To the Special Part of the Contract for the Public Procurement-Sale of Services

Annex No. 7

**ARRANGEMENT ON APPLICABLE ORGANISATIONAL AND TECHNICAL**

**CYBER SECURITY REQUIREMENTS**

When performing the Contract for the Public Procurement-Sale of Services (hereinafter referred to as the Contract), the Provider shall be obliged to ensure an adequate level of data security, i.e. the constant confidentiality, integrity, availability of the personal data processed and resilience of the data processing IT systems, and to make appropriate decisions on the use of technical and organisational security measures for this purpose. If the Provider serves a critical information and communication technology (hereinafter referred to as the ICT) infrastructure, or provides other essential services in Lithuania provided for in Annex 1 to the Law on Cyber Security of the Republic of Lithuania, it shall comply with the provisions of the Cyber Security Requirements approved by Resolution No 818 of the Government of the Republic of Lithuania of 13 August 2018 On the Implementation of the Law on Cyber Security of the Republic of Lithuania applicable to the central cyber security entity. In the case of a foreign Provider who processes the data transferred to it outside the ICT infrastructure of the State Enterprise Centre of Registers (hereinafter referred to as the Centre of Registers), the requirements of international standards such as ISO/IEC 27001 or equivalent standards (NIST CSF, SOC 2, etc.) shall be complied with.

The Provider undertakes to ensure the implementation of the following organisational and technical cyber security requirements:

|  |  |
| --- | --- |
| 1. Organisational security measures for data processing | * 1. Upon conclusion of the Contract, the employees appointed by the Provider who will provide services under this Contract and connect to the ICT infrastructure of the Centre of Registers shall be required to read through the Cyber Security Policy adopted by the Information Resource Manager and the implementing legislation, and to comply with the established requirements. In cases where the Provider is transferred to process the data of the Centre of Registers in its (Provider’s) infrastructure, the Provider must comply with the information and/or cyber security policy adopted by the Provider’s organisation.   2. Maintain the confidentiality of information transmitted, stored or otherwise processed throughout the term of the Contract and thereafter, and to undertake in writing to protect such information prior to the commencement of such processing.   3. Ensure the security of the login data received and not to disclose it to third parties.   4. Grant, modify and/or revoke user rights on a need-to-know principle, or ensure that access to information is limited to execution of specific functions (carrying out work) and/or for a specific period.   5. The Provider shall apply appropriate and adequate procedures for granting of rights or lifting of obligations, transfer or assignment of roles and responsibilities in the event of dismissal and change of their functions within its organisation.   6. The Provider must ensure that providers (sub-providers) involved comply with the same information and cyber security requirements.   7. The Provider shall immediately inform the Centre of Registers of the termination of employment relationship with the employee of the organisation who has been granted access to the information processed in the ICT infrastructure of the Centre of Registers.   8. The Provider shall have the obligation to immediately inform about any major and/or other electronic information security incidents observed in the information technology infrastructure of the Centre of Registers during the performance of the Contract, non-functioning or improperly functioning security measures, non-compliance with information security requirements, signs of criminal activity, detected security gaps (vulnerabilities) that pose a risk to the networks and information systems of the cyber security entity and other important safety events. It shall also inform the Centre of Registers, but not later than within 24 hours, when the said cases have been identified in the information systems infrastructure managed by the Provider, which affect the data processed by the Centre of Registers. It shall provide the cyber security entity with a report on the investigation of a cyber incident when the investigation is completed.   9. The Provider shall be responsible for facilitating a cyber security entity or its authorised service providers to carry out a Provider’s compliance audit (including an unplanned one) during the Contract period or in the event of a major incident.   10. Perform the *Service level Agreement*, SLA.   11. Use only legal software. |
| 2. Technical security measures for data processing | 1. An access control system shall be in place and implemented, which is applicable to all users of the IT system. The access control system must allow the creation, validation, review and deletion of user accounts. 2. The use of shared user accounts shall be avoided. Where a shared user account is necessary, all users of the shared account shall have the same rights and obligations. 3. An authentication mechanism must be in place allowing access to the IT system. The minimum requirement for the user to log in to the IT system shall be a username and a password. The password shall be created according to a certain level of complexity. The password must consist of letters, numbers and special characters; the personal information (such as date of birth, family names, etc.) must not be used for passwords. The user password must consist of at least 10 characters, which must be changed at least every six months; and the administrator password must consist of at least 15 characters, which must be changed at least every six months. The security of the login data must be ensured. All measures must be taken to prevent login names and passwords becoming known to third parties. 4. The password must be prohibited from being stored in the computer workstation or its software. 5. The access control system must be able to detect and prevent the use of passwords that do not meet a certain level of complexity. 6. Technical logs must be implemented for each IT system, which is used to process personal data under the Contract. Technical logs shall contain all possible information on access to personal data (e.g. date, time, review, modification, cancellation). The retention period shall be at least 6 months. Technical logs shall bear time stamps and shall be protected against possible tampering, falsification or unauthorized access. Time-keeping mechanisms used in IT systems shall be synchronised according to the common time reference source. 7. Protection of computer workstations used for data processing under the Arrangement:    * 1. Users of workplaces may not be able to disable or bypass and avoid IT system security settings;      2. Users may not have privileges (rights) to install, remove, administer unauthorised software;      3. After work is completed, or when leaving the workplace, the network and information systems must be disconnected, the screen saver with a password must be activated.      4. Critical security updates for the operating system of computer workstations must be installed regularly and immediately;      5. Anti-virus applications and their databases of information about viruses and malware must be updated at least once a day;      6. Where access to the IT systems used for processing data under the Arrangement is provided via the Internet, data must be encrypted using Virtual Private Network (VPN) technology with TLS/SSL certificate, or using *Access Point Name* (APN) technology, applying streaming data encryption with TLS/SSL certificate when VPN technology is not supported by mobile devices.      7. Wireless connection to IT systems must be allowed only for certain users and processes. The wireless subnet shall be separated from other subnets. Wireless communication must be encrypted in accordance with the encryption length key recommended by good security practices. Use keys and protocol versions, which are generally acknowledged as secure. The standard manufacturer keys must be changed in the wireless access point.      8. Mobile and portable devices to be used for work with information systems must be registered and authorised before their use.      9. Mobile, portable devices must have a sufficient level of access control procedures, as well as other equipment used to process personal data; 8. The confidentiality of sensitive information transmitted to a cyber security entity through public electronic communications networks must be ensured through encryption and must be protected by passwords. 9. Network and information system data stored on mobile devices and external computer media must be encrypted. Encrypt data at the hard disk level. 10. Before removing any data medium, all data contained therein must be destroyed using a dedicated software that supports reliable data destruction algorithms. If this is not possible (e.g. USB, DVD media), the data media must be destroyed physically without the possibility of restoring it, e.g. using shredders or other mechanical means. 11. Physical protection of the environment and premises with IT system infrastructure from unauthorised access must be implemented. |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_