Approved; 01.06.2022

Requirements for the Handling of Confidential Information by Suppliers of the Central Statistical Bureau

It is important for the Central Statistical Bureau (Registration No LV90000069830), hereinafter referred to as the Customer, to ensure the continued confidentiality, integrity, availability and sustainability of information (including the personal data).

These requirements (hereinafter referred to as "the Requirements") shall be binding on anyone (hereinafter referred to as "the Supplier") who carries out, handles or is likely to handle Confidential Information under the control of the Customer access, directly or indirectly, including items (e.g. devices, equipment, furniture, belongings) containing Confidential Information in the performance of the Customer's task or otherwise cooperating with the Customer (hereinafter referred to as "the Service"), such as, but not limited to, by providing a service, carrying out construction work, supplying goods, cooperating under a contract, etc.

Confidential Information - for the purposes of the Requirements, means any information under the control of the Customer, including personal data to which the Supplier has or may have access (including but not limited to technical information, technology related information, system access data, information resources and their backup copies, personal data) in any form, including information systems and paper documents (hard copies), other than publicly available information.

The Customer has established Requirements to ensure that the Supplier complies with recommendation for international standards and 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 (General Data Protection Regulation) ("GDPR"), and other requirements laid down in laws, regulations and administrative provisions when processing the Confidential Information or accessing the Confidential Information.

The requirements shall apply to the extent that they are applicable without prejudice to the statutory sectoral specific regulations.

1. General Provisions

1.1. Supplier, a private person, certifies that:

1.1.1. he/she is a legal entity registered in a Member State of NATO, the European Union or the European Economic Area or is a natural person who is a national of the Republic of Latvia or a citizen of NATO, the European Union or the European Economic Area Member State;

1.1.2. this person is not subject to international or national sanctions or sanctions imposed by a Member State of the European Union or the North Atlantic Treaty Organisation which have a significant impact on the financial and capital market interests. The Supplier shall notify the Purchaser within two days of any circumstances which may give rise to the application of this Article.

1.2. In addition to the provisions of Article 1.1, the Supplier who provides external security controls for the Information Systems of the CSB shall certify that:

1.2.1. its employees involved in the security audit are citizens of NATO, European Union, European Economic Area countries or non-citizens of the Republic of Latvia;

1.2.2. the information obtained during the audit shall be processed only within the territory of NATO, European Union and European Economic Area Member States.

1.3. In addition to the requirements set out in Article 1.1, the Supplier outsourcing the maintenance of the Information Systems of the CSB or supplying services, software or equipment for the Information Systems of the CSB shall certify that:

1.3.1. that its beneficial owner is a national of a NATO, European Union, European Economic Area member State or a non-citizen of the Republic of Latvia;

1.3.2. the manufacturer of the software or equipment used to provide the service is a legal entity registered in a Member State of NATO, the European Union or the European Economic Area or a natural person who is a national of the Republic of Latvia or a citizen of a NATO, European Union or European Economic Area Member State.

2. Rights and Obligations

2.1. The Customer shall have the right to:

2.1.1. to monitor the quality of the service at all times. The person responsible for the Service shall be defined in the mutually concluded legal transaction

(e.g. the Contract);

2.1.2. to give instructions to the Service Provider on matters which are mandatory, relating to the integrity, quality, timeliness and regulatory compliance of the Service performance;

2.1.3. to make a reasoned written request to the Service Provider without delay to terminate the concluded legal transaction for the Service if the Customer has established that the Supplier fails to comply with the requirements of the legal transaction in respect of the scope or quality of the service.

2.2. **Obligations of the Supplier**

2.2.1. To enable the Customer to monitor the quality of the service at all times;

2.2.2. To respect the laws and regulations applicable in the Republic of Latvia (including the GDPR) applicable to the cooperation between the Supplier and the Customer, taking into account the nature and essence of such cooperation, the terms of the mutually concluded legal transaction, these Requirements, and to ensure that the Supplier and his or her activities comply with the foregoing;

2.2.3. To ensure the protection of Confidential Information in accordance with the procedures set out in these Requirements. In the event that the legal transaction concluded between the Supplier and the Customer contains classification of information, the Supplier is obliged to ensure the classification and protection of the information set out in the legal transaction (e.g. the Contract) in addition to these Requirements. The Supplier shall immediately inform the Customer in the event that the Supplier does not comply with the Requirements or is unable to comply with any of the instructions contained in the Requirements;

2.2.4. In the event of any change affecting or likely to affect the Supplier and its operations compliance with these Requirements, the Supplier shall promptly inform the Customer, prior to the changes mentioned above may affect the Supplier's operation or status;

2.2.5. At the request of the Customer, the Supplier shall review its compliance with these Requirements and provide the Customer with a written assessment of the Supplier's and his or her activities' compliance with these Requirements, or of any aspects of the Supplier or his or her activities that do not comply with these Requirements;

2.2.6. As soon as the Supplier becomes aware of a security incident involving Customer Information and/or Confidential Information, including a breach of the protection of personal data held by the Customer, without undue delay, but not later than 24 hours, notify the Customer and take all necessary measures to remedy the incident. This Requirement also applies to subcontractors;

2.2.7. As soon as such information becomes available, and without any delay, to inform or publish facts about disclosed vulnerabilities in the information and communication technology product or service supplied, the measures to remedy them and the deadlines for doing so;

2.2.8. To give information about the subcontractor and his or her compliance with these terms

and conditions and security Requirements set out in the concluded legal transaction;

2.2.9. During the term of the mutually concluded legal transaction, to promptly report any changes concerning the beneficial owner,

2.2.10. When developing a new data processing system for the Customer -

2.2.10.1. to ensure that the development process complies with the Customer's Security Policy Requirements. The Supplier shall request the Customer the information concerning the Security Policy Requirements;

2.2.10.2. To comply with the agreed system maintenance, support and warranty period (including system security vulnerability remediation);

2.2.10.3. To ensure the transfer of the source code of the system software and the rights to use it to the Customer, not later than the date specified in sub-paragraph 2.2.10.2 of these Requirements and after any changes or improvements to the system have been made;

2.2.10.4. To ensure that it is possible to continue, within the period specified in sub-paragraph 2.2.10.2 of these Requirements, to operate the system with the latest versions of the software (e.g. operating system, database management system, interpreter), required for the functioning of the system;

2.2.11. The Supplier shall comply with the following guidelines for the maintenance of the equipment:

2.2.11.1. to maintain the equipment in accordance with the manufacturer's recommended service intervals and specifications;

2.2.11.2. repairs and servicing of equipment shall be carried out only by authorised personnel;

2.2.11.3. to keep a record (logbook) of all breakdowns, preventive and maintenance work;

2.2.11.4. technical maintenance personnel shall be sufficiently identified: records containing the information about the persons carrying out the technical maintenance on the equipment shall be kept in a logbook;

2.2.11.5. to comply with the warranty conditions for the equipment;

2.2.12. to be familiar with the Customer's quality policy, available on its website: https://www.csp.gov.lv/lv/media/1253/download;

2.2.13. to be familiar with the Customer's privacy policy, available at: https://www.csp.gov.lv/lv/privatuma-politika.

2.3. The Customer shall have the right, in developing the handling and security requirements for Confidential Information unilaterally make changes to these Requirements once per calendar month by publishing the current version on the Customer's website on the first working day of the month at: https://www.csp.gov.lv/lv/informacijas-drosibas-pamatnostadnes. The Supplier and his or her subcontractor is obliged to consult the current version of this document before providing any service or supply within each calendar month.

3. Liability of the Supplier

3.1. The Supplier shall ensure and be able to demonstrate that, in the scope of his or her cooperation with the Customer, the Supplier's status, activities, processes and applicable means for processing the Confidential Information shall comply with the provisions of the laws and regulations applicable in the Republic of Latvia (including the GDPR) as well as the provisions of the mutually concluded legal transaction and the Requirements. For any non-compliance with the Requirements, the Supplier shall immediately inform the Customer.

3.2. The Supplier shall, at the request of the Customer, provide the Customer, within a period to be determined by the Customer, with the information and evidence requested by the Customer concerning the Supplier's and its activities' compliance with these Requirements, and shall provide the Customer with the opportunity to carry out the audit of the Supplier's information

management and processing, by enabling the Customer's representatives access to and inspect the documents substantiating the Supplier's and its activities' compliance with the requirements of the laws and regulations applicable in the Republic of Latvia (including the requirements of the GDPR), these Requirements and the requirements of the mutually concluded legal transaction, in accordance with the nature of the cooperation between the Customer and the Supplier. The Customer reserves the right, by agreement with the Supplier, to require an independent audit carried out by third party in order to assess the Supplier's information management and processing.

3.3. When performing technical tasks on the Customer's IT systems, the Supplier shall only use access methods and means specified by the Customer and shall act only in accordance with the procedures, specified by the Customer.

3.4. According to paragraph 16 of Cabinet Regulation No. 508 of 6 July 2021 "Procedures for the Identification of Critical Infrastructure, Including European Critical Infrastructure and Planning and Implementation of Security Measures" and paragraph 6 of Cabinet Regulation No. 100 of 1 February 2011 "Procedures for the Planning and Implementation of Security Measures for the Critical Infrastructure of Information Technologies", the Constitution Protection Bureau may examine the Suppliers' employees, members of the Board and owners who, during the performance of the Service, have access to information or technological equipment important for the functioning of Customer's infrastructure or who provide services important for the functioning of infrastructure.

4. Security Rules for Handling Confidential Information

4.1. The Supplier shall ensure that Confidential Information is not disclosed and is not accessible to any third party, other than the Supplier's subcontractor engaged in his or her duties in accordance with Clause 5 of these Requirements, and only to the extent necessary for the performance of his or her duties, and shall ensure the protection of that information against unauthorised access, accidental destruction or leakage.

4.2. The Supplier shall ensure that the Customer's infrastructure (IT systems, servers and/or other information processing sites and facilities) where Confidential Information is processed and stored, as well as the content of such information, shall not be accessible to any person, other than the Supplier and/or the Supplier's subcontractor and, as defined in Clause 5 of these Requirements, employees of the subcontractor to whom access is necessary for the performance of their direct duties and for the performance of the legal transaction concluded between the Supplier and the Customer. This applies both to physical and logical access (via information systems) and access to hard copy (paper) documents.

4.3. The Supplier has implemented and documented a process that enables the traceability of entities, who has accessed the Confidential Information and when. This applies to both physical and logical access (via information systems) and access to hard copy (paper) documents.

4.4. The Supplier shall ensure the technical protection of the Confidential Information by physical and logical means of protection.

4.5. The Supplier shall establish and control information management within its undertaking which shall, inter alia, include security requirements for the handling of the Confidential Information.

4.6. The Supplier shall be obliged, by the end of a term concerning a mutually agreed legal transaction (e.g. a contract) to delete the Confidential Information in his possession, unless the Customer has specified otherwise.

4.7. Confidential Information may only be stored in resources located exclusively in the territory of European Union or European Economic Area.

5. Management of Personnel

5.1. The Supplier shall have written agreements with all employees who have access to or handle in any way Confidential Information. In these agreements, an employee of the Supplier shall

undertake to ensure the confidentiality, integrity, availability and durability of the information and to keep the information confidential for an indefinite period of time, i.e. both during and after the termination of the employment relationship, in accordance with the laws, laws and regulations applicable in the Republic of Latvia, binding on the Supplier, including agreements concluded between the Supplier and the recipients of the Services provided by the Supplier.

5.2. The Supplier's employees involved in the provision of the Services to the Customer shall be trained in data protection and information security.

5.3. The Supplier shall ensure that its employees involved in the provision of the Services to the Customer are informed, aware of and shall comply with these Requirements, laws and regulations applicable in the Republic of Latvia (including the GDPR), applicable to the provision of the Service, the terms of the legal transaction between the Supplier and the Customer and the Customer's terms of use of information, infrastructure and systems.

5.4. The Supplier shall inform the Customer of any changes concerning the personnel, involved in the provision of services to the Customer and/or who work with the Customer's information.

5.5. The Supplier shall give information on the transfer of personal data to those of his or her employees involved in the performance of the Service whose data have been transferred to the Customer as part of the performance of the Service, specifying the purpose of the processing of the personal data, the types of data transferred, and informs that additional information on how the Customer will process the personal data received, and how he or she will respect the data protection and the rights of the data subject is available from the Customer.

6. Recruitment or Replacement of a Subcontractor

6.1. The Supplier shall have the right to engage a new subcontractor or to change an existing subcontractor only with the written consent of the Customer and subject to the requirements (if any) of the legal transaction between the Supplier and the Customer. Before recruitment of a subcontractor the Supplier shall provide the Customer with the information requested by the Customer, as well as submit a statement written by the subcontractor of compliance with these Requirements and the laws and regulations applicable in the Republic of Latvia (including the GDPR), and other requirements contained in the legal transaction concluded between the Supplier and the Customer.

6.2. The Supplier assumes full responsibility for the subcontractor, his or her activities and the personal data processing, and shall bear any losses incurred by the Customer as a result of the acts or omissions of such subcontractor.

6.3. The Supplier shall provide an audit of the subcontractor's information management and processing at the request of the Customer, within a mutually agreed time period between the Customer and the Supplier, as well as provide the Customer with the opportunity to carry out his or her own audit of the information management and processing performed by subcontractor, providing the Customer's representatives with the opportunity to access and familiarise themselves with the documents substantiating the subcontractor's and his or her activities' compliance with the laws and regulations applicable in the Republic of Latvia (including the GDPR), these Requirements and the requirements of the legal transaction concluded between the Supplier and the Customer. The Customer shall be responsible for all costs incurred in connection with audits requested by the Customer.

Acting Head of Information Security M. Deaks