

Data Processing Agreement

1. Introduction

This Data Processing Agreement is between The Customer (as defined below, the "Controller") and **NEXUSMEDIA OÜ**, a private limited company, registered at Harju maakond, Tallinn, Lasnamäe linnaosa, Sepapaja tn 6, 15551, Republic of Estonia, code № 14227173, email address support@nexusmedia-ua.com, represented by Denys Shchotkin, the Management Board Member, (hereinafter - the "**Processor**"). This Data Processing Agreement reflects the parties' agreement with respect to the terms governing the processing and security of Customer Data.

Data Processing Agreement (DPA) regulates processing of Controller's Data by **Processor** on behalf of the Controller.

2. Key definitions

- 2.1. "Agreement" means NexusMedia's Privacy Policy and this DPA.
- 2.2. "App" means any of such applications: EasyAuth, EasyOrder, EasyLocation or EasyLockdown.
- 2.3. "Customer" means the person or the organization, agreeing to this DPA.
- 2.4. "Controller's Data" means data received via Customer website using Apps.
- 2.5. "Controller's Personal Data" means personal data contained within the Controller's Data.
- 2.6. "Data Incident" means a breach of NexusMedia's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Controller's Personal Data on systems managed by or otherwise controlled by NexusMedia. "Data Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Controller's Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.
- 2.7. "DPA Effective Date" means the date on which Customer purchases the App via Shopify App store (<https://apps.shopify.com>).
- 2.8. "EEA" means the European Economic Area.
- 2.9. "Applicable Data Protection Legislation" means, as applicable: a) [Personal Data Protection Act](#) of the Republic of Estonia; b) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) - to come into force on 25 May 2018.

- 2.10. "Non-Applicable Data Protection Legislation" means data protection or privacy legislation other than the Applicable Data Protection Legislation.
- 2.11. "Services" means maintenance Apps to work in accordance with the declared functionality and any related professional services.
- 2.12. "Sub-Processors" means persons authorized under this Data Processing Agreement to have logical access to and process Customer Data in order to provide parts of the Services and related technical support.
- 2.13. "Term" means the period from the DPA Effective Date until the end of NexusMedia's provision of the Services under the applicable Agreement.
- 2.14. The terms "personal data", "data subject", "processing", "controller", "processor" and "Supervisory authority" as used in this Data Processing Agreement have the meanings given in the GDPR, in each case irrespective of whether the Applicable Data Protection Legislation or Non-Applicable Data Protection Legislation applies.

3. Legislation

- 3.1. The Data Processing Agreement shall ensure that the Processor complies with the Applicable Data Protection Legislation.

4. Processing of Controller's Data

- 4.1. In connection with the Processor's delivery of the Services to the Controller, the Processor will process certain categories and types of the Controller's Personal data on behalf of the Controller.
- 4.2. The categories and types of Controller's Personal data processed by the Processor on behalf of the Controller are listed in sub-appendix A. The Processor only performs processing activities that are necessary and relevant to perform the Services. The parties shall update sub-appendix A whenever changes occur that necessitates an update.
- 4.3. The Processor shall have and maintain a register of processing activities in accordance with GDPR, article 30 (2).
- 4.4. The Processor shall collect and maintain records of certain information, including the name and contact details of each Controller on behalf of which the Processor is acting and, where applicable, of such controller's local representative and data protection officer and make such information available to the supervisory authorities.
- 4.5. The Processor processes personal data about the Controller and the Controller's employees in connection with the Processor's support, communication and marketing. These personal data are not comprised by this Data Processing Agreement, because the Processor is the Controller

for said personal data, and reference is made to the Processor's privacy policy available at the Processor's website.

5. Instruction

- 5.1. The Processor may only act and process the Controller's Data in accordance with the documented instruction from the Controller (the "Instruction"). The Instruction at the time of entering into this Data Processing Agreement is that the Processor may only process the Controller's Personal Data with the purpose of delivering the Services as described in the Agreement.
- 5.2. The Controller guarantees that the Controller's Data transferred to the Processor is processed by the Controller in accordance with the Applicable Law, including the legislative requirements and lawfulness of processing.
- 5.3. The Processor shall give notice without undue delay if the Processor considers the at the time being Instruction to be in conflict with the Applicable Law.

6. The Processor's obligations

6.1. Confidentiality

- 6.1.1. The Processor shall treat all the Controller's Data as strictly confidential information. The Controller's Personal Data may not be copied, transferred or otherwise processed in conflict with the Instruction, unless the Controller in writing has agreed hereto.
- 6.1.2. The Processor's employees and Sub-Processors shall be subject to an obligation of confidentiality that ensures that the employees and Sub-Processors shall treat all the Controller's Personal Data under this Data Processing Agreement with strict confidentiality.

6.2. Security

- 6.2.1. The Processor shall implement the appropriate technical and organizational measures as set out in this Agreement and in the Applicable Data Protection Legislation, including in accordance with GDPR, article 32.
- 6.2.2. The Processor shall always use pseudonymisation as a method of securing the Personal Data.
- 6.2.3. The Processor shall ensure that access to the Controller's Personal Data is restricted to only the employees and Sub-Processors to whom it is necessary and relevant to process the Controller's Personal Data in order for the Processor to perform its obligations under Data Processing Agreement.

6.2.4. The Processor shall also ensure that the Processor's employees and Sub-Processors processes the Controller's Personal Data only in accordance with the Instruction.

6.2.5. The Processor shall provide documentation for the Processor's security measures if requested by the Controller in writing.

6.3. Data protection impact assessments and prior consultation.

6.3.1. If the Processor's assistance is necessary and relevant, the Processor shall assist the Controller in preparing data protection impact assessments in accordance with GDPR.

6.4. Rights of the data subjects

6.4.1. If the Controller receives a request from a data subject for the exercise of the data subject's rights under the Applicable Data Protection Legislation and the correct and legitimate reply to such a request necessitates the Processor's assistance, the Processor shall assist the Controller by providing the necessary information and documentation. The Processor shall be given reasonable time to assist the Controller with such requests in accordance with the Applicable Law.

6.4.2. If the Processor receives a request from a data subject for the exercise of the data subject's rights under the Applicable Data Protection Legislation and such request is related to the Personal Data of the Controller, the Processor must immediately forward the request to the Controller and must refrain from responding to the person directly.

6.5. Data Incident

6.5.1. The Processor shall give immediate notice to the Controller if the Data Incident occurs.

6.5.2. The Processor shall have and maintain a register of all Data Incident. The register shall at a minimum include the following:

- A description of the nature of the Data Incident, including, if possible, the categories and the approximate number of affected Data Subjects and the categories and the approximate number of affected registrations of Controller's Personal Data.
- A description of the likely as well as actually occurred consequences of the Data Incident.
- A description of the measures that the Processor has taken or proposes to take to address the Data Incident, including, where appropriate, measures taken to mitigate its adverse effects.

- 6.5.3. The register of Data Incident shall be provided to the Controller in copy if so requested in writing by the Controller or the Supervisory authority.

6.6. **Documentation of compliance**

- 6.6.1. The Processor shall after the Controller's written request hereof provide documentation substantiating that:
- the Processor complies with its obligations under this Data Processing Agreement and the Instruction; and
 - the Processor complies with the Applicable Data Protection Legislation in respect of the processing of the Controller's Personal Data.
- 6.6.2. The Processor's documentation of compliance shall be provided within reasonable time.

7. **Sub-Processors**

- 7.1. The Processor is given general authorization to engage Sub-Processors to process the Controller's Data without obtaining any further written, specific authorization from the Controller, provided that the Processor notifies the Controller in writing about the identity of a potential Sub-Processor (and its processors, if any) before any agreements are made with the relevant Sub-Processors and before the relevant Sub-Processor processes any of the Controller's Personal Data. If the Controller wish to object to the relevant Sub-Processor, the Controller shall give notice hereof in writing within seven (7) calendar days from receiving the notification from the Processor. Absence of any objections from the Controller shall be deemed a consent to the relevant Sub-Processor.
- 7.2. The Processor shall conclude a written Sub-Processing agreement with any Sub-Processors. Such an agreement shall at minimum provide the same data protection obligations as the ones applicable to the Processor, including the obligations under this Data Processing Agreement. The Sub-Processors only access and use Controller's Personal Data to the extent required to perform the obligations subcontracted to it, the data protection obligations set out in Article 28(3) of the GDPR, are imposed on the Sub-Processors. The Processor shall on an ongoing basis monitor and control its Sub-Processors' compliance with the Applicable Data Protection Legislation. Documentation of such monitoring and control shall be provided to the Controller if so requested in writing.
- 7.3. The Processor is responsible to the Controller for any Sub-Processor in the same way as for its own actions and omissions.
- 7.4. The list of Sub-Processors which are used by the Processor on the time of entering into this Data Processing Agreement will be provided to the Controller if so requested in writing by email.

- 7.5. If the Processor initiates sub-processing with a new Sub-Processor, such new Sub-Processor shall be added to the list.

8. Location of Controller's Data

- 8.1. Controller's Data processed by the Processor will be stored and processed exclusively in secure hosting facilities provided by DigitalOcean LLC (<https://www.digitalocean.com>) and located in The Kingdom of the Netherlands. DigitalOcean's infrastructure is secured through a defense-in-depth layered approach.
- 8.2. The Processor may transfer the Controller's Personal Data to third countries outside of the EEA only when it is necessary to solve the Controller's problem and the Controller request for it. Any transfer of the Controller's Personal Data to any third countries shall only be done to the extent such transfer is permitted and done in accordance with the Applicable Data Protection Legislation.
- 8.3. Transfer of Controller's Personal Data to countries outside of the EEA is relied on a consent obtained from Controller. The Controller give consent to transfer Controller's Personal Data in every case of such transfer.

9. Termination

- 9.1. The Processor's authorization to process Controller's Data on behalf of the Controller shall be annulled at the termination of this Data Processing Agreement.
- 9.2. At the termination of this Data Processing Agreement, the Processor and its Sub-Processors shall delete all the Controller's Data and provide documentation for such deletion to the Controller.

10. Governing law

- 10.1. This DPA and any dispute or claim arising out of or in connection with it shall be governed by and construed in accordance with the law of the Republic of Estonia.

Sub-appendix A

Controller's Personal Data

The Processor processes the following types of Controller's Personal Data in connection with its delivery of the Services:

- Controller's Clients Data: geolocation data, IP-addresses, social network authenticators, email address, phone number and billing information.
- Personal data provided by the Clients and Visitors of the website in connection with their use of the website of the Controller (these personal data are not seen or accessed by the Processor unless the Processor after the request hereof from the Controller assists with support and bug fixing).

Categories of data subjects

The Processor processes Controller's Personal Data about the following categories of data subjects on behalf of the Controller:

- Controller's Clients.
- Visitors of the Controller's website.

Sub-appendix B

Current Sub-Processors

The following Sub-Processors shall be considered approved by the Controller at the time of entering into this Data Processing Agreement:

- Hosting supplier: DigitalOcean LLC (<https://www.digitalocean.com>) located in The Kingdom of the Netherlands.
- Work organizers: Trello (<http://trello.com/>) provided by Trello, Inc., Front (<https://frontapp.com/>) provided by frontapp.com, Inc. and Slack (<https://slack.com/>) provided by Slack Technologies Inc.
- Back-up service: Dropbox (<https://www.dropbox.com/>) provided by Dropbox, Inc.
- Communication: Gmail (<https://mail.google.com/>) provided by Google LLC.