Terms of Data Processing

The collection of personal data by Direct Messenger OÜ is based on law and the data is collected to the extent necessary for the performance of the concluded contracts and for the best service of the Clients.

Definitions:

Data processing - any act performed on personal data, including its collection, storage, organization, preservation, modification, use, transmission, deletion, destruction or several of the above operations, irrespective of the manner in which the operations are performed and the means used.

Client - a natural or legal person who uses or has expressed a wish to use the services offered by Direct Messenger OÜ.

Data subject - the person whose data is processed.

Controller - a natural or legal person who determines the purposes and means of processing personal data. Direct Messenger OÜ is the Controller in contractual relations with the Client.

Authorized Processor - a natural or legal person who processes personal data on behalf of the Controller. Direct Messenger OÜ is the Authorized Processor in contractual relations with the Clients using the messaging service and the statistics environment.

1. General Data Processing Principles:

The Principle of Legality - the data is processed only in a fair and lawful manner.

The Principle of Purposefulness - The data is collected only for specified and legitimate purposes. It is not processed in a way that is not consistent with the purpose of the treatment.

The Principle of Minimality - data is collected only to the extent necessary to achieve the specified objectives.

The Principle of Security - Personal data is processed in a manner that ensures security, including protection against unauthorized or unlawful processing, accidental loss, destruction or damage by implementing appropriate technical or organizational measures.

Company details - Direct Messenger OÜ, reg. number 11981389, Falgi tee 6/ Toompuiestee 18, Tallinn 10149,

tel +372 5302 5691, support(at)messenger.ee

2. Purpose of Data Processing:

performance of contractual relations;

providing messaging services;

conducting consumer campaigns.

We implement the Google Analytics web analytics tool on our external website, which collects general information about how the visitor uses our site. The data collected is not associated with personally identifiable information and we use it in compiling website statistics.

3. The Composition of Data:

data of the objects of the contract;

data provided by Clients;

data collected in consumer campaigns.

4. Data Security

We use reasonable and appropriate organizational, technical and administrative measures in accordance with applicable law to protect the confidentiality, integrity and availability of personal data.

Databases with personal information are stored on servers protected by firewalls, passwords and other necessary technical solutions to protect our servers from unauthorized system access, allowing only trusted personnel to manage our systems. Use of necessary security measures when accessing and handling the data is required. Security copies of databases are held in locked location accessible only by authorized persons.

Direct Messenger OÜ uses HTTPS connection, which means that the computer connection with our system is encrypted. The green field of the Internet browser with a padlock icon indicates a secure connection. To verify the authenticity of the certificate press the padlock icon.

All of our authorized personnel involved in the processing of your and third persons' personal data, that you have provided us, have committed themselves to confidentiality obligations and shall not access or otherwise process your personal data without your authorization if it is not for the purposes of providing you our services.

We encourage you to take care of the personal data in your possession that you process online and set strong passwords for your SMS account, limit access of your computer and browser by signing off after you have finished your session. Avoid providing any sensitive information which disclosure you believe could cause you substantial harm.

Direct Messenger OÜ is not responsible for violations of security requirements arising from the Client's own actions / inactions.

5. Data Transmission

Direct Messenger OÜ does not transmit personal information to third parties unless the obligation to provide information arises from a contract or by law. For example, Direct Messenger OÜ has agreements with all Estonian mobile operators to provide messaging services.

Transfer of personal data to third countries (i.e., countries which are not Members of European Union or not incorporated in the Agreement on the European Economic Area) is only allowed with the consent of the Controller unless otherwise provided by law.

6. Data Subject Rights:

- to request access to data collected on them;

- to require the correction, deletion, transfer of data collected on them;

- to refuse in whole or in part of the data being processed.

In order to exercise the rights of the data subject, a corresponding digitally signed application must be sent to the address: dpo(at)messenger.ee

In case of violation of rights, the data subject has the opportunity to file a complaint with the data protection supervisory authority - the Data Protection Inspectorate.

7. Data Retention Period

Data is retained until a legitimate aim is attained.