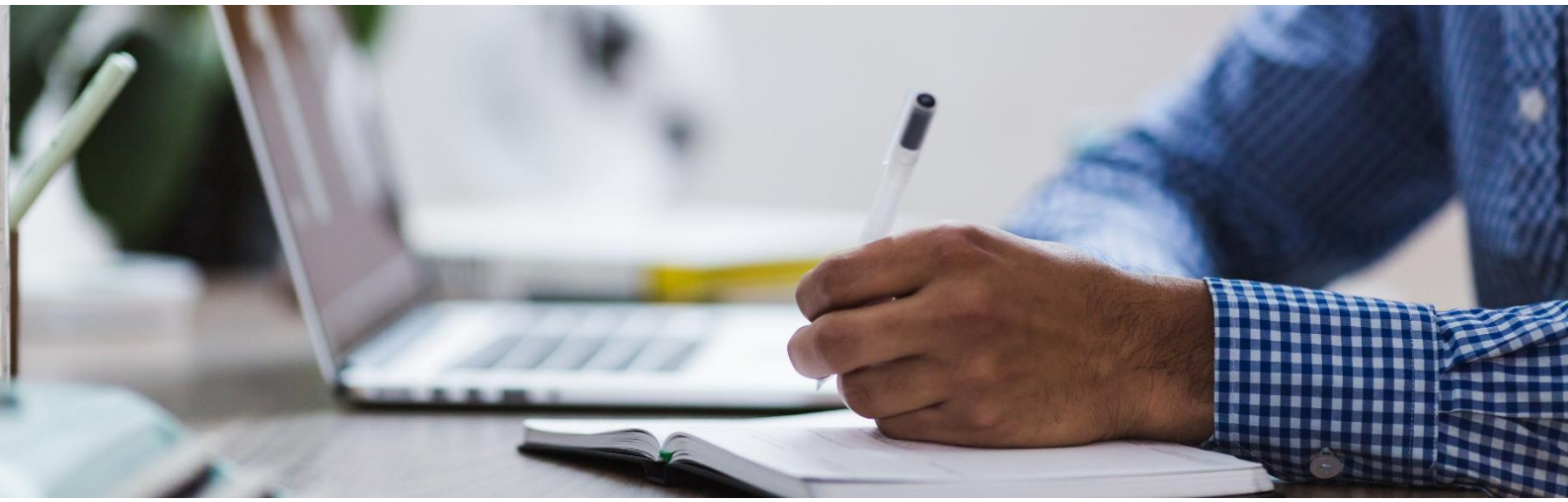
UAB „NEVDA“ AGREEMENT ON THE PROCESSING OF PERSONAL DATA

version 1.1



© UAB „NEVDA“, 2022. Konfidencialu. Visos teisės priklauso dokumento rengėjui.

Contents

© UAB „NEVDA“, 2022. Konfidencialu. Visos teisės priklauso dokumento rengėjui.

1 Introduction

The core business of UAB Nevda is the development, implementation and maintenance of information systems for public sector organizations and businesses.

1.1 Overview

This Agreement on the processing of personal data is concluded between LLC Nevda, legal entity code 121931451, hereinafter referred to as the (Service provider) and the Client, together in the Agreement referred to as the "Parties" or each individually as the "Party", and taking into account that:

- the Parties will enter into a service contract on the basis of which the Data Processor shall provide services to the Data Controller (hereinafter referred to as the Contract);
- on the basis of the Contract, the Data Processor shall process the personal data of the respective data subjects submitted by the Data Controller on behalf of the Data Controller;
- the Parties seek to ensure the implementation of the Contract in accordance with the requirements of the protection of personal data and have therefore concluded this Agreement (hereinafter referred to as the Agreement) on the processing of personal to the Contract under the conditions set out below

1.2 Terms and Definitions

Sąvokų trumpiniai	Aprašymas
Personal data	personal data (excluding specific categories of personal data) as defined in Article 4(1) of the Regulation, which are provided and / or access granted thereto to Data Processor by the Data Controller in accordance with the conditions set out in this Agreement;
Personal data subject	a natural person whose Personal Data are processed in accordance with the provisions specified in the Regulation, other legal acts regulating the legal protection of personal data and this Agreement
Data processing	any operation or set of operations which is performed on personal data, whether or not by automated means, including, but not limited to: recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, as well as alignment or combination with other data, restriction, erasure or destruction;
Regulations or GDPR	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

© UAB „NEVDA“, 2022. Konfidencialu. Visos teisės priklauso dokumento rengėjui.

	and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
Incident	an event or set of circumstances that has occurred in the information technology infrastructure managed by the Data Controller that affects the of the provision services or operation of systems provided by the Data Processor.
Breach of the security of personal data	an event or set of circumstances that may affect the destruction, loss, alteration, unauthorized disclosure or unlawful acquisition of access to personal data.
Data Controller's responsible person	a responsible person (administrator or security representative) appointed by the Data Controller who coordinates the resolution of incidents and controls the granting of access rights to the data stored in the Data Controller's IS;

Other terms used in the Agreement shall have the meanings as defined in the Contract and in the legislation on the protection of personal data.

2 Purpose and nature of data processing

Subject matter and purpose of the data processing: for the purpose of performance of the Contract, personal data processed by the Data Controller and / or their sets with which the Data Processor is required to perform data processing operations by automated means shall be transferred to the Data Processor.

3 Duration of data processing

This Agreement shall apply for as long as the Data Processor processes personal data on behalf of the Data Controller in accordance with the Contract and this Agreement.

4 Obligations of the data processor

- The Data Processor shall undertake to process only the personal data specified in this Agreement and for the purposes set forth in the Agreement, as well as in accordance with the legislation on the protection of personal data, the Regulation and the instructions documented by the Data Controller.
- The Data Processor shall appoint a Data Protection Officer who shall ensure the proper performance of the tasks referred to in Article 39 of the GDPR.
- During the period of validity of the Agreement, the Data Processor shall implement appropriate technical and organizational measures to ensure the compliance of the processing of personal data carried out by it with the provisions of this Agreement, with the applicable legislation on the protection of personal data, in particular with GDPR, and shall guarantee the protection of data subjects' rights. A description of the technical and organizational measures used by the Data Processor during the conclusion of the Contract and this Agreement shall be provided in Annex No. 1.

© UAB „NEVDA“, 2022. Konfidencialu. Visos teisės priklauso dokumento rengėjui.

- The Data Processor shall, taking into account the nature of the data processing and to the extent possible, using appropriate technical and organizational measures, assist the Data Controller in performing the Data Controller's obligation to respond to requests of data subjects to exercise their rights. The rights of the data subject under this Agreement shall include the right to request information and, at the request of the data subject, to rectify, destroy or suspend the processing of personal data.
- The Data Processor shall, taking into account the nature of data processing and the information available, assist the Data Controller in fulfilling its specific obligations under the applicable legislation on the protection of personal data. Specific obligations shall include the security of data processing (Article 32 of the GDPR), notification of a personal data breach (Articles 33-34 of the GDPR) and data protection impact assessment and prior consultation (Articles 35-36 of the GDPR).
- The Data Processor shall undertake to provide the Data Controller with all information and assistance in proving that the obligations assumed under this Agreement have been fulfilled, and to facilitate and assist the Data Controller or any other auditor authorized by it to perform an audit, including on-site inspections.
- The Data Controller may carry out more detailed audits at his own expense, which shall be:
    - limited only to matters specifically related to the Data Controller and coordinated in advance with the Data Processor;
    - carried out with reasonable notice, which may not be less than 4 weeks, unless there are identifiable significant obstacles to doing so;
    - carried out in such a way as not to interfere with the day-to-day operations of the Data Processor.

5 Subsidiary data processors

- The Data Processor shall have the right to invoke another Data Processor. The Data Processor shall ensure that the person it invokes complies with the requirements of the legislation on the protection of personal data (including the implementation of appropriate organizational and technical measures) and that the obligations are no less than the ones imposed on the Data Processor by this Agreement itself and shall be liable to the Data Controller for the performance of the obligations of the third party invoked.
- The Data Processor shall ensure and, at the request of the Data Controller, document that the subsidiary data processors are bound by written contracts, according to which, in addition to the obligations laid down in this Agreement, they are required to fulfil the relevant data processing obligations. The Data Processor shall be fully liable to the Data Controller for the obligations performed by the subsidiary data processors.

6 Transmission of data to third parties

The obligation to process personal data under this Agreement may be exercised only in a Member State of the European Union (EU) or the member state of the European Economic Area (EEA). Any transfer of personal data to a country other than EU or EEA Member State may only take place subject to prior written consent of the Data Controller and only if the special conditions, set out in the applicable legislation on the protection of personal data, Chapter V of the GDPR, are met.

© UAB „NEVDA“, 2022. Konfidencialu. Visos teisės priklauso dokumento rengėjui.

7 Security and confidentiality of information

- The Data Processor shall ensure adequate protection of personal data in accordance with this Agreement for the purpose of protecting personal data against destruction, alteration, unauthorized dissemination or unauthorized access. Personal data shall also be protected against other forms of unlawful processing.
- The Data Processor shall draw up and keep up-to-date a description of its technical, organizational and physical measures to comply with the applicable legislation on the protection of personal data.
- Without the prior written consent of the Data Controller, the Data Processor shall undertake not to disclose personal data processed under this Agreement or not to allow other access to them to any third party, except for subsidiary data processors which are invoked under this Agreement.
- The Data Processor shall ensure that all persons involved in the processing of personal data have a permanent obligation of confidentiality by means of a confidentiality contract or that they are subject to an appropriate legal obligation of confidentiality.
- If, for any reason, either Party is unable to comply with the terms of this Agreement, it shall immediately inform the other Party.

8 Breaches of personal data security

- In the event of a personal data breach or upon a reasoned suspicion by the Data Processor of such a breach, the Data Processor shall immediately, but in any case not later than within 24 hours after it has become aware of it, inform the Data Controller in writing and provide the available information and data related to such breach.
- Upon the request of the Data Controller, the Data Processor shall provide the Data Controller without undue delay with the required additional documents, information and data necessary for the Data Controller to identify and / or verify the fact of a breach of personal data security, investigate its circumstances and take immediate measures to eliminate the breach or reduce its negative consequences.

9 The liability of the dataprocessor, dispute resolution procedures and contact persons

- Depending on the nature, scope, context and purposes of the processing of Personal Data, including the fact that the Data Processor is obliged to process Personal Data as an integral part of proper performance of the Contract, the Parties shall consider that in the event of a breach / improper performance of the Agreement, breach of the Regulation, the Data Processor will compensate the damage incurred.
- The parties shall not be liable for operating losses, loss of profits, loss of goodwill and any other indirect losses and damages resulting there from.

© UAB „NEVDA“, 2022. Konfidencialu. Visos teisės priklauso dokumento rengėjui.

Annex No.1

A check-list of technical and organizational security measures used by the Data Processor

Priemonės pavadinimas	Priemonės naudojimo aprašymas
Risk management (regular review, assessment and evaluation of effectiveness)	• regular analysis of tangible and intangible losses that may occur in the course of data processing activities and in the main data processing systems; • a risk assessment (ISO 27005 standard) for information security and conformity assessment shall be carried out once a year.
Access control	• the concept of physical security is established, which defines security zones (public spaces, office, data centre); • access is controlled by access permissions; • access to the data centre is protected by advanced security measures; • access to personal data is provided by ensuring a secure registration process and a secure password policy (strong passwords, regular password change)' • a procedure for confirming and revoking access permissions has been established and passwords are securely transmitted; • access permissions are regularly checked and updated; • external access to personal data is only possible using encryption methods (SSL and / or VPN).
Information network control	• a firewall is used to securely isolate information systems from external access from public networks; • the use of anti-virus software is regularly checked; • relevant security updates are imported on a regular basis.
Transmission control	• remote access (via public networks) is always encrypted; • specifications and processes for the physical destruction of documents are established.
Storage control	• rules on the storage of personal data are laid down; • access to personal data, based on assigned personal user accounts; • data transfer log files/protocols are present.
Control of instructions	• responsibilities (e.g., data owner, system administrator) for the tasks of data processing and related systems are present; • the areas of responsibility for data processing are clearly regulated (data controller <-> data processor, subsidiary data processor, etc.); • staff members are trained in data protection and awareness-raising measures are in place;

© UAB „NEVDA“, 2022. Konfidencialu. Visos teisės priklauso dokumento rengėjui.

	• Data Processor's employees are required to comply with a separate confidentiality agreement; • Subsidiary data processors who are granted access to the Data Controller's data comply with all the technical and organizational measures included in this check-list.
Accessibility control	• physical security measures are present to protect access to personal data (fire protection measures, air conditioning, UPS protection); • a back-up copy of the data is made regularly; • backup copies of the data are stored in an external storage facility or in a secure alternative environment; • the operation of the systems is constantly monitored automatically; • reporting IT incidents and measures taken to resolve system performance issues; • measures are in place to identify potential data protection incidents.
Separation control	• production and testing systems are present; • employees of the Data Processor are instructed that personal data may only be processed for the defined purposes.