Updated on 6 May 2026

REQUIREMENTS FOR PROVIDERS OF OUTSOURCED SERVICES

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

Terms used in this document and their definitions

Information and Communication Technology Resources, hereinafter referred to as the ICT Resources, means a set of technical and information resources. Examples include servers, computer networks, firewalls, data storage devices, workstations, active network equipment, and other elements of ICT infrastructure.

Technical Resource means hardware or equipment forming part of a network or information system or used to exchange data with an information system. It also includes software, such as operating systems, system files, system software, application software and utility programs.

Information Resource means a structured set of digital data processed electronically within an information system. Examples include databases, document repositories and register records.

Confidential Information for the purposes of these 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, information about technologies, system access data, resources and their backup copies, personal data) in any form, including information systems and paper documents (hard copies), other than publicly available information.

These requirements, hereinafter referred to as the Requirements, shall be binding on any supplier, hereinafter referred to as the Supplier, that, in the performance of tasks for the Customer or otherwise in cooperation with the Customer, including in the course of maintaining or developing information systems, processes Confidential Information under the control of the Customer and may gain direct or indirect access to Confidential Information or to items containing Confidential Information (e.g. information systems, devices, equipment, furniture, belongings). The service, hereinafter referred to as the Service, includes, but is not limited to, the provision or receipt of services, the supply of ICT Resources, outsourced services relating to ICT Resources, construction works, supply of goods, and cooperation under a contract, etc.

The Customer has established these Requirements to ensure that the Supplier complies with the requirements set out in recommendations contained in international standards, 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), hereinafter referred to as the GDPR, Law on International Sanctions and National Sanctions of the Republic of Latvia, National Cybersecurity Law, Cabinet Regulation No 397 of 2 July 2025 on the minimum cybersecurity requirements, and other laws and regulations.

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

1. GENERAL PROVISIONS

1.1 The Supplier, being a private individual, i.e. a natural person, a legal person governed by private law or an association of such persons, confirms that:

1.1.1 it is a legal entity registered in a Member State of North Atlantic Treaty Organization, hereinafter referred to as the NATO, the European Union, the European Free Trade Association, hereinafter referred to as the EFTA, or a NATO Indo-Pacific partner country, hereinafter referred to as an the IP4 country, or is a natural person who is a national of the Republic of Latvia or a citizen of a NATO, European Union, EFTA or IP4 country;

1.1.2 the management board and supervisory board of the Supplier, as a legal entity, consist of natural persons who are not citizens of the Russian Federation, the Republic of Belarus or a state recognised by the European Parliament or the Parliament of the Republic of Latvia as a state supporting terrorism;

1.1.3 it is not subject to international or national sanctions, or sanctions imposed by a Member State of the European Union or the NATO that materially affect financial and capital market interests. The Supplier shall notify the Customer within two days of any circumstances that may give rise to the application of this clause.

2. RIGHTS AND OBLIGATIONS

2.1 Rights of the Customer

2.1.1 The Customer shall the have right to continuously monitor the quality of the service provided or received. The person responsible for service supervision on behalf of the Customer shall be specified in the legal arrangement concluded between the parties (for example, in the Agreement) or in a notice issued by the Customer to the Supplier.

2.1.2 The Customer shall have the right to receive the information necessary for service supervision, including log files.

2.1.3 The Customer shall have the right to issue binding instructions to the Supplier or recipient in matters related to the ethical, high-quality, timely and legally compliant performance of the service.

2.1.4 If the Customer has established that the Supplier has failed to comply with the requirements set out in the legal arrangement regarding the scope or quality of the service, the Customer shall have the right to submit a justified written request to the Supplier or recipient for the immediate termination of the concluded legal arrangement (for example, the Agreement).

2.1.5 Pursuant to Paragraph 16 of Cabinet Regulation No 508 of 6 July 2021 on procedures for the identification of critical infrastructure, including European critical infrastructure, planning and implementation of security measures and business continuity, the Constitution Protection Bureau may verify employees, management board members and owners of the Supplier who, during the provision of the Service, have access to information or technological equipment significant for the functioning of the Customer’s infrastructure, or who provide services significant for the functioning of the infrastructure.

2.1.6 The Customer shall have the right to unilaterally amend these Requirements once per calendar month.

2.2 Obligations of the Supplier

2.2.1 The Supplier shall ensure that the Customer can continuously monitor the quality of the services provided or received.

2.2.2 The Supplier shall comply with the laws and regulations of the Republic of Latvia applicable to the cooperation between the Supplier and the Customer, as well as with the terms of the mutually concluded legal arrangement, these Requirements, and to ensure that its activities comply with the above requirements.

2.2.3 The Supplier shall ensure the protection of Confidential Information in accordance with the procedures set out in these Requirements. Where the legal arrangement concluded between the Supplier and the Customer contains information classification requirements, the Supplier shall, in addition to these Requirements, ensure the classification and protection of information specified in the legal arrangement (for example, the Agreement). The Supplier shall immediately notify the Customer if the Supplier does not comply with the Requirements or is unable to fulfil any of the requirements or instructions contained therein.

2.2.4 In the event of any changes affecting or potentially affecting the compliance of the Supplier or its activities with these Requirements, the Supplier shall immediately inform the Customer of such changes prior to their implementation and, upon the Customer's request, review its compliance with these Requirements and provide the Customer with a written assessment of the compliance of the Supplier or its activities with these Requirements or of any non-compliant aspects.

2.2.5 The Supplier shall provide information on subcontractors and their compliance with the security requirements set out in these Requirements and in the mutually concluded legal arrangement (for example, the Agreement).

2.2.6 The Supplier shall ensure that all provisions of the mutually concluded legal arrangements (for example, Agreements) and these Requirements apply to subcontractors.

2.2.7 During the term of the mutually concluded legal arrangement (for example, the Agreement), the Supplier shall notify the Customer of any change in the beneficial owner immediately.

2.2.8 Upon termination of the contract or at the Customer's request, the Supplier shall ensure the secure transfer or deletion of all Customer data used for the provision of the Service (for example, Customer data stored in an information system maintained by the Supplier).

2.2.9 The Supplier shall read the Customer's Privacy Policy available on the Customer's website: https://www.csp.gov.lv/en/privacy-policy.

2.2.10 The Supplier shall ensure that the Supplier and its subcontractor review the current version of this document prior to each service or delivery provided or received during the relevant calendar month. The current version is available on the Customer's website: https://www.csp.gov.lv/en/information-security-guidelines.

2.3 Obligations of the Supplier in the event of information security incidents and threats

2.3.1 As soon as the Supplier becomes aware of a security incident related to the information under the control of the Customer and/or a breach of the protection of Confidential Information, including information containing personal data under the

control of the Customer, the Supplier shall notify the Customer thereof without undue delay and no later than within 1 (one) hour, and to take all actions necessary to resolve the incident. This requirement shall also apply to subcontractors engaged by the Supplier.

2.3.2 In the event of an incident, the Supplier shall collect all information relating to the incident that may be useful for resolving and investigating it, and to provide such information to the Customer.

2.3.3 The Supplier shall inform the Customer of identified vulnerabilities in the supplied information and communication technology product or the service provided immediately upon becoming aware thereof, as well as of the measures and time frames for remedying such vulnerabilities.

2.4 Obligations of the Supplier in the development of a new information system for the Customer, implementation of changes to an existing information system, maintenance of an information system, or maintenance of ICT Resources

2.4.1 No later than upon conclusion of the contract for the development of an information system, implementation of changes to an existing information system, maintenance of an information system or maintenance of ICT Resources, the Supplier shall submit to the Customer a list of the natural persons involved in the provision of the outsourced service, together with an explanation of the involvement of each person in the performance of the outsourcing contract. The Supplier shall inform the Customer of any changes to the natural persons involved in the provision of the outsourced service during the term of the contract.

2.4.2 The Supplier shall not permit natural persons to perform the Service unless such persons have been approved in writing by the Customer in accordance with Subparagraph 2.4.1 of these Requirements.

2.4.3 The Supplier shall ensure the recovery point objective (RPO) and recovery time objective (RTO) specified in the legal arrangement (for example, the Agreement).

2.4.4 The Supplier shall retain machine-readable log records meeting the respective security class of the information system for which the outsourced service is provided. The retention period for log records shall be determined according to the security class of the information system: 18 months for Class A information systems, 12 months for Class B information systems, and 6 months for Class C information systems.

2.4.5 The Supplier shall ensure that backup copies of the information system are accessible, both physically and electronically, to persons authorised by the Customer.

2.4.6 The Supplier shall ensure that the requirements set out in the Customer’s Cybersecurity Policy are complied with during the development process. The Supplier shall request access to the contents of the Cybersecurity Policy necessary for the provision of the Service from the Customer.

2.4.7 The Supplier shall ensure that only synthetic data are used in the test environment of information systems with Class A and Class B confidentiality classification.

2.4.8 The Supplier shall ensure that the provision of the Service for information systems with Class A or Class B confidentiality classification is not carried out in the production environment of the respective information system.

2.4.9 The Supplier shall ensure that the source code of the system and the related rights of use are transferred to the Customer no later than by the deadline specified in the legal

arrangement (for example, the Agreement), as well as after each modification or improvement made to the system.

2.4.10 The Supplier shall ensure continued operation of the system using the latest versions of the software required for the functioning of the system (for example, the operating system, database management system, or scripting interpreter).

2.5 Obligations of the Supplier in carrying out maintenance of equipment, including ICT Resources

2.5.1 The Supplier shall maintain equipment in accordance with the service intervals and specifications recommended by the manufacturer.

2.5.2 The Supplier shall ensure that repair and servicing work is carried out only by authorised personnel.

2.5.3 The Supplier shall maintain records (logbooks) of all faults and all preventive and corrective maintenance activities.

2.5.4 The Supplier shall properly identify personnel performing technical maintenance and ensure that records of persons performing technical maintenance of equipment are maintained in a logbook.

2.5.5 The Supplier shall comply with the warranty conditions applicable to the equipment.

2.6 Obligations of the Supplier when processing personal data available to the Customer

2.6.1 The Supplier shall process personal data only in cases and to the extent necessary for the provision of the Service.

2.6.2 The Supplier shall not use personal data available to the Supplier for purposes unrelated to the Service or otherwise than in accordance with the written instructions of the Customer, unless otherwise required by law.

2.6.3 The Supplier shall ensure and maintain confidentiality, integrity, availability and resilience of the personal data being processed.

2.6.4 The Supplier shall comply with the technical and organisational data protection requirements laid down in applicable legislation. When selecting technical and organisational measures for the protection of personal data, the Supplier shall ensure protection against threats to personal data caused by physical impact as well as protection implemented through software tools, passwords, encryption and other logical protection measures.

2.6.5 The Supplier shall ensure that employees authorised to process personal data have undertaken confidentiality obligations and undertake not to retain or unlawfully disclose personal data transferred by the Customer to the Supplier, including after termination of employment or civil service relationships.

2.6.6 The Supplier shall maintain a register of personal data processing activities and provide it to the Customer within three working days following a justified request from the Customer.

2.6.7 The Supplier shall inform the Customer about any data subject request concerning personal data processing or the exercise of data subject rights within three working days of receiving such request and shall, where possible, assist the Customer through appropriate technical and organisational measures in responding to such request. The

Supplier shall not respond directly to the data subject unless authorised by the Customer.

2.6.8 The Supplier shall inform the Customer of a data incident (an event or act related to a personal data breach, as well as any other harmful event or act compromising the integrity, availability, confidentiality or resilience of personal data) no later than within one hour of becoming aware of the incident. Where possible, the Supplier shall assist the Customer in recording personal data breaches, investigating incidents, mitigating their consequences, and notifying the supervisory authority or the data subject, insofar as this relates to information containing personal data available to the Supplier.

2.6.9 In cases provided for by law, the Supplier shall transfer personal data to public authorities or law enforcement authorities upon request, and the Customer shall be informed thereof within three working days following such transfer, unless such notification is prohibited by law.

2.6.10 The Supplier shall not transfer data to a third country or international organisation without the Customer's prior written consent.

2.6.11 Upon fulfilment of the obligations relating to the Service, the Supplier shall transfer all personal data to the Customer and delete any copies containing personal data and shall provide the Customer with confirmation that this has been done where the legal basis for processing no longer exist and applicable legislation does not require retention of the relevant personal data.

2.6.12 Taking into account the nature of the personal data processing and the information available to the Supplier, the Supplier shall, where possible, provide recommendations to assist the Customer in carrying out a personal data protection impact assessment.

2.6.13 The Supplier shall provide the Customer with the information necessary for carrying out an audit or inspection relating to the fulfilment of obligations arising from the Service.

2.6.14 The Supplier shall store the documents containing personal data in compliance with the requirements of applicable legislation.

2.6.15 The Supplier shall grant the Customer access, in the presence of the Supplier, to the territory and premises used for personal data processing in order to inspect the relevant processing activities. The Supplier shall immediately inform the Customer if the Data State Inspectorate initiates or plans to initiate an inspection relating to the processing of personal data under the control of the Customer within the Supplier's territory, premises and/or information systems.

2.6.16 In the event of a physical or technical incident, the Supplier shall restore the availability of and access to personal data as quickly as possible.

2.6.17 Where necessary, the Supplier shall develop a process for regular testing, assessment and evaluation of the effectiveness of technical and organisational measures in order to ensure the security of processing.

2.6.18 Taking into account the nature of the processing and the information available to the Supplier, the Supplier shall provide assistance to the Customer in ensuring compliance with the obligations referred to in Articles 32 to 36 of the GDPR.

2.6.19 In cases specified in Article 37 of the GDPR, the Supplier shall appoint a data protection officer.

2.7 Obligations of the Supplier regarding the secure processing of Confidential Information

2.7.1 The Supplier shall ensure that Confidential Information is not disclosed or made available to any third party, except to subcontractors engaged by the Supplier in accordance with Section 4 of these Requirements and only to the extent necessary for the performance of their duties. The Supplier shall also ensure protection of such information against unauthorised access, accidental destruction, or leakage.

2.7.2 The Supplier shall ensure that no person other than the Supplier and/or employees of subcontractors engaged by the Supplier in accordance with Section 4 of these Requirements gains access to the Customer's infrastructure (IT systems, servers and/or other locations and objects where information is processed or stored), or to the contents of Confidential Information processed therein, unless such access is necessary for the performance of direct duties and fulfilment of the legal arrangement concluded between the Supplier and the Customer. This shall apply to physical access, logical access (through information systems) and access to documents in paper form.

2.7.3 The Supplier shall implement procedures ensuring the tracking and identification of persons who have accessed Confidential Information and shall maintain records of such access, including the time of access. This shall apply to physical access, logical access (through information systems) and access to documents in paper form;

2.7.4 The Supplier shall ensure technical protection of Confidential Information through physical and logical security measures.

2.7.5 The Supplier shall establish and supervise information management within its organisation, including, inter alia, security requirements for the processing of Confidential Information.

2.7.6 Upon expiry of the mutually concluded legal arrangement (for example, the Agreement), the Supplier shall delete all Confidential Information that has come into its possession, unless otherwise specified by the Customer.

2.7.7 The Supplier shall ensure that Confidential Information, including backup copies, is processed and stored only on resources located within the territory of the European Union or the European Economic Area.

3. PERSONNEL MANAGEMENT MATTERS

3.1 The Supplier shall conclude written agreements with all employees who may access or process Confidential Information in any manner. Under such agreements and in accordance with the laws and regulations of the Republic of Latvia binding upon the Supplier and other applicable regulatory or legal acts, including agreements concluded between the Supplier and recipients of the services provided by the Supplier, the employees of the Supplier shall undertake to ensure the confidentiality, integrity, availability and resilience of information and not to disclose the information obtained for an indefinite period of time, i.e. both during the employment relationship and after its termination.

3.2 The Supplier shall ensure that employees involved in the provision of Services to, or their receipt from, the Customer are trained in data protection and information security matters.

3.3 The Supplier shall ensure that employees involved in the provision of Services to, or their receipt from, the Customer are informed of, understand and comply with these Requirements, the laws and regulations of the Republic of Latvia applicable to the provision of the Service (including the GDPR), the terms of the legal arrangement (concluded between

the Supplier and the Customer, and the information, infrastructure and system usage rules established by the Customer.

3.4 The Supplier shall inform the Customer of changes in personnel engaged in the provision of Services for the Customer and/or working with information under the control of the Customer.

3.5 The Supplier shall inform employees involved in the provision of the Service about the transfer of their personal data to the Customer for the purposes of Service provision, specifying the purpose of the processing, the categories of data transferred, and informing them that additional information regarding how the Customer processes the personal data received, ensures data protection and respects the rights of the data subject is available from the Customer.

4. ENGAGEMENT AND REPLACEMENT OF SUBCONTRACTORS

4.1 The Supplier shall have the right to engage a new subcontractor or replace a subcontractor only after obtaining written consent from the Customer and in compliance with the requirements of a legal arrangement concluded between the Supplier and the Customer (for example, the Agreement) if such requirements are stipulated therein. Prior to engaging a subcontractor, the Supplier shall provide the Customer with the information requested by the Customer, as well as a confirmation from the subcontractor regarding compliance with these Requirements, the requirements of the laws and regulations applicable in the Republic of Latvia (including the GDPR), and other requirements contained in a legal arrangement concluded between the Supplier and the Customer (for example, the Agreement).

4.2 The Supplier shall assume full responsibility for the subcontractor, its activities, and the personal data processing carried out thereby, and shall compensate the Customer for any losses incurred as a result of the actions or omissions of such subcontractor.

4.3 Upon a request from the Customer, the Supplier shall ensure that an audit/review of how the subcontractor manages and processes information is carried out within a period mutually agreed between the Customer and the Supplier. The Supplier shall also ensure that the Customer is able to carry out its own audit/review of the information management and processing practices employed by the subcontractor. For this purpose, the Supplier shall provide the Customer's representatives with access to documents evidencing compliance of the subcontractor and its activities with the laws and regulations applicable in the Republic of Latvia (including the GDPR), these Requirements and the legal arrangement concluded between the Supplier and the Customer (for example, the Agreement). The Customer shall be responsible for all costs arising in connection with audits requested by the Customer.

5. FINAL PROVISIONS

5.1 If these Requirements conflict with the terms of mutually concluded legal arrangement (for example, the Agreement), the provisions which, as determined by the Customer, ensure a higher level of protection of information and personal data shall prevail.