DDOS-GUARD

IQWeb FZ-LLC
DDoS Protection Company

Personal data processing policy

Revision date and effective date – 12.09.2022

1. General terms and conditions

1.1. The Personala data processing policy (hereinafter - Personal Data Processing Policy)of IQWeb FZ-LLC (hereinafter — as the «Provider») on the processing of personal data determines the list of personal data of Clients who sign up on the Provider's website or who already use the Provider's services and website (hereinafter — as the «Client»), the source of their obtaining, the order of personal data processing, purposes and/or personal data processing conditions.

1.2. The Personal Data Processing Policy applies to all Client's personal data receiving by the Provider

1.3. Sign up on the Provider's website by sending the completed sign up form on this website or entering the signs of consent to the personal data processing in the corresponding web forms of this website or by using the Provider's services or website means that the Client consents tothe personal data processing under the Personal Data Processing Policy and the Privacy Policy.

2. Personal data processing essentials

2.1. The Provider processes personal data to the following purposes:

2.1.1. conclude and execute the Providers service agreement, such as the agreement for the provision of compensated rendering of services (avaliable at - https://ddos-guard.net/file/sladdg_en.pdf), including:

- providing access to the Client Area section in the secure part of the Provider's website to enter into an agreement for the provision and ordering of services;

  - in the performance of concluded service agreements;

  - providing answers to the requests sent by the website user when filling out web forms on the Providers website to services to enter into an agreement for the provision of services.

2.1.2. for technical data of «cookie» to ensure the functioning and improvement of the Provider's website quality towards technical cookie.

2.2. The Provider processes personal data (collection, systematization, buffering, storing, refining (updating, change), blocking, personal data termination) and is a personal data processor.

2.3. The Provider personal data processing is carried out using automated and non-automated means.

2.4. The basis for the personal data processing is the consent of the Client on the purpose of the personal data processing, expressed by placing necessary marks of consent in the web forms on the Provider's website.

3. Sources of personal data obtention

3.1. Personal data is processed and obtained by the Provider from the following sources:

3.2. provided by the Client him/herself when entering the information necessary to render the service or sign up an account or fill out web forms on the Provider's website;

3.3. provided by or on behalf of the pclent when authorizing through third-party websites or when entering such information on a retailer and service outlet specialized page, with which the Company has an agreement for the provision of information and technological interaction of compensated rendering of services.

One should note that the Client authorizes the submission of information. It is impossible to obtain such information without his/her permission.

3.4. when receiving technical data that is automatically transmitted by the device with the help of which the cusomer enters the Provider's website.

4. List of obtained and processed personal data

4.1. The list of the Client's personal data, processed by the Provider following the purposes of processing specified in A. 3 of this Personal Data Processing Policy:

What is obtaining?	How can it be used?
Surname, first name, and patronymic (if any) of the Client (or his/her legal representative).	• to enter into an agreement for the provision of services, including the creation of a user account and identification when signing into the account or responding to requests for services to conclude an agreement for the provision of services; • to perform the agreement for the provision of services; • to identify the Client when signing into the account during the performance of the service agreement; • to record service agreements, including entering data into the Provider's billing system.
E-mail address; phone number; Client's address.	• to perform the service agreement (e.g., access to the personal account or to restore such access) • to send notifications into the concluded service agreement (the option can be disabled in the user account settings).
IP address or other log-information.	• to identify the Client with the intent of

	performing the service agreement.
information provided by the Client only in inquiries regarding the provision of services, internal service identifiers, Client's login.	• to perform the agreement for the provision of services.
the host country of the Client	• to gather statistics on the Client's geolocation (data used in an impersonal form).
data when signing in to the website through third-party platforms (data when signing in with «Google» specified in statement 4.5 of this Policy).	• for the intent of Client authorization and identification for the conclusion of an agreement for the provision of services or its execution.
technical data stored in cookie (for more information on disabling, see Cookie Policy - https://ddos-guard.net/file/cookie_privacy_en.pdf).	• to assist the Client with the website; • to improve the quality of the website (including visits recording statistics) and the quality of service delivery.

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

4.3. If the Client is not an adult or his/her consent is subject to other legal requirements, his/her consent must be established by legislation to use the website or services in the absence of such requirements. The company services usage in the absence of such requirements (e.g., for children under 13) is prohibited.

4.4 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.

4.5. As it pertains to authorization with the Google website (platform), when authorizing, the client provides the following data:

- Name or pseudonym, host country (if specified);

- ID number - Google user personal identifier provided to him/her as part of the account registration on the Google platform.

5. Notice of cookie using. Ways to disable cookie

5.1. 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).

5.2. Our Cookie Policy is available at https://ddos-guard.net/file/cookie_privacy_en.pdf. Note that the Clientr can disable cookie in his/her browser settings at any time.

6. Personal data transfer and dissemination

6.1. The Provider provides personal data processing to fulfill its agreement obligations to the Client, with whom the agreement on the provision of services concluded.

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

6.3. The Provider has the right to provide the processed personal data to the third parties when it is necessary to meet its obligations into the paid services agreement in the process of payment settlements.

Such third parties receive the strictly limited data that is needed to the provision of services to the Client. Providertakes 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 , Firebase Google, Tune, Amplitude, Segmento.

6.4. 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.

6.5 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 Client is a party. By submitting personal data, the Client acknowledges that his/her personal data may be transferred outside of the EEA. In accordance with the clauses 45-49 of the GDPR, the Client 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 Client must also be informed that without his/her consent, the Provider will not be able to provide the Service.

7. Personal data period of storing and personal data processing termination

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

7.2. 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.

7.3. 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.

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

8. The rights of the Client

8.1. The Client has the right to receive information regarding the personal data he/she provides and information relating to its processing, the right to withdraw this consent at any time, to request correction of his/her personal data if inaccuracies are found in the personal data processed by the Provider, the right to request a list of the personal data available to the Provider for processing and entrust the Provider with the transfer of their personal data to a third party if the Provider is technically capable of doing so, the right to erasure, the right to demand clarification (if the data is not accurate or expired), the right to request block or termination (if the data was obtained illegally or is not necessary for the stated purpose of processing) of personal data and other rights due to applicable legislation.

8.2. The Client has the right to withdraw the consent given by him/her by sending a relevant notification to the Provider. The Client 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.

8.3. The r has the right to take measures to protect their rights and legitimate interests, including applying with the appropriate application.

8.4. The r has the right to unsubscribe from newsletters regarding the provision of services or news items under the agreement on the provision of services by going to the Client Area and clicking the «unsubscribe from the newsletter».

8.5. After receiving a corresponding request from the Client, the Provider:

8.5.1. performs identification of the r;

8.5.2. establishes the fact of personal data processing of the r;

8.5.3. provides the r an opportunity to get familiar with the complete information about his personal data, processed by the Provider free of charge;

8.5.4. amends, terminates, or blocks the r's personal data when he/she provides information confirming that the processed personal data is incomplete, expired, unreliable, illegally obtained, or is not necessary for the stated purpose of the processing;

8.5.5. notifies all Parties who have previously been reported incorrect or incomplete personal data of the r; reports of all corrections and / or additions made to them;

8.5.6. informs the r on the results of the requested actions.

8.5.7. performs other actions prescribed by law.

9. Personal data protection

9.1. 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.

9.2. 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.

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

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

9.5. 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.

9.6. 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».

10. The Personal Data Processing Policy Modification

10.1. The Provider has the right to unilaterally change the Personal Data Processing Policy at any time without prior notice. All changes become effective on the date of the relevant version of the Personal Data Processing Policy placement on the Provider's website.

10.2. If rs who already use the services and/or the Provider's website - continue to use the services or specified website after changes made in this edition, agree to the changes.

11. Contact details for questions

11.1. A responsible employee has been assigned by the Provider. to interact on all issues related to this Personal Data Processing Policy.

11.2. 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: pdn@ddos-guard.net

The response period to requests is 1 month.