Cloud computing and server experts

Baltnetos komunikacijos, UAB

Data Processing Agreement (DPA)

This Data Processing Agreement (hereinafter referred to as the "DPA") regulates the processing of personal data carried out by Baltnetos komunikacijos as the "Processor" on behalf of you as the "Controller". The DPA becomes binding between the Processor and the Controller upon execution of this DPA.

1. The subject-matter, purpose, and nature of processing, type of personal data and categories of data subjects

1.1. The nature, subject-matter and the purpose of the Processor's processing of personal data on behalf of the Controller, information regarding type of personal data processed and categories of data subjects are set out in Appendixes to this DPA.

2. Duration of the processing

2.1. This DPA shall apply during such time the Processor processes personal data on behalf of the Controller.

2.2. Upon the Controller's request, termination or expiry of this DPA, the Processor shall cease its processing activities, and, at the choice of the Controller, delete or return all the personal data to the Controller and delete the existing copies of such data, unless otherwise required under the applicable data protection law.

3. Processing of personal data – obligations of the Processor

3.1. The Processor has implemented appropriate technical and organizational measures in such a manner that its processing of personal data under this DPA will comply with applicable data protection law, in particular Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 (hereinafter referred to as the "GDPR"), and ensure the protection of the rights of the data subject.

3.2. The Processor undertakes to only process personal data in accordance with documented written instructions communicated by the Controller, unless required to do so pursuant to the applicable law. In such case the Processor shall, to the extent permitted by law, inform the Controller of that legal requirement before such processing takes place. The Processor shall immediately inform the Controller if the Processor does not have an instruction for how to process personal data in a particular situation or if any instruction infringes the applicable data protection law.

3.3. The Processor shall assist the Controller in fulfilling the Controller's obligation to respond to requests for exercising the data subject's rights taking into account the nature of data processing and, to the extent possible, using appropriate technical and organizational measures. Hereunder, the data subject's rights include the rights to request information and, at the data subject's request, to rectify, destroy personal data or suspend further processing of personal data.

3.4. The Processor shall assist the Controller in fulfilling specific obligations under the applicable data protection laws, taking into account the nature of the processing and the information available to the Processor. Specific obligations are include security of data processing (Article 32 of the GDPR), notification of personal data breach (Articles 33-34 of the GDPR), as well as data protection impact assessment and prior consultation (Articles 35-36 of the GDPR).

3.5. The Processor undertakes to make available to the Controller all information and all assistance necessary to demonstrate compliance with the obligations laid down in this DPA and allow for and contribute to audits, including on-site inspections conducted by the Controller or another auditor mandated by the Controller.

4. Sub-processors

4.1. The Controller has approved that the Processor can engage the companies listed in Appendix 1 as sub-processors. The Processor shall inform the Controller of any intended changes concerning the engagement or replacement of sub-processors with a right for the Controller to object.

4.2. The Processor shall ensure and upon the Controller's request document that sub-processors are bound by written agreements that impose the same obligations when processing personal data as those obligations laid down in this DPA. The Processor shall remain fully liable to the Controller for the performance of the sub-processor's obligations.

4.3. The Controller may request that the Processor verify the sub-processor or provide confirmation that such verification has taken place, or, where available, obtain or assist the Controller in obtaining a third-party audit report concerning sub-processor's operations to ensure compliance with the applicable data protection laws.

5. Transfer to third countries

5.1. The undertaking of the agreed processing of personal data shall be carried out exclusively within a member state of the European Union (EU) or within a member state of the European Economic Area (EEA). Each and every transfer of personal data to a country, which is not a member state of either the EU or the EEA, may only take place with the prior written consent of the Controller and only occur if the special conditions set out in the applicable data protection legislation, Chapter V of the GDPR, are met.

5.2. The Controller may at any time withdraw its consent to the transfer of data to third countries in accordance with Sub-clause 5.1 of this DPA. In such case, the Processor shall immediately terminate the data transfer and, upon the Controller's request, provide written confirmation of such termination.

6. Information security and confidentiality

6.1. The Processor shall ensure adequate protection of personal data hereunder for the purpose of protecting personal data against destruction, alteration, unauthorized distribution or access to such data. The personal data shall also be protected against all other forms of unlawful processing.

6.2. The Processor shall draw up and keep up-to-date a description of its technical, organizational, and physical measures to comply with the applicable data protection legislation.

6.3. The Processor undertakes not to, without the Controller's prior written consent, disclose or otherwise make personal data processed under this DPA available to any third party, except for sub-processors engaged in accordance with this DPA.

6.4. The Processor shall ensure that any persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7. Applicable law and dispute resolution

7.1. This DPA shall be governed by and construed in accordance with the laws of jurisdiction indicated in the Appendixes of this DPA without reference to any conflict-of-law principles, under which different law might otherwise be applicable.

7.2. The parties agree that the sole and exclusive jurisdiction as well as venue for any and all disputes arising out of or in connection with this DPA shall be the court of agreed jurisdiction.

8. Limitation of liability and indemnity

8.1. Unless otherwise agreed, the parties shall be liable according to the general rules of applicable law according to the section 7 of the DPA. Notwithstanding the foregoing, the parties exclude any liability for operational loss, profit loss, loss of goodwill, and any other indirect loss as well as consequential damage. Data loss shall be considered an indirect loss.

8.2. The Processor's total aggregate liability under this DPA shall under any circumstances be limited to the remuneration of the last six (6) months paid for the services and obligations according to this DPA before the cause of action arose. If less than six (6) months have passed, the remuneration paid shall be considered as an average of the remuneration paid multiplied equaling to six (6) months.

Appendix 1 to the Data Processing Agreement for Server and Computer Maintenance Services

The subject-matter and the purpose of processing	The delivery of the following services or tasks by the Processor to the Controller: Server and computer maintenance services
Types of personal data processed	Personal data processed includes personal business contact information such as full name, phone or cell phone number, email address, passwords, employment details including employer name, and personal identification numbers.
Categories of data subjects	The Controller's representatives and end users, such as employees, job applicants, contractors, co-workers, partners, also the Controller's customers, hospital patients, and other persons to be entered into the Controller's central data system.
Data processing operations/activities	Entering, adjusting, and deleting personal data, also backing up and storing servers that may contain personal data for no longer than the Controller has purchased the backup service.
List of sub-processors	N/A
Jurisdiction	Lithuania

Appendix 2 to the Data Processing Agreement for IaaS services

The subject-matter and the purpose of processing	The delivery of the following services or tasks by the Processor to the Controller: IaaS services
Types of personal data processed	Only the Controller's contact information, full name, position, phone number, cell phone number, email address, encrypted password for login to the control panel.
Categories of data subjects	The Controller's representatives.
Data processing operations/activities	Backing up virtual machines based on a backup service acquired by the customer.
List of sub-processors	N/A
Jurisdiction	Lithuania

Appendix 3 to the Data Processing Agreement for Shared Hosting and Virtual Dedicated Server Services

The subject-matter and the purpose of processing	The delivery of the following services or tasks by the Processor to the Controller: Shared hosting and virtual dedicated server services
Types of personal data processed	Only the Controller's contact information, full name, position, phone number, cell phone number, email address, encrypted password for login to the control panel.
Categories of data subjects	The Controller's representatives.
Data processing operations/activities	Backing up and storing virtual machines and websites for no longer than 14 days.
List of sub-processors	N/A
Jurisdiction	Lithuania

J. Rutkausko str. 6, 05132, Vilnius
Brastos str. 14, 47185, Kaunas
Šilutės rd. 2 - 517, 91111, Klaipėda

tel. (8-5) 274 5 444
tel. (8-37) 400 140
tel. (8-46) 397 080

info@balt.net
www.balt.net

Appendix 4 to the Data Processing Agreement for VoIP Services

The subject-matter and the purpose of processing	The delivery of the following services or tasks by the Processor to the Controller: VoIP services
Types of personal data processed	The Controller's contact information, full name, position, phone number, cell phone number, email address, encrypted password for login to the control panel. The Controller's client/partner calling information, time, duration, CDR, name, surname, email address, job title and functions.
Categories of data subjects	The Controller's representatives and customers.
Data processing operations/activities	CDR storage no more than 6 months.
List of sub-processors	Debesų verslas, UAB
Jurisdiction	Lithuania

Appendix 5 to the Data Processing Agreement for All Services Collectively

The subject-matter and the purpose of processing	The delivery of the following services or tasks by the Processor to the Controller: Provision of services - Data subject's service purchase (order) processing, administration, request processing; For identification of the data subject in the information systems of the Processor.
Types of personal data processed	Only the Controller's contact information, full name, position, phone number, cell phone number, email address, encrypted password for login to the control panel.
Categories of data subjects	The Controller's representatives
Data processing operations/activities	Entering, adjusting, and deleting personal data, as well as backing up and storing servers that may contain personal data.
List of sub-processors	N/A
Jurisdiction	Lithuania

Appendix 6. Technical and organizational measures used by the Processor

The Processor has implemented the service management system ISO/IEC 20000 and the information security management system ISO/IEC 27001 in the organization, where the list of technical and organizational measures is more extensive. The following measures are main measures for the protection of personal data:

1. Secure access to information is ensured by these measures:
   - **1.1.** IT systems change management is performed;
   - **1.2.** Access is given on a "need to know" basis;
   - **1.3.** Identification and authentication of users is performed from the moment of turning on the computer until the launching of the program and accessing the database;
   - **1.4.** Special requirements for passwords are applied;
   - **1.5.** Periodic review of access to information resources as well as access cards is performed;
   - **1.6.** Protection (lock) system controls the access to the Processor's premises;
   - **1.7.** Alarm is used (against break-in, fire);
   - **1.8.** Personal data on a hard copy is retained only in lockable drawers;
   - **1.9.** Personal data in an electronic form is retained only in those information systems, to which access is strictly limited;
   - **1.10.** Clean desk and screen policy are being adhered to;
   - **1.11.** Access to the server-rooms (data center) is only granted after having read the data center rules of conduct subject to pre-registration and the express written permission to access the data center;
   - **1.12.** Only the system administrator has access to the control and configuration of operating systems of the servers from one fixed IP;
   - **1.13.** When the computer and/or mobile device is not in use, their screens are locked;
   - **1.14.** External storage devices are being encrypted; personal data is not stored in non-encrypted storage devices;
   - **1.15.** Information located in laptops is protected by the name and password of the operating system's user, hard disk is encrypted.
2. Identification of users:
   - **2.1.** Passwords are used in every level – from the moment of turning on the computer until the launching of the program and accessing the database;
   - **2.2.** Special requirements for passwords are determined (mandatory periodic password reset, limitations on the length and complexity of password, old passwords are prohibited);
   - **2.3.** Two-factor authentication is used.
3. Employees of the Processor are prohibited from sharing access data with other persons.
4. Information system testing is performed only with depersonalized data.
5. When communicating about problems encountered and submitting print screens in the documentation, personal data is removed or depersonalized (by shading over).
6. Prior to sending personal data via email, personal data is encrypted by submitting the unlocking key via separate email or by using other communication channel (e.g., SMS).
7. Information processed by other than system means (e.g., electronic documents created by using Word, Excel, PowerPoint, communications created by using Outlook) is classified by having regard to the content of the document.
8. Backup copies of the databases used are made to ensure the data security from data loss. Access to backups is strictly controlled and data recovery is recorded. The backups that need to be transferred are encrypted.
9. Deleting of information retained in the storage devices (e.g., SSD, HDD, USB flash drives, external hard drives, memory cards, and mobile phones) is performed by using specialized software or physically destroying the storage.
10. CDs and DVDs that are no longer used must be physically destroyed.
11. Computer equipment is handed over for recycling without storage devices.
12. Before transferring the computer to another controller, it must be reinstalled.
13. Before transferring mobile devices (e.g., phones, tablets) to another controller or for repairs, recycling, the device's memory is erased by resetting the device to factory settings and the memory cards are removed.

J. Rutkausko str. 6, 05132, Vilnius
Brastos str. 14, 47185, Kaunas
Šilutės rd. 2 - 517, 91111, Klaipėda
tel. (8-5) 274 5 444
tel. (8-37) 400 140
tel. (8-46) 397 080
info@balt.net
www.balt.net

14. All of the Processor's employees sign a confidentiality undertaking of a prescribed form, which obligates them to keep the personal data, which has been made available to them, for an indefinite period.

15. Communication security is ensured, when the external data transfer connections must be protected by using technical measures, which ensure that the communication would be authorized and encrypted when transferring personal data via communications channels through external systems controlled by the Processor.

16. Possibility is ensured to trace access to personal data in the past through a log or similar information base. Logs must be protected, and unauthorized persons cannot access them. The Processor must have a possibility to inspect information base and inform the Controller about this.

17. After the end of the data processing period, all of personal data and copies thereof are deleted and/or returned to the Controller.

J. Rutkausko str. 6, 05132, Vilnius
Brastos str. 14, 47185, Kaunas
Šilutės rd. 2 - 517, 91111, Klaipėda
tel. (8-5) 274 5 444
tel. (8-37) 400 140
tel. (8-46) 397 080
info@balt.net
www.balt.net