**Security requirements for Providers of consulting and advisory services**

**Introductory provisions**

For the purpose of this attachment to the Agreement, the following abbreviations and terms are used:

|  |  |
| --- | --- |
| **Act or** **CSA** | Act No. 181/2014 Coll., concerning Cyber security and change of related laws (Cyber Security Act), in the wording of later regulations |
| **CSD** | Decree No. 82/2018 Coll. on security measures, cybersecurity incidents, reactive measures, particulars of filings concerning cybersecurity, and disposal of data (Cybersecurity Decree), as amended. |
| **Regulation** | Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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) |
| **Personal information** | All information about an identified or identifiable physical person (such as name, identification number, location data, network identifier, or one or more specific physical, physiological, genetic, economic, cultural or social identity of that individual). |
| **Personal information processing** | Any operation or set of operations that is performed with personal data or personal data files, such as collecting, recording, organizing, structuring, storing, customizing or modifying, retrieving, viewing, using, making available through transmission, dissemination or any other disclosure, alignment or combination, restriction, erasure or destruction. |
| **Date of the agreement conclusion** | Date of the conclusion of this agreement or the date of integration of said Security requirements into the agreement through the appendix of this agreement. |
| **Individual prom the Provider’s party** | A physical individual participating in the fulfillment of the contract and having a labor or similar contract relationship with the Provider or their sub-providers |
| **Classification scheme** | Classification scheme specifying handling data and information of UJV Group in paper and electronic form. |
| **Consumer’s environment** | Physical perimeter specified by the physical space in rent or property of the Consumer or a logical perimeter defined by the network elements in the administration or the property of the Consumer. |

# Purpose

1. Define the Security Requirements for providers of consulting and advisory services, if the Provider accesses the Consumer´s Information within this context. If the Provider uses a subcontractor in providing the subject of performance, it is obliged to ensure adequate compliance with these Security Requirements also in contractual relations with its subcontractors.
2. Assure Consumer´s information security, with which the Provider becomes acquainted during the negotiations and subsequent performance of the contract.

# Security Requirements

1. The Provider acknowledges, that the Consumer has established the Information Security Management System according to ISO/IEC 27001 and is a subject according to § 3 paragraph c) and d), eventually f) and g) of the Act 181/2018 Coll. and is obliged to meet the requirements of the related legislation.

### **Information Security Management System**

1. The Provider will actively participate, according to the terms and conditions of the contract, in observing, operating and developing security measures. The Provider is, at least, bound to:
2. Implement security principles and processes, which will cover the data and information security, that can be created and processed on by the Consumer when providing the subject of performance.
3. Manage their own risks that can affect the provision of the subject of performance.
4. Based on security needs and risk evaluation results, implement appropriate security measures within the scope of the provided subject of performance, monitor them and evaluate their effectiveness.
5. Create and approve a security policy that will cover the data and information security that may be created and processed by the Provider in providing the subject of performance.
6. Establish and maintain current security measures in the form of processes and technological means that ensure compliance with the security policy.
7. Ensure the safe operation of the information system and infrastructure used to provide the subject of performance.
8. Ensure the collection of information on operational and safety activities within the scope of the subject of performance and the protection of the information obtained against its unauthorized reading or change.
9. Upon request, provide the Consumer with an overview, report or other adequate information on security measures implemented in its information system and infrastructure.

### **Access to Consumer´s information**

1. All available information remains the Consumer property and the Provider is entitled to use this information only for the purposes of fulfilling the subject of performance.
2. The Provider is, at least, bound to:
3. Communicate the Consumer´s information only to their employees or cooperating persons who necessarily need to know the information for the purposes of performance of this contract, are simultaneously bound to confidentiality and have been acquainted with these security requirements.
4. Not to misuse the Consumer´s information for a purpose other than the subject of performance, not to handle information contrary to the Consumer´s legitimate interests.
5. Secure the Consumer´s information against the access of unauthorized third parties by taking the necessary technical and organizational measures to prevent unauthorized or accidental access to the Consumer´s information, its destruction or loss, or unauthorized usage.
6. Make copies of the Consumer´s information only in necessary cases.
7. Protect all information provided by the Consumer by appropriate encryption and against unauthorized access, especially on mobile devices.
8. After the termination of the performance of the contract, without undue delay, dissolve all Consumer´s information and data which were handed over in connection with performance of the contract.
9. In case when Provider accesses the Consumer´s ICT system:
10. The Provider acknowledges, that the access to the ICT system of UJV Group companies can be allowed only to the physical identity of the Provider´s / subcontractor´s employee, verified by an identity document and with the generated unique identifier for ICT system access and registered in the registry of identities, based on the Provider´s request for access. For registration in the identity register, it is necessary to disclose these personal data to the Provider´s employee:
11. Name (Identity register)
12. Last name (Identity register)
13. Maiden name (Identity register)
14. Gender (only for verification purposes, without registration in the Identity Register)
15. Date of birth (Identity register)
16. Personal Identification Number (only for verification purposes, without registration in the Identity Register, we do not store PIN in the system, we do not require it to be sent or recorded in the form, but it is required for the verification of physical identity to generate the unique identifier, physical identity communicates it at the moment of verification. In case of person´s disagreement, verification is carried out based on the date of birth and other personal data).
17. Email (Identity register)
18. Mobile phone or landline (Identity Register)
19. The Provider acknowledges informing the employees and subcontractors, to whom the access (physical, logical) to the ICT system will be assigned, the manner of processing their personal data.
20. The Provider acknowledges that authorization assigning to the Provider´s employee must be controlled by the principle of least privilege and is not claimable.
21. The Provider acknowledges that the activities of users accessing the Client’s information systems using privileged user accounts may be monitored and recorded for the purposes of security auditing, investigation of security incidents, and ensuring compliance with the Client’s internal security policies.
22. The user is clearly informed at the start of each session that their activity is being actively recorded.
23. The Provider undertakes to inform all relevant persons (e.g., employees, subcontractors, partners) who will participate in the performance of this agreement and access the aforementioned systems of the possibility of such monitoring and recording.
24. The Provider acknowledges that in case of unsuccessful attempts to authorize a user (an individual from Provider´s party), the respective account can be blocked and treated as a security incident and measures for security incident management can be applied (e.g.: immediate cancellation of access to the information assets).

### **Security of data and information transfer**

1. For the purposes of data and information transfer, a Contact Person must be assigned (appointed) on both sides, who is authorized to perform data and information transfer. Secure data and information transfer options are:
2. Encrypted email communication ([MIP](https://www.microsoft.com/cs-cz/security/business/information-protection), [S/MIME](https://cs.wikipedia.org/wiki/S/MIME) or zip with password);
3. Data storage of the UJV Group with controlled external access;
4. Encrypted portable device secured by PIN (USB flash disc);
5. Transmission of printed information (in person / by mail);
6. Data box;
7. Secure section for suppliers on the portals of UJV Group companies.

### **Security Events and Incidents Management**

1. The Provider is, at least, bound to:
2. Without unnecessary delay, report all security events and incidents with potential negative impact to the Consumer through a specified communication channel or through the Contact Person.
3. In case of security event and following treatment and evaluation of the security incident, and/or in case of suspicion of a security incident, provide the Consumer with the relevant information concerning an identified suspicious device or individual from the Provider´s party.
4. Without unnecessary delay, and after agreement with the Consumer, implement measures requested by the Consumer within the agreed terms in order to reduce the impact of a security incident or prevent the continuation of the incident, that can make an impact to the Customer.
5. Co-operate in the analysis of the causes of security incident and suggest measures with the intention to prevent its recurrence in case the security incident was caused by the Provider, or the Provider participated in its origin.
6. The Provider acknowledges that the process of security incidents management, or other consequential breach of the Security Requirements, caused by the Provider will not be considered as a circumstance excluding the responsibility of the Provider for delaying the fulfilment of the terms and conditions of the contract and will not be a basis for a compensation of any kind in case of damage to the Provider or any other individual from the Consumer´s party. Other provisions concerning the accountability of the Provider for extensions included in the contract are not influenced by the provision.