absence of other grounds for personal data processing.

4.4. The Provider is taking the necessary steps to terminate or anonymize expired data.

5. Client's rights

5.1. The Data subject has the right to:

- receive information regarding to his/her personal data;
- the right to withdraw this consent at any time;
- request correction of his/her personal data;
- the right to request block or termination (if the data was obtained illegally or the purpose of processing has come to its end) of personal data and other rights due to applicable legislation.

5.2. The Data subject has the right to withdraw the consent given by him/her by sending a relevant notification to the Provider. The Data subject agrees that when the specified personal data is necessary for rendering services, rendering services and contractual relations between the Parties will be considered terminated from the moment of consent withdrawal for personal data processing.

5.3. The Data subject has the right to unsubscribe from newsletters regarding the provision of services or news items under the agreement on the provision of services by and clicking the «unsubscribe from the newsletter» .

6. Personal data protection

6.1. Measures to protect technical means exclude unauthorized access to stationary IT equipment that process personal data, the means that ensure the functioning of the information system and the premises in which they permanently located, the protection of technical means from external influences, as well as the protection of personal data in the form of informative electrical signals and physical fields.

6.2. Measures to supervise (analyze) the security of personal data ensure the control of the personal data security level by conducting methodical steps to investigate the security of information system and test the personal data system protection performance. Security event logging allows to collect, record, store and protect information on security events in the data system and the ability to view and analyze information about such events and respond to them.

6.3. The Provider employees, under their authority, are allowed to work with personal data, to sign a non-disclosure obligation of confidential information.

6.4. The Information Security Department monitors and supervises personal data processing.

6.5. All disputes arising from this Agreement shall be resolved by following applicable law. Before bringing the court action, the r must comply with the mandatory pre-trial procedure and send the operator a corresponding complaint in writing. The deadline for responding to the complaint is 30 (thirty) business days.

6.6. All other issues not regulated in this Agreement are regulated by the current legislation of the United Arab Emirates and the FZE «Dubai Internet City».

6.7. Any purchase, dispute or claim arising out of or in connection with this website shall be governed and construed in accordance with the laws of UAE.

7. Policy changes

7.1. The Personal Data Processing Policy may be changed or updated occasionally to meet the requirements and standarts. The data of the new version is set in the term "Revision date and effective date".

7.2.Therefore, the Data subject is encouraged to frequently visit these sections in order to be updated about the changes. New version replace the old one, and will be effective on the day it is posted.

7.3. If Data subject, who already uses the Services and/or the Provider's website, will continue to use the Services or the website after the changes of the new version, that means that he/she agrees with the changes.

7.4. The current version of the Policy is available at the following address on the Internet: https://ddos-guard.net/file/PP_ru.pdf.

8. Contact details

8.1. If you have any questions on the performance of this Personal Data Processing Policy, please get in touch with us at the following contact information:

- mailing address: Office No 122, dic Building 03, Al Sufouh second, Dubai;
- e-mail: finance@iqweb.io.

The minimum response period to requests is 1 month.