DDOS-GUARD

Privacy Policy

IQWeb FZ-LLC

IQWeb FZ-LLC is a legal entity and managing company operating under well-known brand name DDoS-Guard

+55 613 550-74-40
+31 970 1028-0960
+971 58 506-81-27

sales@ddos-guard.net

Table of contents

1. General Terms

Revision Date and Effective Date — 31.01.2025

1.1. This Privacy Policy of IQWeb FZ-LLC (hereinafter referred to as the "Provider") describes how the Provider processes the personal data of the Clients or website users (hereinafter referred to as the "Data Subject").

1.2. By using the Services or the website of the Provider, the Data Subject agrees unconditionaly to the terms of this Privacy Policy.

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

2. Processing Purposes

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

- Concluding and fulfilling the contract between the Data Subject and the Provider;
- Providing access to the website;
- Providing access to the Client area;
- Providing the Services;
- Providing consultation about the services and other information;
- Improving the website and the Services;
- Marketing and information purposes.

2.2. The sourses of personal data and ways of its use:

Purposes	Data
Providing information about the Provider, the Services, informational and news materials, providing answers to requests; participation of the Data Subject in contests and events held by the Provider; conducting advertising and marketing campaigns and research.	Data filled in the website forms, including surname, first name, email address, contact phone number, data in the attached documents.
Concluding and/or fulfilling the contract between the data subject and the Provider, including the creation of the Client Area Account and access credentials, communicating, sending notifications, handling payments in fulfillment of contractual obligations; storing concluded contracts.	Personal data that the Data Subject provides when registering the Client Area Account, such as last name, first name, phone number, email address, address (country) of location, internal identifiers of the services, expiration date of the bank card and other payment information required for payment, any data obtained during authorization in Client Area via third-party platforms (e.g., 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 from which the Data Subject accesses the Client Area; information provided by the Data Subject in requests for the Services.
Improving the quality of the Provider's website and the Client Area (including gathering statistics of the visits); assisting the Data Subject with the Provider's website; evaluating the effectiveness of marketing campaigns.	Technical data and cookie information, data that is transmitted by the device from which the Data Subject accesses the Provider's website or the Client Area.

2.3. The Data Subject is obliged to enter their real and correct information and is solely responsible for its accuracy.

2.4. If the Data Subject is not an adult or if other legal requirements are imposed on their consent, the consent must be given in accordance with the procedure established by law. The use of the Provider's website, Client Area, or the Provider's Services without such consent is prohibited.

2.5. The Provider processes personal data, which includes collecting, systematizing, buffering, storing, refining (updating and modifying), blocking, deleting personal data.

2.6. The Data Subject is not allowed to use the personal data of third parties on the Provider's website. The Data Subject is responsible for the fidelity of the provided data.

2.7. The Provider does not collect or process any sensitive data such as: biometric data, information about political or religious beliefs, criminal record, health, or other similar information.

2.8. All credit/debit card details and personally identifiable information will not be stored, sold, rented or leased to any third party.

2.9. The Provider's website uses cookies. Cookies are used to improve the Provider's website (e.g., to authenticate the website user, to gather statistics on website visits, to keep website user preferences). The Cookie Policy is available at: https://ddos-guard.net/file/cookie_en.pdf. Note that the Data Subject can disable cookies in the 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 these websites and encourages the Data Subject to consult the privacy policy and terms of use of any linked website, as their policies may differ from this Privacy Policy.

3. Transfer of Personal Data

3.1. The Provider may use personal data to fulfill the obligations towards the Data Subject described in clause 2.2. of the Agreement.

3.2. The Provider does not transfer or disclose personal data to third parties without the consent of the Data Subject, uness such obligation is explicitly stated by law or is aimed at meeting obligations under the agreement with the Data Subject. The Provider does not place personal data in publicly available sources.

3.3. The Provider has the right to provide the processed personal data to third parties when itis necessary to fulfill the obligations with the Data Subject.

Such third parties receive the strictly limited data, that is necessary to provide the Services. Provider takes possible precautions to guarantee confidentiality of data transfer.

The third parties may include:

- Other service providers, if it is necessary to perform a contract;
- Affiliated companies of the Provider (namely DDOS-GUARD LLC located in the Russian Federation);
- Web analytics partners: Yandex Metrica, Google Analytics, JivoChat, Google Firebase, 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. The third party must observe the principles and rules of personal data processing set by the applicable legislation regarding the personal data protection.

The agreement determines the actions to be performed by the third party, and the purpose of personal data processing. It is establishing the obligation of the third party to protect the confidentiality of personal data during and after its processing .

3.5 Personal data may be transferred to, and stored at, a destination outside the European Economic Area ("EEA"), in countries that do not provide the same level of data protection as the EEA, if such cross-border transfer is necessary to fulfill the contract with the Data Subject. By submitting personal data, the Data Subject acknowledges that their personal data may be transferred outside the the EEA. In accordance with the clauses 45-49 of the GDPR,

the Data Subject residing in the European Union is informed about the possible risks of such transfer, as different data protection standards may be established by laws on the territory of other countries. The Data Subject must also be informed that without their consent to these terms, the Provider will not be able to provide the Services.

4. Period of Storage and Removal

4.1. Personal data of the Data Subject will be stored until the purposes of personal data processing are achieved, unless a different period is required by law.

4.2. The processing of personal data ends when:

- The purpose of the data processing is achieved;
- The consent to personal data processing is withdrawn, unless other grounds for personal data processing are provided for by the applicable legislation;
- The consent to the personal data processing is expired, or in other cases provided for by law.

4.3. The personal data will be removed after the termination of contractual relations and when all responsibilities assumed by the parties are fulfilled, unless there are other grounds for personal data processing.

4.4. The Provider will take the necessary steps to remove or anonymize expired data.

5. Client's Rights

5.1. The Data Subject has the right to:

- Receive information regarding their personal data;
- Withdraw their consent at any time;
- Request the rectification of their personal data;
- Request blocking or removal of personal data, if the data was obtained illegally or if it is not relevant to the purposes of processing;
- As well as other rights according to the to applicable legislation.

5.2. The Data Subject has the right to withdraw their consent by notifying the Provider. The Data Subject agrees that if the specified personal data was necessary for providing the services, the provision of the services and contractual relations between the parties will be terminated from the moment of consent withdrawal.

5.3. The Data Subject has the right to unsubscribe from emails regarding the provision of services or news items by clicking the "unsubscribe from the newsletter" link .

6. Personal Data Protection

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

6.2. Personal data security monitoring (analysis) measures ensure personal data security level control by performing methodical steps to investigate information system security and test performance of personal data protection system.

Event logging allows collecting, recording, storing and protecting information about information system security events and provides the possibility to view, analyze and respond to such events.

6.3. The Provider employees who, under their authority, are allowed to work with personal data, are to sign a non-disclosure agreement.

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

6.5. All disputes arising from this Privacy Policy shall be resolved in accordance with applicable law. Before filing a lawsuit, a Client must follow the mandatory pre-trial procedure and send the Provider a relevant complaint in writing. The time limit for responding to the complaint is 30 (thirty) business days.

6.6. All other issues not regulated in this Privacy Policy are regulated by the current legislation of the United Arab Emirates and the FZ "Dubai Internet City".

7. Changes to the Policy

7.1. The Personal Data Processing Policy may be changed or updated occasionally to meet the requirements and standarts. The date of the last update is stated under "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. the new version will replace the old one, and will be effective from the day it is published.

7.3. If a 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 to the Privacy Policy, that means that the Data Subject fully accepts the changes introduced by the new version.

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

8. Contact Information

In you have any questions regarding the processing of your personal data or your privacy rights, please contact us using the following contact information:

- Mailing address: Dubai Internet City 3, 122, Dubai, UAE;
- Email: pdn@ddos-guard.net.

Inquiries will be processed within 1 month.