**Corporate Information Security and Data Protection Clause**

**(Valid as of: 01.09.2016)**

1. Supplier shall maintain strict secrecy concerning all information made available in the course of the performance of the contractual relationship between Slovak Telekom, a.s and the Supplier (hereinafter only “Cooperation”) and shall not exploit or make available to third parties such information. This shall relate to all technical, financial or other information (hereinafter only the “Confidential Information”) of which the Supplier becomes aware of within the Cooperation, irrespective of whether the Confidential Information is declared as confidential. The obligation to maintain confidentiality endures also after the cessation of the Cooperation.
2. Supplier shall not have any access to and shall not obtain:

1. any personal data of Slovak Telekom, a.s according to the Act No. 122/2013 Coll. on Personal Data Protection as later amended, and

2. any data, which are subject of telecommunications privacy according to Act No. 351/2011 Coll. on Electronic Communications as later amended.

1. Slovak Telekom, a.s will take all necessary and reasonable measures not to allow and/or to actively deny such an access. Supplier undertakes not to evade any of these measures securing the access deny to the data defined in this point. In case that the Supplier obtains for any reason an access to the data defined in this point, Supplier shall inform Slovak Telekom, a.s without undue delay about such a situation and give Slovak Telekom, a.s all details about the obtained data.
2. Supplier is obliged to delegate an employee as a single point of contact for dealing with information security issues, providing of information, cooperation in information security and data protection area (hereinafter only the “Information security officer”).
3. Information security officer of the Supplier is responsible to ask Slovak Telekom, a.s (project manager, internal client or person authorized by them) for specification of relevant security directives and security requirements.
4. Supplier undertakes to adopt and maintain appropriate technical, organizational, personal or other measures as may be necessary to maintain confidentiality, availability and integrity of Confidential Information that have or will be disclosed or made accessible to it by Slovak Telekom, a.s or its contractual partners. If specification of Slovak Telekom, a.s. according to point e) not stated otherwise, measures of ISO 27001 and measures as specified in Annex 1 (Security measures and requirements) of this document are to be implemented.
5. Supplier is allowed to use Confidential Information solely for the purposes Cooperation and following its termination, the Supplier shall not use Confidential Information for any purpose without limitation of time. At the same time, the Supplier shall not disclose any Confidential Information to any third party without limitation of time, unless expressly written agreed with Slovak Telekom, a.s..
6. Supplier is allowed, to contract out services to a subcontractor only after Slovak Telekom´s explicit approval. Supplier is obliged to shift all requirements defined in this document on all subcontractors providing services on behalf of the Supplier. Subcontractors are not allowed to have any other subcontractors.
7. Supplier shall ensure, that only the designated personnel of the Supplier who absolutely need to know the Confidential Information in order to perform Cooperation activities, shall have the access to the Confidential Information provided by Slovak Telekom, a.s. or its contractual partners.
8. Supplier undertakes, that its employees, personnel, and persons and its subcontractors (hereinafter only the “Authorized persons”) shall observe valid organisational and technical security measures of Slovak Telekom, a.s regulating access and movement of persons and vehicles in the premises and buildings of the Slovak Telekom, a.s..
9. Slovak Telekom, a.s (project manager, internal client or person authorized by them) shall be responsible for acquaintance of the Supplier with entry permission request, handover of the identification tools and keys determined for Authorized persons.
10. Supplier undertakes that the Authorized persons will not allow the access to the premises of Slovak Telekom, a.s to persons not having valid permission to entry the premises and buildings of Slovak Telekom, a.s..
11. Supplier undertakes, that all identification tools and keys of Authorized persons to entry the premises and buildings of Slovak Telekom, a.s will be hand over back to Slovak Telekom, a.s immediately after the respective Authorised person is not more providing services to Slovak Telekom, at latest before the termination of the Cooperation.
12. Access of Authorised persons and authentication means to the systems of Slovak Telekom, a.s are provided to the Authorised persons based on request addressed to Slovak Telekom, a.s (project manager, internal client or person authorized by them).
13. Supplier is obliged to consistently ensure the protection of confidentiality and integrity of the authentication means (e.g. user ID, password, OTP, token, smart card, etc.) into the electronic systems of Slovak Telekom, a.s made available and provided to the Supplier and not to make them accessible or not to let their accessing to unauthorized persons.
14. Supplier undertakes that all authentication means to the systems of Slovak Telekom, a.s will be hand over back to Slovak Telekom, a.s immediately after the respective Authorised person is not more providing services to Slovak Telekom, at latest before the termination of the Cooperation. Supplier undertakes to pay Slovak Telekom, a.s. compensation for loss of the authentication means. Authorised persons are obliged to notify immediately Slovak Telekom, a.s on damage, loss or theft of the authentication means via Security Management Center, the contact details: e-mail address: smc@telekom.sk, telephone: 0800 100 166.
15. Supplier shall be obliged to always inform Slovak Telekom, a.s if any of the Authorised persons entitled to enter electronic systems of Slovak Telekom, a.s terminated its relationship with the Supplier (e.g. termination of the employment or other contractual relationship, termination of office, termination of the membership in any body of the Supplier, etc.).
16. Supplier undertakes that the Authorized persons shall use established security mechanisms in accordance with the guidelines and shall not perform any activities to violate or damage them. Authorized persons shall carry a visibly placed visit identity card and shall be accompanied with the responsible employee of Slovak Telekom.
17. Supplier shall notify the Authorized persons that Slovak Telekom, a.s monitors the assets (premises by a CCTV system, application/technologies by logs auditing system) in order to reach the requested standard of the security. Records and logs are stored in central monitoring and archiving system.
18. Transfer of Confidential Information between Supplier and Slovak Telekom, a.s must be performed end to end encrypted if electronic form is used. Information security officer of the Supplier is responsible to ask Slovak Telekom, a.s (project manager, internal client or person authorized by them) for specification of security requirements.
19. Supplier undertakes to have business continuity plans and disaster recovery plans in place to be able to provide continuous services to Slovak Telekom, a.s in case of nonstandard situations. Supplier shall regularly update and exercise these plans. Supplier is obliged to provide support to Slovak Telekom, a.s when preparing or exercising business continuity plans of Slovak Telekom.
20. Supplier is obliged to report any nonstandard situations, suspicious events or security incidents to Security Management Center of Slovak Telekom, a.s. Supplier undertakes to put the best effort within Cooperation with Slovak Telekom, a.s to prevent continuation of the security incident, to eliminate the consequences of the security incident, to prevent from other security incidents and also to ensure and restore all measures necessary for the protection of Confidential Information of Slovak Telekom.
21. Supplier is obliged to provide cooperation to Slovak Telekom, a.s staff, or delegated third party staff, when performing controls, audits on observing the security measures set out in this document or when performing risk analysis. Slovak Telekom, a.s is entitled to perform these activities randomly. Supplier is obliged to provide any evidence, documents, access to premises, systems connected or used for providing of services. Supplier undertakes to provide Cooperation in implementation of corrective measures to findings of the controls.
22. In case of breach of the obligations pursuant to this document Slovak Telekom, a.s. shall be entitled to claim the contractual penalty towards Supplier in the amount of 10 000 € (in words: ten thousands EUR) for each particular breach. Claim on compensation for damages exceeding the contractual penalty is not affected by payment of the contractual penalty.

Annex 1: Security measures and requirements

