UAB "DEBESŲ VERSLAS" GENERAL DATA PROCESSING AGREEMENT

2023
Vilnius

JSC "Debesų verslas", legal entity code 304249354, registered office address Gurių Sodų 11th, str. 38, Vilnius, represented by Director Martynas Vyžintas, (hereinafter referred to as the **Data Processor**),

Phas signed this Data Processing Agreement (hereinafter referred to as the **Agreement**).

1. ABBREVIATIONS

Unless expressly provided otherwise in this Agreement, the terms capitalized in the first capital shall have the meanings set out below:

Person (Data subject) The person (natural person) whose data is being processed;

Personal data any information relating to an identifiable Person;

Data processor UAB "Debesų verslas" , which processes Personal Data on behalf of and in the interests of the Data Controller and in accordance with his instructions;

Controller UAB "Debesų verslas" , which processes Personal Data on behalf of and in the interests of the Data Processor and in accordance with his instructions;

Data sub-processor JSC "RACKRAY", which is a provider of data storage services. It processes Personal Data on behalf of and in the interests of the Data Controller and in accordance with his instructions.

Sub-processor A third party used by the Data Processor, which shall follow the instructions of the Data Processor and process personal data on behalf of and in the interests of the Data Controller.

Applicable data protection laws any national or international data protection laws or regulations applicable during the term of this Agreement, as the case may be, to the Data Controller or data processor. "Applicable data protection laws" includes the General Data Protection Regulation (GDPR) of the European Union.

Management any operation or set of operations performed using personal data or sets of Personal Data, whether or not it is carried out by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, search, consultation, use, disclosure by transmission, dissemination and availability, coordination, restriction, erasure or destruction;

2. PROCESSING OF PERSONAL DATA

2.1 The Data Processor shall, in the interests and on behalf of the Data Controller, process the Personal Data transferred by the Data Controller in the performance of the Main Agreement.

2.2 The Data Processor shall process the Personal Data transferred by the Data Controller during the period of validity of the Main Agreement.

2.3 The specific aspects of the Processing of Personal Data performed by the Data Processor – the purposes, the categories of personal data subjects, the categories of Personal Data processed, the processing operations performed, the duration of personal data storage, security measures and auxiliary data processors are specified in Annex No. 1 to this Agreement.

2.4 The Processing of Personal Data by the Data Processor is governed by this and the Main Agreements, the instructions of the Data Controller, the Applicable Data Protection Act, which are mandatory for the Data Controller and the Data Processor. When providing instructions regarding the processing of Personal Data to the Data Processor, as well as the Data Processor, when processing Personal Data, the Data Controller complies with the Applicable Data Protection Laws, the Recommendations, Guidelines and other clarifications of the State Data Protection Inspectorate and other competent institutions of the State or the European Union.

2.5 The Data Processor shall not perform any Personal Data Processing Operations that would result in the Data Controller violating the Applicable Data Protection Laws. The Data Processor has the right not to follow the instructions provided by the Data Controller if they contradict the Applicable Data Protection Laws, recommendations, guidelines or other interpretations of the competent state or european Union institutions. The Data Processor shall inform the Data Controller about such refusal to comply with the instructions of the Data Controller by means of communication commonly used.

2.6 In the event of conflicts between the terms of this Agreement, the instructions of the Data Controller, the applicable data protection laws and the recommendations of the State Data Protection Inspectorate or other competent institutions of the State or the European Union, the Data Processor shall immediately inform the Data Controller and resolve this situation in the following sequence of priorities, giving the highest priority to the first and the lowest – to the last:

I) Applicable data protection laws;
II) recommendations, guidelines and explanations of the State Data Protection Inspectorate or other competent institutions of the State or the European Union;
III) the terms of this Agreement;
IV) Instructions from the controller.

2.7 The Data Processor shall immediately inform the Data Controller if there are no instructions regarding the Processing of Personal Data in a particular situation.

2.8 The Data Processor assists the Data Controller in fulfilling its statutory obligations provided for in the Applicable Data Protection Laws, including, but not limited to, the obligation of the Data Controller to respond to the requests of Individuals for the implementation of rights in the field of personal data protection, to carry out an impact assessment on data protection.

2.9 If the Persons, competent authorities or any other third parties request the Data Processor for information about the Personal Data being processed as specified in this Agreement, the Data Processor shall inform the Data Controller of such a request. In no case may the Data Processor act on behalf of the Data Controller or as its representative, and may not transfer or in any other way disclose Personal Data or other information related to the Processing of Personal Data to third parties without prior instructions of the Data Controller. If the Data Processor is obliged to disclose personal data processed by the Data Processor on behalf of the Data Controller in accordance with the Applicable Data Protection Laws or other legal acts, the Data Processor must immediately inform the Data Controller with a request to disclose personal data.

3. SUB-PROCESSORS

3.1 By signing this Agreement, the Data Controller shall give prior consent to the Data Processor to use the Auxiliary Data Processors specified in Annex No. 1 to this Agreement. The Data Processor shall inform the Data Controller thereof before using a different Auxiliary Data Processor than specified in Annex No. 1 to this Agreement and grant the right to object to the use of a new Sub-Processor.

3.2 The Data Processor, regardless of the fact that the Data Controller has given its consent to the use of a certain Auxiliary Data Processor, the Data Processor shall remain fully responsible for the Processing operations of personal data performed by the Sub-Processor.

3.3 The Data Processor shall ensure that all sub-processors engaged assume the same obligations in the field of data protection as assumed by the Data Processor himself under this Agreement.

3.4 The Data Controller has the right to require the Data Processor to carry out an audit of the Sub-Processors or to provide confirmation that such an audit has taken place and to provide information confirming the compliance of the Sub-Processor with the Applicable Data Protection Laws and the requirements of this Agreement. The costs of such audit shall be borne by the Data Processor. The processor may agree with the Sub-Processors specific conditions for the payment of such an audit.

3.5 The processor may not use an sub-processor who is established in a third country in respect of which an adequacy decision has not been taken or is not subject to other appropriate safeguards.

4. TRANSMISSION OF DATA

4.1 The Data Processor may transfer the Processed Personal Data to other data recipients, including the recipients of the data in third countries, on behalf of the Data Controller and in the interests of the Data Controller, only on the instructions or with the consent of the Data Controller, if such a transfer is necessary for the provision of the Data Processor's services.

4.2 Upon receipt of an order from the Data Controller to transfer Personal Data to a third country, the parties to the data transfer establish mandatory data protection measures in accordance with the Applicable Data Protection Laws. If the instruction or consent to the transfer of Personal Data to a third country has been given by the Data Controller, the responsibility for such transfer lies with the Data Controller, regardless of the fact that the transfer was carried out by the Data Processor on behalf of the Data Controller.

4.3 The Data Controller may at any time withdraw an order or consent to the transfer of Personal Data to a specific recipient of data, including recipients of data in third countries. In this case, the Data Processor shall immediately terminate the transfer of Personal Datato the specified data recipients. Such withdrawal of the instruction or consent shall not affect the transfers of Personal Data that have already taken place.

5. SECURITY AND CONFIDENTIALITY OF INFORMATION

5.1 The Data Processor shall ensure that it has taken appropriate technical and organizational measures to protect the processed Personal Data and complies with all data security policies and instructions specified by the Data Controller. The measures must ensure an adequate level of security, taking into account:

5.1.1. existing technical capabilities;
5.1.2. special risks related to the processing of Personal Data;
5.1.3. processing of special categories of Personal Data;
5.1.4. the cost of measures.

5.2 The data processor must ensure a sufficient level of security of personal data. The Data Processor protects Personal Data from destruction, alteration, unauthorized disclosure or unauthorized access. Personal data is also protected from all other unlawful methods of Processing Personal Data. Taking into account the level of technical feasibility, the nature, scope, context and purposes of the processing of Personal Data, the costs of implementing security measures, as well as the risks of varying probability and seriousness posed by the Processing of Personal Data to the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including, *inter alia*, if necessary:

5.2.1. pseudonymisation of personal data and its encryption;

5.2.2. the ability to ensure the continuous confidentiality, integrity, accessibility and resilience of personal data processing systems and services;

5.2.3. the ability to restore conditions and access to Personal Data in a timely manner in the event of a physical or technical incident;

5.2.4. a regular process for the verification, evaluation and evaluation of the effectiveness of technical and organisational measures to ensure the security of the processing of Personal Data.

5.3 Implementing technical and organisational measures as specified in 5.2. The Data Processor shall apply the following or other technical and organizational security measures ensuring an adequate level of data security:

5.3.1. physical access protection. Unattended premises of the Data Processor, with computer equipment and personal information, must be kept locked in order to protect Personal Data from unauthorized use, exposure or theft;

5.3.2. a data recovery process to retrieve Personal Data recovered from backups;

5.3.3. authorisation control, according to which access to Personal Data is possible through the technical permit control system. The permit must be valid only for those persons who need personal data for the performance of direct work functions. Usernames and passwords must be private and cannot be transferred to other entities. Procedures should also be laid down for the allocation and withdrawal of allowances.

5.3.4. the possibility to register logins to personal data. It must be possible to retrospectively view such connections in databases. The Data Processor must check the databases and submit reports to the Data Controller;

5.3.5. secure communication, where external data transmission communications are protected using technical functions that ensure the permission to connect, as well as content encryption in data transmission channels transmitted in transit outside the systems controlled by the Data Processor;

5.3.6. processes designed to ensure the secure destruction of Personal Data when fixed or interchangeable media are no longer used for their intended purpose;

5.3.7. conclusion of confidentiality agreements with service providers that provide maintenance and maintenance of equipment used for the storage of Personal Data;

5.3.8. supervision of service providers at the premises of the Data Processor. The media containing the Personal Data must be removed from the premises if care is not possible.

5.4 The Data Controller may specify in Annex No. 1 to this Agreement specific technical and organizational security measures to be taken by the Data Processor. Other technical and organizational security measures are chosen by the Data Processor at its own discretion, but, in any case, it must ensure that appropriate technical and organizational security measures are implemented to protect personal data.

5.5 The Data Processor, having become aware of any unauthorized access to Personal Data or other security incident (Data Breach), must take all necessary actions and notify the Data Controller without undue delay no later than within 24 hours after becoming aware of the breach. The notification shall include at least:

5.5.1. describe the nature of the personal data breach, including, if possible, the categories and approximate number of persons concerned, as well as the categories and approximate number of extracts of the relevant Personal Data;

5.5.2. the name and contact details of the data protection officer or other contact person who can provide further information;

5.5.3. describe the likely consequences of a personal data breach for individuals;

5.5.4. describe the measures taken or proposed to be taken by the Data Controller to remedy the personal data breach, including, where appropriate, measures to mitigate its possible adverse consequences.

5.6 Without the prior written consent of the Data Controller, the Data Processor undertakes not to disclose the personal data processed to any third parties, except for the use of Other Data Processors, as specified in this Agreement.

5.7 The Data Processor is obliged to ensure that access to Personal Data is granted only to those employees who are necessary for the performance of direct labor functions in accordance with this Agreement. The Data Processor shall ensure that such employees comply with their confidentiality obligations to the same extent as the Data Processor under this Agreement.

6. TERM

6.1 The provisions of this Agreement shall apply to the extent that the Data Processor processes Personal Data on behalf of and in the interests of the Data Controller.

6.2 Upon expiry of this Agreement, the Data Processor shall, at the request of the Data Controller, delete or return all Personal Data to the Data Controller and shall ensure that any Other Data Processor has done the same.

6.3 At the request of the Data Controller, the Data Processor shall inform the Data Controller in writing about the measures taken after the completion of the data processing.

7. APPLICABLE LAW AND DISPUTE SETTLEMENT

7.1 This Agreement shall be regulated and interpreted in accordance with the substantive law of the Republic of Lithuania.

7.2 Any dispute or requirement arising from this Agreement shall be resolved by negotiation or in the courts of the Republic of Lithuania, according to the place of the data controller's registered office.

8. SALARY

8.1 The Data Processor shall not have any right to remuneration for the performance of the obligations provided for in this Agreement.

9. RESPONSIBILITY

9.1. In addition to indemnification for damages for a breach that may occur due to non-compliance with this Agreement and /or other agreements, the Data Controller shall be entitled to receive damages from the Data Processor for all costs, fees and fines incurred by the Data Controller in accordance with the Applicable Data Protection Laws, if the Processing performed by the Data Processor or other data processors used by him has led to the occurrence of damages.

9.2. The Data Controller himself shall have the right to take the measures necessary to verify whether the Data Processor is able to fulfill its obligations under this Agreement and whether the Data Processor has indeed taken measures to ensure such compliance. The Data Processor undertakes to provide the Data Controller with all the necessary information proving compliance with the obligations set forth in this Agreement and allows to carry out audits, including on-the-spot inspections, carried out by the Data Controller or another auditor appointed by the Data Controller. The costs of such audit shall be borne by the Data Controller.

9.3. The Data Processor shall not be held liable for the damage caused to the Data Controller when the Instruction of the Data Controller to perform specific actions with the Personal Data was carried out or there was no fault of the Data Processor.

10. MISCELLANEOUS PROVISIONS

10.1 If the Data Controller reasonably and reasonably requests, the Data Processor shall implement additional technical and organizational security measures or implement changes in the Processing without additional costs. The Data Controller may require the Data Processor to implement additional technical and organizational security measures requiring additional costs. In such a case, the Parties shall, by means of the usual means of communication, agree on the periods for the implementation of such technical and organizational measures and the allocation of costs between the Data Controller and the Data Processor.

10.2 The Data Processor may not transfer the performance of this Agreement without the approval of the Data Controller.

11. MESSAGES

11.1 All communications of one Party to the other Party in connection with this Agreement shall be written and sent by e-mail, courier assistance or registered mail to the addresses of the Parties indicated above or subsequently to the addresses of the Parties as adjusted by the Parties.

11.2 Notifications shall be deemed to have been received by the recipient:

a) if sent through the courier service: at the time of delivery,
b) in the case of registered mail: after three (3) working days, after the notification has been received at the post office of the Recipient Party at the address indicated above, or
c) if sent by e-mail: the day after the email was sent.

12. SPECIMENS AND SIGNATURES

ANNEX 1

Description and instructions for data processing

Objectives Indicate all the purposes for which the Data Processor will process personal data.	Provision of services under the Master Agreement - ensuring the use of the fun cionalums of the Tellq multichannel communication platform for customer service.
Categories of personal data Indicate the types of Personal Data that will be processed for each intended Purpose of processing.	Identification data provided by the person (name, surname, personal identification number), contact details.
Categories of data subjects Specify the categories of Data Subjects whose Personal Data will be processed for each of the intended Purposes of processing.	Customers.
Processing operations Specify the Processing Operations that the Data Processor will perform to achieve each of the intended Purposes of processing.	Connecting customers to Tellq software; configuring services purchased by customers; securing customer data; deleting customer data after disabling the service
Storage requirements If applicable, indicate the duration of storage of personal data processed by the Data Processor for each intended purpose of the Processing.	Tellq during the license period of the software.
Security measures Specify what security measures the controller requires the processor to take when processing his personal data	Encrypting data, backing up, distributing access to data, firewalls and vpns are used.
Other data processors If applicable, please indicate the Other Data Processors used to achieve each of the intended Purposes of processing.	Data warehouse maintenance provider / Devops – UAB Hosty.