Agreement on Contract Data Processing

Zmluva o spracúvaní osobných údajov

uzatvorená medzi

Business Name/Obchodné Meno:	**Mobis Slovakia s.r.o.**
Registered Seat/Sídlo:	MOBIS ulica 1, Gbeľany 013 02, Slovak Republic/ Slovenská republika
ID No/IČO:	
Registered with/Zápis v:	Business Register of District Court Žilina, Section Sro, Insert No 14983/L / Obchodný register Okresného súdu Žilina, oddiel Sro, vložka č. 14983 /L
Represented by/ Zast.:	Younghwa Kim, CEO / konateľ

and / *a*

Business Name/Obchodné Meno:	**Stredná odborná škola elektrotechnická**
Registered Seat/Sídlo:	Komenského 50, 010 01 Žilina
ID No/IČO:	
Represented by/ Zast.:	Ing. Ľubomír Králik, riaditeľ/director

CONTENTS / OBSAH

CLAUSE / ČLÁNOK PAGE / STRANA

AGREEMENT ON CONTRACT DATA PROCESSING
ZMLUVA O SPRACÚVANÍ OSOBNÝCH ÚDAJOV

Between
Uzatvorená medzi

(1)

Business Name/Obchodné Meno:	**Mobis Slovakia s.r.o.**
Registered Seat/Sídlo:	MOBIS ulica 1, Gbeľany 013 02, Slovak Republic/ Slovenská republika
ID No/IČO:	
Registered with/Zápis v:	Business Register of District Court Žilina, Section Sro, Insert No 14983/L / Obchodný register Okresného súdu Žilina, oddiel Sro, vložka č. 14983 /L
Represented by/ Zast.:	Younghwa Kim, CEO / konateľ

hereinafter referred to as **„Company"** and also as **„controller" /** ďalej len ***„Spoločnosť" a tiež „prevádzkovateľ"***

And / A

(2)

Business Name/Obchodné Meno:	**Stredná odborná škola elektrotechnická**
Registered Seat/Sídlo:	Komenského 50. 010 01 Žilina
ID No/IČO:	
L	
Represented by/ Zast.:	Ing. Ľubomír Králik, riaditeľ/director

hereinafter referred to as **„Company"** and also as **„controller" /** ďalej len ***„Spoločnosť" a tiež „prevádzkovateľ"***

hereinafter jointly referred to as "**Parties**". */ďalej spoločne ako „* ***Zmluvné strany****".*

PREAMBLE /ÚVOD

The Company and the Service Provider have entered into a contractual relationship about providing of services connected with below mentioned processing activities/systems by the Service Provider to Company ("**Main Contract**"):

- Zabezpečenie praktického vyučovania formou odbornej praxe pre žiakov prevádzkovateľa.

*Spoločnosť a Poskytovateľ služieb spolu vstúpili do zmluvného vzťahu, ktorého predmetom je poskytovanie služieb súvisiacich s nižšie uvedenými činnosťami/systémami spracúvania osobných údajov Poskytovateľom služieb voči Spoločnosti (ďalej len „**Hlavná zmluva**"):*

- To ensure practical training of students of controller.

For the Main Contract under this Agreement are considered one or more of the contractual relationships concluded between the Parties, irrespective of their form (oral, written, based on the purchase order or bilateral agreement).

Za Hlavnú zmluvu sa podľa tejto zmluvy považuje jeden alebo viac zmluvných záväzkov, ktoré boli medzi Zmluvnými stranami uzatvorené, a to bez ohľadu na ich formu (ústna, písomná, založená objednávkou alebo dvojstrannou zmluvou).

In performance of its obligations under the Main Contract, the Service Provider processes Personal Data on behalf of the Company as set forth herein and in the Main Contract ("**Contract Data Processing**").

*V rámci plnenia svojich záväzkov podľa Hlavnej zmluvy Poskytovateľ služieb spracúva Osobné údaje menom Spoločnosti v súlade s ustanoveniami uvedenými v tejto zmluve a v Hlavnej zmluve (ďalej len „**Spracúvanie osobných údajov**").*

This agreement("**Agreement**") specifies the rights and obligations of the Parties in connection with the Contract Data Processing.

*Táto zmluva (ďalej len „**Zmluva**") určuje práva a záväzky Zmluvných strán v súvislosti so Spracúvaním zmluvných údajov.*

In consideration of the Parties' mutual rights and obligations set out in this Agreement the Parties hereby agree as follows:

S ohľadom na vzájomné práva a povinnosti Zmluvných strán uvedených v tejto Zmluve sa Zmluvné strany dohodli takto:

1. **DEFINITIONS / *VYMEDZENIE POJMOV***

Capitalized terms used herein shall have the meaning assigned to them in the Main Contract or in Section 15 (List of Definitions) below. Unless otherwise defined herein, the definitions of the European General Data Protection Regulation 2016/679 ("**GDPR**"), in particular the terms "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processor**", **Processing**" " and "**Supervisory Authority**"shall apply.

*Výrazy tu použité s veľkými písmenami budú mať význam, ktorý je definovaný v Hlavnej zmluve alebo v článku 15 (zoznam vymedzených pojmov) nižšie. Pokiaľ tu nie je určené inak, bude platiť vymedzenie pojmov uvedené v Európskom Všeobecnom Nariadení o Ochrane osobných údajov 2016/679 (ďalej jen „**GDPR**"), predovšetkým sa to týka výrazov „**prevádzkovateľ**", „**dotknutá osoba**", „**členský štát**", „**osobné údaje**", „**porušenie ochrany osobných údajov**", „**sprostredkovateľ**", „**spracúvanie**" a „**dozorný orgán**".*

2. **SUBJECT MATTER AND TERM OF AGREEMENT / *PREDMET ZMLUVY A JEJ TRVANIE***

2.1 The Service Provider shall process Company Personal Data for the purpose of providing the services described in the Main Contract ("**Contract Services**")and any additional services under this Agreement ("**Processing Services**") to the Company ("**Admissible Purpose**").

*Poskytovateľ služieb bude spracúvať osobné údaje Spoločnosti za účelom poskytovania služieb popísaných v Hlavnej zmluve (ďalej iba „**Zmluvné služby**") a všetkých doplnkových služieb podľa tejto Zmluvy (ďalej jen „**Spracovateľské služby**") pre Spoločnosť (ďalej len „**Prípustný účel**").*

The Parties agree and acknowledge that the Company will be qualified as Controller and the Service Provider will be qualified as Processor when processing Company Personal Data hereunder. The Service Provider shall not use or disclose Company Personal Data for any other than the Admissible Purpose.

Zmluvné strany sa dohodli a potvrdzujú, že Spoločnosť bude oprávnená pôsobiť ako prevádzkovateľ a Poskytovateľ služieb ako sprostredkovateľ pri spracúvaní osobných údajov Spoločnosti podľa tejto Zmluvy. Poskytovateľ služieb nesmie používať ani sprístupniť osobné údaje Spoločnosti pre žiadny iný účel ako pre Prípustný účel.

2.2 Annex 2.2 sets forth details of

(a) purpose sof the Processing;
(b) type of Company Personal Data;
(c) categories of Data Subjects concerned by the Processing.
(d) List of authorized operation

In the event of changes to the Processing, Company may make reasonable amendments to Annex 2.2 by written notice to Service Provider from time to time as Company reasonably considers necessary to meet statutory requirements.

Príloha 2.2 stanoví podrobné informácie o

(a) *účeloch spracúvania;*
(b) *typoch osobných údajov Spoločnosti;*
(c) *kategóriách dotknutých osôb dotknutých spracúvaním.*
(d) *zoznam povolených spracovateľských činností*

V prípade zmien v spracúvaní môže Spoločnosť vytvoriť primerané dodatky k prílohe 2.2 pomocou písomného oznámenia Poskytovateľovi služieb podľa toho, ako Spoločnosť uzná za primerane nevyhnutné za účelom splnenia právnych požiadaviek.

2.3 The Service Provider shall process Company Personal Data only on behalf of the Company and in strict accordance with the Company's documented instructions, unless otherwise required to

do so by Union or Member State law to which the Service Provider is subject. In such a case, the Service Provider shall immediatelyinform the Company of that legal requirement in writing prior to commencing such processing, unless that law prohibits such information on important grounds of public interest. For the avoidance of doubt, whenever this Agreement or the Main Contract include provisions relating to the Processing of Company Personal Data (e.g. an obligation to anonymise certain Company Personal Data) such Processing shall be considered an instruction of the Controller pursuant to this Agreement.

Poskytovateľ služieb bude spracúvať osobné údaje Spoločnosti iba menom Spoločnosti a výhradne podľa doložených pokynov Spoločnosti, pokiaľ nebude požadované inak únijným právom alebo právom členského štátu, ktorému Poskytovateľ služieb podlieha. V takom prípade musí Poskytovateľ služieb bezodkladne informovať Spoločnosť o takej právnej požiadavke pred tým, ako začne také spracúvanie, pokiaľ však dané právo nezakazuje zasielanie takých informácií z dôvodu verejného záujmu. Aby sa zabránilo akýmkoľvek pochybnostiam, kedykoľvek táto Zmluva alebo Hlavná Zmluva obsahuje ustanovenia týkajúce sa osobných údajov Spoločnosti (napr. záväzok anonymizovať určité osobné údaje Spoločnosti), také spracúvanie bude považované za pokyn Spoločnosti podľa tejto Zmluvy.

2.4 The Processing shall at all times be conducted in a professional manner and in compliance with the principles of proper data processing, the provisions of the Main Contract, this Agreement and applicable law. The Service Provider shall immediately inform the Companyif, in its opinion, an instruction of the Company infringes applicable law (Art. 28 par. 3 GDPR).

Spracúvanie údajov bude vždy realizované profesionálne a v súlade so zásadami správneho spracúvania údajov, ustanoveniami Hlavnej zmluvy, tejto Zmluvy a príslušného právneho predpisu. Poskytovateľ služieb musí bezodkladne informovať Spoločnosť, ak pokyn Spoločnosti (podľa jeho názoru) porušuje príslušné právo (článok 28 ods. 3 GDPR).

2.5 Unless expressly provided otherwise herein, the Company shall not be liable for any additional charges for the Processing Services under this Agreement and the Parties acknowledge and agree that all costs, charges and fees in connection with the Processing Services are fully and adequately compensated by the fees and charges payable under the Main Contract.

Pokiaľ tu nie je vyslovene stanovené inak, Spoločnosť neponesie zodpovednosť za akékoľvek dodatočné poplatky za Spracovateľské služby poskytované podľa tejto Zmluvy a Zmluvné strany potvrdzujú a súhlasia s tým, že všetky náklady, poplatky a platby v súvislosti so Spracovateľskými službami sú plne a adekvátne pokryté platbami a poplatky splatnými na základe Hlavnej zmluvy.

2.6 The duration (term) of this Agreement is equal to the term of the Main Contract and this Agreement shall terminate automatically when the Main Contract terminates, with the exception of any provisions intended to survive termination hereof or the Main Contract. Any right to terminate this Agreement separately prior to such termination date shall be excluded to the extent permitted by applicable law.

Trvanie tejto Zmluvy bude zhodné s trvaním Hlavnej zmluvy a táto Zmluva bude automaticky ukončená s ukončením Hlavnej Zmluvy okrem ustanovení, ktoré sú koncipované tak, aby ostali v platnosti aj po ukončení tejto Zmluvy alebo Hlavnej zmluvy. Právo ukončiť túto Zmluvu samostatne pred stanoveným termínom ukončenia je vylúčené v rozsahu požadovanom príslušným právnym predpisom.

2.7 In the event the EU Commission or a competent Supervisory Authority lays down standard contractual clauses in accordance with Article 28 par.7GDPR, the Parties will upon the Controller's request include one or more of those contractual clauses in this Agreement if so required to comply with applicable law. The same applies to any other changes of applicable law which require an amendment to this Agreement to comply with applicable law.

V prípade, že Komisia EU alebo príslušný dozorný úrad ustanoví štandardné zmluvné doložky v súlade s článkom 28 ods. 7 GDPR, Zmluvné strany na žiadosť prevádzkovateľa zapracujú jednu alebo viacero týchto doložiek do tejto Zmluvy, pokiaľ to bude nevyhnutné pre súlad s príslušným právnym predpisom. To isté platí pre akékoľvek ďalšie zmeny príslušného právneho predpisu, ktoré vyžaduje doplnenie tejto Zmluvy, aby bola dosiahnutá zhoda s príslušným právnym predpisom.

3. REQUIRED TECHNICAL AND ORGANISATIONAL MEASURES / *POŽADOVANÉ TECHNICKÉ A ORGANIZAČNÉ OPATRENIA*

3.1 The Service Provider shall ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services as well as the ability to restore the availability and access to Company Personal Data in a prompt manner in the event of a physical or technical incident as required under applicable law.

The Service Provider shall implement appropriate technical and organizational measures as required by applicable law and in line with the state of technological development andapplicable data security standards in order to

(a) prevent (i) unauthorised or unlawful processing of the Company Personal Data; and (ii) the accidental loss or destruction of, or damage to, the Company Personal Data and

(b) ensure a level of security appropriate to (i) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and (ii) the nature of the Company Personal Data to be protected;

including the measures referred to in Article 32 GDPR ("**Data Security Standards**").

Poskytovateľ služieb zaistí nepretržitú dôvernosť, neporušenosť, dostupnosť a odolnosť spracovávajúcich systémov a služieb a tiež schopnosť obnovovať dostupnosť a prístup k osobným údajom Spoločnosti urýchleným spôsobom v prípade fyzickej alebo technickej nehody v súlade s príslušným právnym predpisom.

Poskytovateľ služieb musí prijať zodpovedajúce technické a organizačné opatrenia požadované príslušným právom a v súlade so stavom technického vývoja a použiteľné štandardy ochrany údajov, aby sa

(a) *zabránilo (i) neoprávnenému alebo nezákonnému spracovaniu osobných údajov Spoločnosti; a (ii) náhodnej strate alebo zničeniu alebo poškodeniu osobných údajov Spoločnosti a*

(b) *zaistila úroveň zabezpečenia zodpovedajúca (i) škode, ktorá by mohla vzniknúť v dôsledku takéhoto neoprávneného nebo nezákonného spracovania alebo náhodnej straty, zničenia alebo poškodenia a (ii) povahe osobných údajov Spoločnosti, ktoré majú byť chránené;*

*vrátane opatrení uvedených v článku 32 GDPR (ďalej len „**Štandardy zabezpečenia údajov**").*

3.2 Without prejudice to the generality of the foregoing, the Data Security Standards that the Service Provider shall implement and maintain, as determined and approved by the Company, are defined in Annex 3.2.

Bez toho, aby bola ovplyvnená platnosť vyššie uvedeného, v prílohe 3.2 sú definované Štandardy zabezpečenia údajov určené a schválené Spoločnosťou, ktoré musí Poskytovateľ služieb zaviesť a udržiavať.

3.3 The Service Provider warrants that it has implemented the Data Security Standards and that it will maintain such Data Security Standards during the term hereof. The Service Provider shall ensure by means of appropriate protective mechanisms that access to Company Personal Data is strictly limited to those employees of the Service Provider who require access in order to fulfil the Admissible Purpose.

Poskytovateľ služieb sa zaručuje, že zaviedol Štandardy zabezpečenia údajov a že ich bude počas platnosti tejto Zmluvy udržiavať. Poskytovateľ služieb musí pomocou vhodných ochranných mechanizmov zaistiť, že k osobným údajom Spoločnosti budú mať prístup prísne vymedzení zamestnanci Poskytovateľa služieb, ktorí tento prístup potrebujú, aby mohli splniť Prípustný účel.

3.4 Acknowledging that the Data Security Standards are subject to technical progress and development, the Parties agree that the Service Provider shall be authorized to implement adequate alternative technical and organizational measures provided, however, that such measures shall not fall short of the level of security provided by the Data Security Standards, comply with the requirements under applicable data protectionlaws. The Service Provider shall immediately notify the Company of any changes to the Data Security Standards. The Service Provider shall regularly test and audit the Data Security Standards for adequateness and compliance with applicable law and immediately take any corrective action required.

Berúc do úvahy to, Štandardy zabezpečenia údajov podliehajú technickému pokroku a rozvoju, Zmluvné strany súhlasia s tým, že Poskytovateľ služieb je oprávnený zaviesť primerané alternatívne technické a organizačné opatrenia s tým, že tieto opatrenia nesmú znížiť úroveň ochrany, ktorú poskytujú Štandardy zabezpečenia údajov, a ktoré budú zodpovedať požiadavkám platných právnych predpisov na ochranu osobných údajov. Poskytovateľ služieb je povinný okamžite informovať Spoločnosť o všetkých zmenách Štandardov zabezpečenia údajov. Poskytovateľ služieb musí pravidelne vykonávať testy a audity Štandardov zabezpečenia údajov

s poukazom na primeranosť a súlad s platným právom a okamžite vykonať všetky kroky vedúce k náprave.

4. DATA SUBJECT RIGHTS/ *PRÁVA DOTKNUTÝCH OSÔB*

4.1 The Parties acknowledge and agree that the Company is legally responsible to deal with any requests or enquiries from Data Subjects in relation to their rights under applicable law in relation to the Processing of Company Personal Data ("**Data Subject Requests**") and that the Service Provider shall not respond to any such Data Subject Requests unless otherwise required by documented instructions by the Company.

*Zmluvné strany berú na vedomie a súhlasia, že Spoločnosť je právne zodpovedná za plnenie požiadaviek a dotazov dotknutých osôb týkajúcich sa ich práv, ktoré majú podľa príslušného práva v súvislosti so spracúvaním osobných údajov Spoločnosti (ďalej len „**Požiadavky dotknutých osôb**") a že Poskytovateľ služieb nebude odpovedať na žiadne takéto požiadavky dotknutých osôb, ak to nebude požadovať Spoločnosť formou písomného pokynu.*

4.2 The Service Provider shall take all action reasonably requested by the Company and make all required information available to the Company in a format requested by the Company in order to comply with such Data Subject Requests. Service Provider shall implement the necessary technical and organisational measures for this purpose.

Poskytovateľ služieb vykoná všetky činnosti, ktoré od neho môže Spoločnosť spravodlivo požadovať a poskytne Spoločnosti všetky požadované informácie vo formáte požadovanom Spoločnosťou , aby mohli byť splnené požiadavky dotknutých osôb. Poskytovateľ služieb príjme pre tento účel všetky nevyhnutné technické a organizačné opatrenia.

4.3 The Service Provider shall

(a) immediately notify the Company of any Data Subject Requests or other enquiries relating to this Agreement received by it or any Sub-Processor without responding to such requests or enquiries unless expressly otherwise instructed by the Company; and

(b) ensure that any Sub-Processors do not respond to any Data Subject Requests unless expressly otherwise instructed by the Company or required by applicable law, in which case Service Provider shall to the extent permitted by applicable law inform Company of that legal requirement before the Sub-Processor responds to the request.

Poskytovateľ služieb je povinný

(a) *bezodkladne informovať Spoločnosť o akýchkoľvek požiadavkách dotknutých osôb alebo iných dotazoch týkajúcich sa tejto Zmluvy, ktoré obdržal on alebo jeho sprostredkovateľ bez toho, aby na tieto požiadavky a dotazy odpovedal, kým nie je vo výslovných pokynoch od Spoločnosti uvedené inak; a*

(b) *zaistiť, aby všetci jeho ďalší sprostredkovatelia neodpovedali na požiadavky dotknutých osôb, kým im to výslovne neuloží Spoločnosť, alebo to nebude vyžadované platným právom, v ktorom prípade je Poskytovateľ služieb povinný o tomto rozšírení oprávnenia vyplývajúcom z príslušného právneho predpisu informovať Spoločnosť pred tým, než jeho ďalší sprostredkovateľ odpovie na danú požiadavku.*

4.4 In the event of a dispute with or other claims brought by a Data Subject concerning the Processing of Company Personal Data against the Service Provider, the Service Provider shall promptly notify and inform the Company and shall cooperate and coordinate with a view to effectively defending against such claims or settling them amicably in a timely fashion. In the event of such disputes or claims brought against the Company, the Service Provider shall cooperate and provide the Company with any information and take any action reasonably required by the Company.

V prípade sporu s Poskytovateľom služieb alebo iných nárokov vznesených voči nemu dotknutými osobami týkajúcich sa spracúvania osobným údajov Spoločnosti, Poskytovateľ služieb je povinný bezodkladne informovať Spoločnosť a spolupracovať s ňou za účelom efektívnej obrany voči takýmto nárokom alebo urýchleného urovnania. Ak bude vedený spor alebo vznesený nárok voči Spoločnosti, Poskytovateľ služieb je povinný spolupracovať a poskytnúť Spoločnosti všetky informácie a podniknúť kroky vyžadované Spoločnosťou.

5. FURTHER DATA PROTECTION OBLIGATIONS/ *DALŠIE POVINNOSTI PRI OCHRANE ÚDAJOV*

5.1 The Service Provider shall maintain, and promptly make available to the competent Supervisory Authority on request, a proper documented (electronic form sufficient) record of all categories

of processing activities carried out on behalf of a Companyin accordance with Art. 30 par. 2 GDPR, which at least contains the following information:

(a) The name and contact details of the Service Provider, Sub-Processors and the Company and, where applicable, of the Company's or the Service Provider's representative, and the data protection officer;

(b) The categories of processing carried out on behalf of the Company;

(c) Where applicable, transfers of Personal Data to a non-EU/EEA country or an international organisation, including the identification of that non-EU/EEA country or international organisation and the documentation of suitable safeguards (if required);

(d) a general description of the Data Security Standards.

Poskytovateľ služieb musí udržiavať a urýchlene poskytnúť na vyžiadanie príslušnému dozornému orgánu riadne zdokumentovaný (postačuje aj v elektronickej podobe) záznam o spracovateľských činnostiach vykonávaných za Spoločnosť v súlade s čl. 30 ods. 2 GDPR, ktorý obsahuje minimálne tieto informácie:

(a) *meno a kontaktné údaje Poskytovateľa služieb, ďalších sprostredkovateľov a Spoločnosti a tam, kde sa to uplatňuje aj zástupcu Spoločnosti alebo zástupcu Poskytovateľa služieb a zodpovednej osoby;*

(b) *kategórie spracúvania vykonávané menom Spoločnosti;*

(c) *tam, kde sa tu uplatňuje, prenos osobných údajov do krajín mimo EÚ/EHP alebo medzinárodnej organizácii vrátane uvedenia tejto krajiny mimo EÚ/EHP alebo medzinárodnej organizácie a predloženie vhodných bezpečnostných opatrení (ak sa to vyžaduje);*

(d) *všeobecný popis Štandardov zabezpečenia údajov.*

5.2 The Service Provider shall promptly take any action reasonably required by the Company to assist the Company in relation to the Company's obligations under applicable laws in relation to the Processing, including in relation to

(a) the preparation of the records of processing activities in accordance with Art. 30 GDPR in relation to the Processing under this Agreement and shall immediately upon request provide the Company with any information required for this purpose in a format reasonably requested by the Company;

(b) the data protection impact assessment (DPIA) in accordance with Art. 35 GDPR; and

(c) any requests or consultations with the responsible Supervisory Authority.

The Service Provider shall immediately notify the Company of any changes in relation to the Processing which may require changes to the register of processing activities, the DPIA or any other action to be taken by the Company.

Poskytovateľ služieb musí urýchlene podniknúť všetky kroky, ktoré od neho môže Spoločnosť spravodlivo požadovať, aby poskytol Spoločnosti súčinnosť v súvislosti s jej povinnosťami pri spracúvaní osobných údajov , vrátane

(a) *prípravy záznamov o spracovateľských činnostiach v súlade s čl. 30 GDPR vo vzťahu k spracúvaniu údajov podľa tejto Zmluvy a na vyžiadanie musí Spoločnosti poskytnúť všetky informácie požadované pre tento účel vo formáte, v ktorom ich môže Spoločnosť spravodlivo požadovať;*

(b) *posúdenia vplyvu na ochranu údajov (DPIA) v súlade s čl. 35 GDPR a*

(c) *všetkých požiadaviek a konzultácií s príslušným dozorným orgánom.*

Poskytovateľ služieb je povinný okamžite informovať Spoločnosť o všetkých zmenách v súvislosti so spracúvaním, ktoré si môžu vyžiadať zmeny v registri spracovateľských činností, v DPIA alebo ktoré si môžu vyžiadať vykonanie akýchkoľvek ďalších krokov zo strany Spoločnosti.

6. SERVICE PROVIDER PERSONNEL / DATA PROTECTION OFFICER /ZAMESTNANCI POSKYTOVATEĽA SLUŽIEB / ZODPOVEDNÁ OSOBA

6.1 Service Provider shall ensure that any personnel undertaking or involved in the Processing under this Agreement are properly qualified and trained, including a specific and appropriate data protection training, and have committed themselves to keep Company Personal Data confidential or are under an appropriate statutory obligation of confidentiality in accordance with applicable law which shall survive termination of this Agreement.Service Provider shall ensure that access to Company Person al Data is strictly limit to those individuals who need to know or access the relevant Company Personal Data, as strictly necessary for the Admissible Purposes in the context of that individual's duties.

Poskytovateľ služieb je povinný zaistiť, aby všetky osoby vykonávajúce spracúvanie údajov podľa tejto Zmluvy alebo zahrnuté do tohto spracúvania sú riadne kvalifikované a zaškolené,

vrátane špecifickej a príslušnej odbornej prípravy v oblasti ochrany údajov, a aby sa zaviazali uchovávať osobné údaje Spoločnosti v tajnosti, alebo aby sa na nich vzťahovala zákonná povinnosť mlčanlivosti zakotvená v platnom práve, ktorá zostane zachovaná aj po ukončení tejto Zmluvy. Poskytovateľ služieb je povinný zaistiť, že prístup k osobným údajom Spoločnosti bude prísne obmedzený len pre tie osoby, ktoré tento prístup k relevantným osobným údajom Spoločnosti potrebujú alebo je nevyhnutný vzhľadom na prípustný účel podľa povinnosti týchto osôb.

6.2 The Service Provider shall appoint a data protection officer in accordance with applicable law or,if appointment of a data protection officer is not required under the applicable law, another data protection official responsible for the data protection aspects of the Processing of Company Personal Data and shall immediately provide the Company with relevant up to date contact details.

Poskytovateľ služieb je povinný vymenovať zodpovednú osobu v súlade s platným právom, a ak platné právo nepožaduje vymenovanie zodpovednej osoby, je Poskytovateľ služieb povinný menovať inú osobu zodpovednú za ochranu údajov pri spracúvaní osobných údajov Spoločnosti a okamžite poskytnúť Spoločnosti relevantné a aktuálne kontaktné údaje na túto osobu.

7. SUB-PROCESSING / DALŠIE SPRACÚVANIE

7.1 The Service Provider shall be authorized to engage other Processors in relation to the Contract Data Processing ("**Sub-Processor**") in accordance with the Main Contract and subject to the following provisions. Section **Chyba! Nenašiel sa žiaden zdroj odkazov.** shall apply accordingly with respect to any Processing of Company Personal Data by a Sub-Processor outside of the territory of the European Union.

*Poskytovateľ služieb je oprávnený využiť ďalšieho sprostredkovateľa na spracúvanie zmluvných osobných údajov (ďalej len „**ďalší sprostredkovateľ**") v súlade s Hlavnou zmluvou a v súlade s nižšie uvedenými ustanoveniami. Článok 2.3 Zmluvy sa primerane použije aj na spracúvanie osobných údajov Spoločnosti mimo územia Európskej únie ďalším sprostredkovateľom.*

7.2 Any engagement of a Sub-Processor requires prior written consent of the Company.

Každému využitiu ďalšieho sprostredkovateľa musí predchádzať písomný súhlas Spoločnosti.

7.3 Service Provider shall give Company prior written notice of the intended appointment of any new Sub-Processor, including full details of the Processing to be undertaken by the Sub-Processor. If, within three (3) weeks of receipt of that notice, Company notifies Service Provider in writing of any objections on reasonable grounds to the proposed appointment, Service Provider shall work with Company in good faith to take reasonable measures to address the objections raised by the Company. Where such measures cannot be agreed within three (3) weeks from Service Provider's receipt of Company's notice, notwithstanding anything in the Main Contract, Company may by written notice to Service Provider with immediate effect terminate the Main Contract to the extent that it relates to the Contract Services which require the use of the proposed Sub-Processor.

Poskytovateľ služieb je povinný vopred písomne informovať Spoločnosť o každom zamýšľanom pribraní ďalšieho sprostredkovateľa, vrátane podrobných informácií a tom, aké spracúvanie osobných údajov bude ďalší sprostredkovateľ vykonávať. Ak Spoločnosť do troch (3) týždňov od doručenia takej informácie písomne oznámi Poskytovateľovi služieb dôvodné námietky voči takému zamýšľanému pribraniu, Poskytovateľ služieb je povinný spolupracovať so Spoločnosťou za účelom prijatia vhodným opatrení vzhľadom na námietky vznesené Spoločnosťou. Ak sa nedohodnú na opatreniach do troch (3) týždňov od doručenia námietok Spoločnosti Poskytovateľovi služieb, bez ohľadu na ustanovenia Hlavnej zmluvy je Spoločnosť oprávnená ukončiť Hlavnú zmluvu písomným oznámením Poskytovateľovi služieb v rozsahu, akom sa týka dohodnutých služieb, na vykonanie ktorých sa vyžaduje použitie ďalšieho sprostredkovateľa.

7.4 With respect to each Sub-Processor, the Service Provider shall

(a) before any Company Personal Data are transferred to the Sub-Processor, carry out adequate due diligence to ensure that the Sub-Processor is capable of providing the level of protection for Company Personal Data required by this Agreement and the Main Contract;

(b) enter into a written agreement with the Sub-Processor which imposes the same obligations on the Sub-Processorin relation to the protection of Company Personal Data as are imposed on the Service Provider under this Agreement. This shall apply in

particular, but shall not be limited to, the confidentiality obligations and the Data Security Standards to be observed pursuant to Section 3;

(c) immediately upon request provide the Company with the sub-contracting agreement and any other documentation reasonably requested by the Company (it being understood that the Service Provider shall be permitted to redact any commercial terms which are confidential and not required by the Company to assess compliance of the Service Provider with its obligations under this Agreement);

(d) conduct regular audits as required to ensure that the Sub-Processor complies with the Data Security Standards and its other contractual obligations and shall immediately notify the Company in accordance with Section 10 of any breach of a Sub-Processor's obligations. The Service Provider shall secure that the Sub-Processor grants direct audit and inspection rights in accordance with Section 0 to the Company.

Poskytovateľ služieb je povinný vo vzťahu ku každému ďalšiemu sprostredkovateľovi

(a) *vykonať potrebné prešetrenie za účelom uistenia sa, že ďalší sprostredkovateľ je schopný dodržať úroveň zabezpečenia osobných údajov Spoločnosti vyžadovanú touto Zmluvou a Hlavnou zmluvou ešte pred tým, než dôjde k prenosu osobných údajov Spoločnosti na ďalšieho sprostredkovateľa;*

(b) *uzatvoriť s ďalším sprostredkovateľom písomnú zmluvu, ktorá zakotví pre ďalšieho sprostredkovateľa rovnaké povinnosti vzhľadom na ochranu osobných údajov ako tie, ktoré vyplývajú pre Poskytovateľa služieb z tejto Zmluvy. To bude platiť najmä, nie však výlučne vo vzťahu k povinnosti mlčanlivosti a Štandardom zabezpečenia údajov, ktoré musia byť dodržiavané v súlade s čl. 3;*

(c) *okamžite, na základe žiadosti Spoločnosti, poskytnúť Spoločnosti zmluvu s ďalším sprostredkovateľom a ďalšiu dokumentáciu, ktorú môže Spoločnosť spravodlivo požadovať (je pochopiteľné, že Poskytovateľ služieb je oprávnený odstrániť všetky obchodné podmienky, ktoré sú dôverné a Spoločnosť ich nepotrebuje na posúdenie plnenia povinností vyplývajúcich z tejto Zmluvy pre Poskytovateľa služieb);*

(d) *vykonávať pravidelné audity za účelom uistenia sa, že ďalší sprostredkovateľ spĺňa štandardy zabezpečenia údajov a ďalšie zmluvné povinnosti a v súlade s čl. 10 je povinný okamžite upovedomiť Spoločnosť o akomkoľvek porušení povinností zo strany ďalšieho sprostredkovateľa. Poskytovateľ služieb je povinný zabezpečiť, že ďalší sprostredkovateľ udelí Spoločnosti práva na priamy audit a kontrolu v súlade s čl. 9.*

7.5 The Service Provider shall at all times provide the Company with an up to date list of Sub-Processors engaged by the Service Provider for carrying out specific processing activities on behalf of the Company, detailing company name, address and contact details, the specific area of Contract Data Processing operations outsourced and the location of the Processing.

Poskytovateľ služieb je povinný poskytovať Spoločnosti aktuálny zoznam ďalších sprostredkovateľov pribraných Poskytovateľom služieb za účelom vykonávania špecifických spracovateľských činností pre Spoločnosť, s uvedením mena spoločnosti, adresy, kontaktných údajov a špecifikácie oblastí zmluvných spracovateľských operácií a miesto, kde k spracúvaniu dochádza.

7.6 In case of non-compliance of the Sub-Processor with its contractual obligations,

(a) the Service Provider shall remain fully liable to the Company for any damages caused by such non-compliance and shall indemnify and hold harmless the Company against any claims or damages in connection with or resulting from the engagement of the Sub-Processor; and

(b) the Company shall be entitled to withdraw its consent to the engagement of such Sub-Processor in which case the Service Provider shall promptly stop engaging such Sub-Processor in connection with the Contract Data Processing and Section 0 shall apply with respect to such Sub-Processor.

V prípade, ak ďalší sprostredkovateľ neplní svoje zmluvné povinnosti,

(a) *Poskytovateľ služieb nesie voči Spoločnosti plnú zodpovednosť za akúkoľvek škodu spôsobenú týmto nedodržaním povinností, je povinný odškodniť Spoločnosť a zbaviť ju zodpovednosti za akúkoľvek škodu a nároky vyplývajúce alebo súvisiace s využitím ďalšieho sprostredkovateľa*

(b) *Spoločnosť bude oprávnená vziať späť svoj súhlas na zapojenie tohto ďalšieho sprostredkovateľa a Poskytovateľ služieb bude povinný ukončiť zapojenie tohto ďalšieho sprostredkovateľa do spracúvania zmluvných osobných údajov. Čl. 0 sa v tomto prípade bude vzťahovať na tohto ďalšieho sprostredkovateľa.*

8. RESTRICTED TRANSFERS / *OBMEDZENÉ PRENOSY*

8.1 The Parties will immediately upon request of the Company and prior to commencement of any Restricted Transfer (i) enter into the standard clauses set forth in the Commission Decision dated February 5, 2010 (2010/87/EU) and/or (ii) enter into or establish any other appropriate instruments or undertakings required under applicable law to effect such Restricted Transfer without breach of such applicable law. If so required by applicable law or reasonably requested by the Company, Service Provider shall cause any Sub-Processor to enter into such instruments or undertakings directly with the Company.

Pred zahájením obmedzeného prenosu sú strany povinné na žiadosť Spoločnosti (i) uzatvoriť štandardné zmluvné doložky uvedené v rozhodnutí Komisie zo dňa 05.02.2010 (2010/87/EU) a/alebo (ii) uzatvoriť alebo zaviesť akékoľvek iné vhodné dokumenty alebo záväzky vyžadované platným právom za účelom vykonania obmedzeného prevodu bez porušenia príslušného práva. Ak je to vyžadované platným právom alebo dôvodne požadované Spoločnosťou, Poskytovateľ služieb je povinný zaistiť, aby ďalší sprostredkovateľ vo vzťahu k dokumentom a záväzkom vstúpil do vzťahu priamo so Spoločnosťou.

8.2 "**Restricted Transfer**" means any transfer of Company Personal Data by or to any of the Parties or a Sub-Processor which would be prohibited by applicable law in the absence of the instruments or undertakings referred to in Section 0 above.

*„**Obmedzený prenos**" znamená akýkoľvek prenos osobných údajov Spoločnosti Stranami alebo ďalším sprostredkovateľom prípadne k týmto subjektom, ktorý by bol zakázaný platným právom v prípade, ak by neexistovali dokumenty alebo záväzky uvedené vyššie v čl. 8.1*

8.3 When processing Company Personal Data outside of the territory of the European Union or the EEA or engaging in any act or practice regarding Company Personal Data where that act or practice is subject to data protection laws in jurisdictions outside the territory of the European Union or EEA, the Service Provider shall comply with those applicable laws, in particular provide appropriate safeguards to ensure an adequate level of data protection in accordance with Art. 44 etseq GDPR.

Ak sa spracúvajú osobné údaje Spoločnosti mimo územia Európskej únie alebo EHP alebo sa vo vzťahu k osobným údajom Spoločnosti vykonáva akákoľvek činnosť, ktorá z hľadiska ochrany údajov podlieha právu platnému mimo územia Európskej únie alebo EHP, Poskytovateľ služieb musí spĺňať daným právom zakotvené požiadavky a prijať vhodné bezpečnostné opatrenia za účelom uistenia sa, že je zabezpečená potrebná miera ochrany osobných údajov v súlade s čl. 44 a nasl. GDPR.

9. INSPECTIONS AND AUDITS / *KONTROLY A AUDITY*

9.1 Service Provider shall make available to the Company on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to auditsin relation to the Processing of Company Personal Data, including inspections of the data-processing facilities of the Service Provider,by the Company or an auditor mandated by the Company in accordance with this Section 0.

Poskytovateľ služieb je povinný sprístupniť Spoločnosti na jej požiadanie všetky informácie potrebné na preukázanie súladu spracúvania údajov s touto Zmluvou, a v zmysle časti 0 Zmluvy je povinný umožniť Spoločnosti alebo audítorovi poverenému Spoločnosťou vykonať audit a spolupracovať s nimi pri vykonávaní auditov vo vzťahu k spracúvania osobných údajov Spoločnosti vrátane inšpekcií zariadení, kde sa spracúvanie údajov Poskytovateľom služieb vykonáva.

9.2 The Company shall give Service Provider reasonable notice of any audit or inspection to be conducted and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Service Provider's premises, equipment, personnel and business in the course of such an audit or inspection. Audits or inspections shall not be conducted outside normal business hours or without notice, unless (i) the Company has given notice to the Service Provider that the audit or inspection needs to be conducted on an emergency basis or (ii) required to investigate an actual or reasonably suspected breach by the Service Provider of his obligations under this Agreement.

Spoločnosť je povinná vopred vhodným spôsobom oznámiť Poskytovateľovi služieb každý audit alebo inšpekciu a je povinná (vrátane ňou poverených audítorov) vynaložiť nevyhnutné úsilie aby sa predišlo (a ak nie je možné predísť, tak aby sa minimalizovalo nebezpečenstvo) vzniku

akýchkoľvek škôd, zranení alebo narušeniu činnosti Poskytovateľa služieb, jeho zariadení, personálu a podnikania v dôsledku takého auditu alebo inšpekcie. Audity a inšpekcie sa nesmú vykonávať mimo pracovného času alebo bez oznámenia, ibaže (i) Spoločnosť oznámi Poskytovateľovi služieb, že sa audit alebo kontrola musia vykonať naliehavo alebo (ii) je potreba vyšetriť skutočné alebo dôvodne očakávané porušenie povinností Poskytovateľa služieb vyplývajúcich z tejto Zmluvy.

9.3 If the Company notifies the Service Provider about any deficiencies or irregularities related to the Processing of Company Personal Data discovered during such audits or inspections,the Service Provider shall promptly take any action required or reasonably requested by the Company to remedy such findings and provide Company with written documentation evidencing that the audit findings have been remedied as required by applicable law and this Agreement.

Ak Spoločnosť oznámi Poskytovateľovi služieb akékoľvek nedostatky alebo nezrovnalosti pri spracúvaní osobných údajov Spoločnosti zistených auditom alebo inšpekciou, Poskytovateľ služieb je povinný urýchlene urobiť všetky opatrenia vyžadované alebo dôvodne požiadané Spoločnosťou za účelom nápravy zistení a odovzdať Spoločnosti písomnú dokumentáciu, z ktorej bude zrejmé, ako boli auditom zistené nedostatky odstránené v zmysle požiadaviek príslušného práva a tejto Zmluvy.

10. PERSONAL DATA BREACHES AND INCIDENTS / *INCIDENTY A PORUŠENIA OCHRANY OSOBNÝCH ÚDAJOV*

10.1 The Service Provider shall immediately notify the Company of any actual or suspected technical, organizational or other incidents (including incidents at Sub-Processors) which have resulted or may result in a Personal Data Breach in the sense of Art. 33 par. 1 GDPR or otherwise have an adverse effect on the integrity and security of Company Personal Data or the Contract Data Processing ("**Data Security Incident**").Data Security Incidents include in particular, but are not limited to, the following:

(a) Any actual or suspected unauthorized access, disclosure,loss, download, theft, blocking, encryption or deletion by malware or other unauthorized action in relation to Company Personal Databy unauthorized third parties;

(b) any operational incidents which may have an impact on the Processing of Company Personal Data;

(c) any actual or suspected breach of this Agreement or applicable law by the Service Provider, his employees or other vicarious agents to the extent that such breach relates to Company Personal Data or the Service Provider's obligations under this Agreement; or

(d) any legally binding request for disclosure or seizure of Company Personal Data by a law enforcement or other public authority unless the Service Provider is prohibited by statutory law to notify such incident to the Company. In this case, the Service Provider must notify the Company immediately upon such prohibition having ceased.

*Poskytovateľ služieb je povinný bezodkladne oznámiť Spoločnosti všetky uskutočnené technické, organizačné alebo iné incidenty (vrátane incidentov ďalšieho sprostredkovateľa), ktoré vyústili alebo by mohli vyústiť do porušenia ochrany osobných údajov v zmysle čl. 33 ods. 1 GDPR, alebo by mohli mať nepriaznivý vplyv na celistvosť a bezpečnosť osobných údajov Spoločnosti alebo spracúvanie zmluvných osobných údajov, a to aj vrátane podozrenia na takýto incident (ďalej len „**Bezpečnostný incident**"). Bezpečnostným incidentom sa rozumie najmä, nie však výlučne:*

(a) *vykonaný neoprávnený prístup, sprístupnenie, strata, stiahnutie, krádež, zablokovanie, zašifrovanie alebo výmaz uskutočnený malwarom alebo iným neoprávneným konaním tretej strany vo vzťahu k osobným údajom Spoločnosti, vrátane podozrenia na takéto konanie;*

(b) *akékoľvek prevádzkové incidenty, ktoré by mohli mať vplyv na spracúvanie osobných údajov Spoločnosti;*

(c) *Poskytovateľom služieb, jeho zamestnancami a poverenými zástupcami vykonané porušenie tejto Zmluvy alebo príslušného právneho predpisu vrátane podozrenia na takéto porušenie, v takom rozsahu, že sa toto porušenie týka osobných údajov Spoločnosti alebo povinností Poskytovateľa služieb podľa tejto Zmluvy; alebo*

(d) *všetky právne záväzné požiadavky na sprístupnenie alebo zadržanie osobných údajov orgánmi činnými v trestnom konaní alebo iným verejným orgánom okrem prípadu, ak platné právne predpisy zakazujú Poskytovateľovi služieb oznámiť takýto incident Spoločnosti. V tomto prípade je Poskytovateľ služby povinný informovať Spoločnosť bezodkladne po tom, ako bude zákaz zrušený.*

10.2 The Service Provider must notify the Company immediately, but in any case no later than 24 hours after becoming aware of a Data Security Incident. Service Provider's notification to the Company must be comprehensive and include any information the Company specifically requests or which may reasonably be expected to be required or appropriate in order to comply with its legal obligations in relation to the Data Security Incident. This includes in particular any information required under Art. 33 par. 3 GDPR and as a minimum the following:

(a) the nature of the Data Security Incident, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

(b) the name and contact details of Service Provider's data protection officer or other relevant contact from whom more information may be obtained;

(c) the likely consequences of the Data Security Incident; and

(d) the measures taken or proposed to be taken to address the Data Security Incident.

Poskytovateľ služieb je povinný bezodkladne, najneskôr do 24 hodín od kedy sa o ňom dozvie, oznámiť Spoločnosti Bezpečnostný incident. Oznámenie musí byť kompletné a musí obsahovať všetky informácie, ktoré Spoločnosť výslovne požaduje alebo u ktorých možno dôvodne očakávať, že ich bude vyžadovať vzhľadom na svoje zákonné povinnosti pri existencii Bezpečnostného incidentu. To sa týka predovšetkým informácií vyžadovaných podľa čl. 33 ods. 3 GDPR a minimálne týchto informácií:

(a) *povaha Bezpečnostného incidentu, kategórie a počet dotknutých osôb, ktorých sa incident týka a kategórie a počet záznamov o osobných údajoch, ktorých sa Bezpečnostný incident týka;*

(b) *meno a kontaktné údaje na zodpovednú osoby Poskytovateľa služieb alebo kontakt na inú relevantnú osobu, od ktorej bude možné získať viac informácií;*

(c) *pravdepodobné dopady Bezpečnostného incidentu na ochranu osobných údajov a*

(d) *prijaté alebo navrhnuté opatrenia za účelom nápravy Bezpečnostného incidentu.*

10.3 The Service Provider is not authorized to notify a Data Security Incident to a Supervisory Authority or other authority, the data subjects concerned or any other third parties unless the Service Provider is required to do so under applicable law (e.g. if the Data Security Incident results in a Personal Data Breach for which the Service Provider is himself responsible as Controller). In such event, the Service Provider shall, to the extent permitted under applicable law, liaise and coordinate with the Company prior to making a notification. The Parties shall use their best efforts to agree on a joint approach with a view to prevent any contradicting or inconclusive notifications. This includes providing each other with the details of any notification and the date and time on which notification will be made.

Poskytovateľ služieb nie je oprávnený oznámiť Bezpečnostný incident dozorným orgánom, iným orgánom, dotknutým osobám alebo iným tretím stranám, okrem prípadu, ak má takúto povinnosť v zmysle príslušného práva (napr. Bezpečnostný incident vyústi do Porušenia ochrany osobných údajov, v ktorom prípade má Poskytovateľ služieb rovnakú zodpovednosť ako prevádzkovateľ). V takomto prípade je Poskytovateľ služieb povinný v rozsahu povolenom príslušným právom, spolupracovať so Spoločnosťou skôr, než urobí potrebné oznámenie. Zmluvné strany sú povinné vynaložiť najvyššie možné úsilie na dohodu o spoločnom postupe s cieľom zabrániť rozporným alebo bezvýsledným oznámeniam. To zahŕňa vzájomné informovanie sa o detailoch akéhokoľvek oznámenia a dátumu a času, kedy bude toto oznámenie uskutočnené.

10.4 In the event of a Data Security Incident, the Service Provider shall immediately and in coordination with the Company take any measures required and adequate under applicable law and technical standards to restore the confidentiality, integrity and availability of the Company Personal Data and the resilience of the processing systems and services and to mitigate the risk of harm and/or any detrimental consequences for the data subjects affected or potentially affected by the Data Security Incident. The Service Provider shall promptly provide the Company with a written incident report detailing such measures taken and specific measures taken to prevent similar incidents in the future.

V prípade Bezpečnostného incidentu je Poskytovateľ služieb povinný okamžite a v spolupráci so Spoločnosťou prijať akékoľvek vyžadované a primerané opatrenia podľa príslušného práva a technických požiadaviek za účelom obnovenia mlčanlivosti, celistvosti a dostupnosti osobných údajov Spoločnosti, odolnosti spracovateľských systémov a operácií a zníženia rizika škody a/alebo všetkých nežiaducich následkov pre dotknuté osoby, ktorých sa Bezpečnostný incident týka alebo by sa mohol týkať. Poskytovateľ služieb je povinný urýchlene poskytnúť Spoločnosti písomnú správu o Bezpečnostnom incidente s uvedením, aké opatrenia boli prijaté a aké špecifické opatrenia sa prijmú, aby sa predišlo obdobným incidentom v budúcnosti.

11. COMMUNICATION WITH AUTHORITIES / *KOMUNIKÁCIA S ÚRADMI*

To the extent permitted under applicable law,

(a) the Service Provider shall immediately notify the Company in the event of any audits, enquiries, investigations, requests, orders or other proceedings or matters which may relate to Company Personal Data or the Service Provider's obligations under this Agreement by a Supervisory Authority or any other public body in relation to the Processing of Company Personal Data ("**Authority Enquiries**"). The Parties shall use best efforts to support each other and to ensure an aligned and coordinated communication with the Authority in relation to any Authority Enquiries.

(b) in the event of a dispute with, orders or fines imposed or other claims brought by a Supervisory Authority or other competent authority concerning the Processing of Company Personal Data against either or both Parties, the Parties shall promptly notify and inform each other and shall cooperate and coordinate with a view to effectively defend themselves against such claims or settling them amicably in a timely fashion.

V rozsahu povolenom podľa príslušného práva,

(a) *Poskytovateľ služieb je povinný bezodkladne informovať Spoločnosť o auditoch, šetreniach, vyšetrovaniach, žiadostiach, príkazoch alebo iných činnostiach, ktoré by sa mohli dotýkať osobných údajov Spoločnosti alebo povinností Poskytovateľa služieb podľa tejto Zmluvy zo strany dozorného orgánu alebo iného verejného orgánu v súvislosti so spracúvaním osobných údajov (ďalej len „**Úradné šetrenie**"). Zmluvné strany sú povinné vynaložiť maximálne úsilie, aby sa navzájom podporovali, a aby si zaistili spoločnú a koordinovanú komunikáciu s úradmi pri Úradnom šetrení.*

(b) *v prípade sporov, uloženia povinnosti, pokút alebo vznesenia iných nárokov zo strany dozorných orgánov alebo iných zodpovedných orgánov týkajúcich sa spracúvania osobných údajov Spoločnosti voči ktorejkoľvek zmluvnej strane, Zmluvné strany sú povinné navzájom sa informovať a oboznamovať a sú povinné spolupracovať a koordinovane postupovať s cieľom účinne sa brániť voči takýmto nárokom alebo včas dosiahnuť mimosúdne urovnanie.*

12. RETURN AND DELETION OF COMPANY PERSONAL DATA / *VRÁTENIE A VYMAZANIE OSOBNÝCH ÚDAJOV SPOLOČNOSTI*

12.1 Upon termination of the Main Contract or anytime upon request of the Company, the Service Provider shall promptly delete and procure the deletion by Sub-Processors of all copies of Company Personal Data. Service Provider will, upon request of Company return a complete copy of all Company Personal Data to Company by secure file transfer in the format requested by Company.

Pri ukončení Hlavnej zmluvy alebo kedykoľvek o to Spoločnosť požiada, Poskytovateľ služieb je povinný urýchlene vymazať a dosiahnuť vymazanie všetkých kópií osobných údajov Spoločnosti spracúvaných ďalším sprostredkovateľom. Poskytovateľ služieb na žiadosť Spoločnosti vráti Spoločnosti úplnú kópiu všetkých osobných údajov Spoločnosti použitím bezpečného prenosu súborov vo formáte požadovanom Spoločnosťou.

12.2 Service Provider may retain Company Personal Data to the extent required by applicable law and only to the extent and for such period as required by applicable law and always provided that Service Provider shall ensure that such retained Company Personal Datais (i) kept confidential and protected against unauthorized access, disclosure or use and (ii) only processed as necessary for the purpose(s) specified in the applicable law requiring its storage and for no other purpose.

Poskytovateľ služieb je oprávnený uchovávať osobné údaje Spoločnosti v rozsahu nevyhnutnom podľa príslušného práva a len v rozsahu a po takú dobu, ako to požaduje príslušné právo a vždy za predpokladu, že Poskytovateľ služieb zaistí, že uchované osobné údaje spoločnosti (i) zostanú dôverné a chránené pred neoprávneným prístupom, sprístupnením alebo použitím a (ii) budú spracúvané len na nevyhnutný účel špecifikovaný v príslušnom právnom predpise požadujúcom ich uchovávanie a na žiadny iný účel.

12.3 The Service Provider shall not have any right of retention in this respect and shall, upon request of the Company, immediately confirm full compliance with the above obligations in writing. If so reasonably requested by the Company, the Service Provider shall allow for and contribute to audits, including inspections, conducted by the Controller to ascertain compliance with this Section. Such audits are to be conducted in accordance with Section 0 accordingly.

Poskytovateľ služieb nemá žiadne právo na uchovávanie a je povinný na žiadosť Spoločnosti okamžite písomne potvrdiť splnenie vyššie uvedených povinností. Ak to môže Spoločnosť spravodlivo požadovať, Poskytovateľ služieb je povinný umožniť a spolupracovať pri auditoch, vrátane inšpekcií, vykonávaných prevádzkovateľom za účelom dosiahnutia súladu podľa tohto článku. Takéto audity musia byť vykonávané v súlade s čl. 0.

12.4 Service Provider shall promptly ensure that all Sub-Processors comply with this Section accordingly.

Poskytovateľ služieb musí urýchlene zaistiť, aby s týmto článkom vyslovili súhlas všetci ďalší sprostredkovatelia.

13. BREACH OF THIS AGREEMENT /*PORUŠENIE TEJTO ZMLUVY*

13.1 In the event of a material breach of the Service Provider's duties and obligations under this Agreement which affects the integrity and security of Company Personal Data, the Company shall be entitled to terminate this Agreement and the Main Contract for cause with immediate effect.

V prípade podstatného porušenia povinností a záväzkov vyplývajúcich z tejto Zmluvy, ktoré ovplyvňuje celistvosť a bezpečnosť osobných údajov Spoločnosti zo strany Poskytovateľa služieb, Spoločnosť bude z tohto dôvodu oprávnená ukončiť túto Zmluvu a Hlavnú zmluvu s okamžitou účinnosťou.

13.2 Notwithstanding the provisions of the Main Contract, the Service Provider shall be fully liable in accordance with applicable law for any breach of its duties under this Agreement and shall fully indemnify the Company and its Affiliates and each of their respective directors, employees and agents against and hold them harmless from any losses, liabilities, claims, damages, fines, penalties and any other costs (including reasonable costs of investigation and defence and reasonable attorneys' and other professionals' fees) suffered or incurred based upon, attributable to or arising from such breach of this Agreement. Such indemnification obligation shall not be limited by any caps or other restrictions under the Main Contract.

Bez ohľadu na ustanovenia Hlavnej zmluvy, Poskytovateľ služieb bude v súlade s príslušným právom plne zodpovedný za každé porušenie povinností podľa tejto Zmluvy a bude povinný v celom rozsahu uhradiť škodu, ktorá vznikne Spoločnosti, jej pridruženým spoločnostiam, a každému z ich členov predstavenstva, zamestnancov a zástupcov, aby ich ochránil pred akoukoľvek stratou, záväzkami, uplatnenými nárokmi, škodou, pokutami trestami a všetkými ďalšími výdavkami (zahŕňajúc odôvodnené výdavky za vyšetrovanie, obranu, trovy právnych zástupcom a iných odborníkov), ktoré vznikli na podklade vyššie uvedeného porušenia Zmluvy alebo v dôsledku takého porušenia. Povinnosť náhrady škody nebude obmedzená na základe limitov ani iných obmedzení uvedených v Hlavnej zmluve.

13.3 In the event of a dispute between the parties, the legal relationship is governed, in particular, by the GDPR and by law and the legislation of the Slovak Republic. The parties agree that the competent court shall be the general court of the Company at the time of occurrence of the dispute.

V prípade sporu medzi Zmluvnými stranami sa právny vzťah riadi predovšetkým ust. GDPR a právnymi predpismi Slovenskej Republiky.

14. AMENDMENT FOR DATA PROTECTION COMPLIANCE / *DODATOK TÝKAJÚCI SA ZHODY S OCHRANOU OSOBNÝCH ÚDAJOV*

14.1 Company may from time to time by written notice to Service Provider propose any amendments to this Agreement which Company reasonably considers to be necessary to address the requirements of applicable law. If Company gives such notice, the Parties shall promptly co-operate (and ensure that any affected Sub-Processors promptly co-operate) to ensure that appropriate amendments are made to address the requirements identified in Company's notice as soon as is reasonably practicable.

Spoločnosť je oprávnená kedykoľvek navrhnúť Poskytovateľovi služieb písomné dodatky k tejto Zmluve, ktoré Spoločnosť odôvodnene považuje za nevyhnutné za účelom splnenia požiadaviek príslušného práva. Ak Spoločnosť navrhne uzatvorenie dodatku, Zmluvné strany sú povinné urýchlene spolupracovať (a zabezpečiť aby spolupracovali aj ďalší zapojení sprostredkovatelia), aby sa uistili, že boli prijaté vhodné dodatky zodpovedajúce požiadavkám v oznámení Spoločnosti tak rýchlo, ako to je z časového hľadiska uskutočniteľné.

14.2 In the event of any changes of applicable law or guidance by supervisory authorities or any specific instructions or orders by competent supervisory authorities in relation to this Agreement, the Parties shall promptly amend this Agreement as reasonably required and appropriate to ensure compliance with such changed legal requirements.

V prípade akýchkoľvek zmien príslušného práva alebo pokynov dozorného orgánu alebo špecifických pokynov kompetentných dozorných osôb vzťahujúcich sa k tejto Zmluve, Zmluvné strany sú povinné urýchlene uzatvoriť požadovaný a vhodný Dodatok, aby došlo k naplneniu takýchto zákonných požiadaviek.

15. LIST OF DEFINITIONS / ZOZNAM VYMEZENÝCH POJMOV

"**Admissible Purpose**" has the meaning assigned to the term in Section0.

"**Agreement**" has the meaning assigned to the tem in the Preamble.

"**Affiliate**" means any legal entity directly or indirectly controlling or controlled by or under direct or indirect common control with the specified entity. "**Control**", for the purposes of this definition, means the power to direct the management and policies of such entity, directly or indirectly, whether through the ownership of voting securities, by contract or otherwise.

"**Authority Enquiries**" has the meaning assigned to the term in Section11.

"**Company Personal Data**" means any Personal Data processed by the Service Provider on behalf of the Company pursuant to or in connection with the Main Contract.

"**Contract Data Processing**" has the meaning assignedto the term in the Preamble.

"**Contract Services**" has the meaning assigned to the term in Section0.

"**Data Security Incident**" has the meaning assigned to the term in Section 0.

"**Data Security Standards**" has the meaning assigned to the term in Section 0.

"**Data Subject Requests**" has the meaning assigned to the term in Section 0.

"**EEA**" means the European Economic Area.

"**GDPR**" has the meaning assigned to the term in Section1.

"**Main Contract**" has the meaning assigned to the term in the Preamble.

"**Processing Services**" has the meaning assigned to the term in Section0.

"**Sub-Processor**" has the meaning assigned to the term in Section0.

"**Third Country**" means the countries which are not a member of the EU or EEA and have not been recognized by the European Commission as providing an adequate level of Personal Data protection, which include, as of November 2017, Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay.

*Význam termínu „**Prípustný účel**" je uvedený v článku 0.*

*Význam termínu „**Zmluva**" je uvedený v úvode Zmluvy.*

*„**Pridružená spoločnosť**" je akákoľvek právnická osoba priamo alebo nepriamo ovládaná alebo ovládajúca pod priamou alebo nepriamou kontrolu špeciálneho subjektu. „**Ovládanie**" pre účely tejto definície znamená právo riadiť vedenie a politiky takéhoto subjektu, priamo alebo nepriamo, či už na základe väčšinového hlasovacieho práva, zmluvy alebo z iného dôvodu.*

*Význam termínu „**Úradné šetrenie**" je uvedený v článku 11.*

*„**Osobné údaje Spoločnosti**" sú všetky osobné údaje spracúvané Poskytovateľom služieb v mene Spoločnosti na základe alebo v súvislosti s Hlavnou zmluvou.*

*Význam termínu „**Spracúvanie zmluvných osobných údajov**" je uvedený v úvode Zmluvy.*

*Význam termínu „**Zmluvné služby**" je uvedený v článku 0.*

*Význam termínu „**Bezpečnostný incident**" je uvedený v článku 0.*

*Význam termínu „**Štandardy zabezpečenia údajov**" je uvedený v článku 0.*

*Význam termínu „**Požiadavky dotknutých osôb**" je uvedený v článku 0.*

*„**EHP**" znamená Európsky hospodársky priestor.*

*Význam termínu „**GDPR**" je uvedený v článku 1.*

*Význam termínu „**Hlavná zmluva**" je uvedený v úvode Zmluvy.*

*Význam termínu „**Spracovateľské služby**" je uvedený v článku 0.*

*Význam termínu „**Ďalší sprostredkovateľ**" je uvedený v článku 0.*

*„**Tretia krajina**" je krajinu, ktorá nie je členom EÚ alebo EHP a nebola uznaná Európskou komisiou ako krajina poskytujúca zodpovedajúcu úroveň ochrany osobných údajov, medzi ktoré krajiny sa novembru 2017 zahŕňajú krajiny : Andorra, Argentína, Kanada, Faerské ostrovy, Guernsey, Izrael, ostrov Man, Jersey, Nový Zéland, Švajčiarsko a Uruguaj.*

16. FINAL PROVISIONS / ZÁVEREČNÉ USTANOVENIA

16.1 *Order of precedence.* This Agreement varies the terms of the Main Contract and the provisions of this Agreement are incorporated into and form part of the Main Contract as if set out in the Main Contract in full. In the event of any conflict or inconsistency, the provisions of this Agreement shall take precedence over the provisions of the Main Contract. Otherwise, the provisions of the Main Contract shall remain in full force.

Priorita zmlúv. Táto zmluva mení podmienky Hlavnej zmluvy a ustanovenia tejto Zmluvy sú do nej začlenené a tvoria súčasť Hlavnej zmluvy, ako je uvedené v Hlavnej zmluve. V prípade akéhokoľvek rozporu alebo nezrovnalosti, ustanovenia tejto Zmluvy majú prednosť pred ustanoveniami Hlavnej zmluvy. Ostatné ustanovenia Hlavnej zmluvy zostávajú v platnosti v celom rozsahu.

16.2 *Written form.* No change of or amendment to this Agreement and any of its terms shall be valid and binding unless made in writing and unless they make express reference to being a change or amendment to this Agreement. The foregoing shall also apply to the waiver of this mandatory written form.

Písomná forma. Zmeny alebo dodatky k tejto Zmluve nebudú platné a záväzné, ak nebudú urobené písomne a nebude v nich výslovne uvedené, že sú dodatkom k tejto Zmluve. Vyššie uvedené bude platiť aj v prípade zrieknutia sa povinnej písomnej formy

16.3 *Severance.* Should any provision of this Agreement be invalid or unenforceable,then the remainder of this Agreement shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein. This shall apply accordingly in the event of any unintended gaps.

Oddeliteľnosť. V prípade, ak sa niektoré ustanovenie tejto Zmluvy stane neplatným alebo nevymožiteľným, zostávajúce ustanovenia Zmluvy zostávajú platné a účinné. Neplatné alebo nevymožiteľné ustanovenia budú buď (i) doplnené podľa potreby tak, aby sa zaistila platnosť a vynútiteľnosť pri maximálnom zachovaní zámeru Zmluvných strán, a ak to nie je možné (ii) bude Zmluva vykladaná spôsobom, ako keby v nej neboli neplatné a nevymožiteľné ustanovenia vôbec zakotvené. Toto sa použije aj v prípade akýchkoľvek nezamýšľaných medzier.

16.4 *This Agreement is valid and effective upon the signature by both parties,*

Zmluva nadobúda platnosť a účinnosť dňom jej podpisu obidoma Zmluvnými stranami.

16.5 *This Agreement has been executed in the English and Slovak languages. In the case of ambiguity or discrepancies between the two versions, the Slovak version shall prevail.*

Táto Zmluva je vyhotovená v anglickom jazyku a slovenskom jazyku. V prípade nejednoznačností alebo nezrovnalostí medzi oboma verziami, je rozhodujúca slovenská verzia Zmluvy.

16.6 *This Agreement has been executed in two identical copies, one copiy to be received by Company and one by Service Provider.*

*Zmluva je vyhotovená v dv*och vyhotoveniach, z toho jedno pre Spoločnosť a jedno pre Poskytovateľa služieb.

Gbeľany, date 26.8.2018

Gbeľany, dňa 26.8.2018

Mobis Slovakia s.r.o.
MOBIS ulica 1,
013 02 Gbeľany
IČO: 35 876 557 DIČ: 2021787768
IČ DPH: SK2021787768

On behalf of: Mobis Slovakia, s.r.o.

Menom Mobis Slovakia, s.r.o.

Younghwa Kim, CEO/ konateľ

Gbeľany, date 26.8.2018

Gbeľany, dňa 26.8.2018

Stredná odborná škola elektrotechnická
Komenského č. 50
010 01 ŽILINA

On behalf of: Electrotechnical high school (SOŠE), Komenského 50, 010 01 Žilina

Menom: Stredná odborná škola elektrotechnická, Komenského 50, 010 01 Žilina

Ing. Ľubomír Králik, director/riaditeľ

ANNEX 2.2- SPECIFICATION OF DATA PROCESSING/ PRÍLOHA 1 – *ŠPECIFIKÁCIA SPRACÚVANIA OSOBNÝCH ÚDAJOV*

1. PURPOSE OF PROCESING / *ÚČEL SPRACÚVANIA*

Any Processing hereunder will be performed exclusively for the purpose of executing the Main Agreement. This includes in particular the following purposes:

(a) Maintain documentation of practical training

Akékoľvek spracúvanie údajov bude vykonávané výlučne na účel plnenia Hlavnej zmluvy. Tento zahŕňa konkrétne nasledovné účely :

(a) *Vedenie dokumentácie súvisiace s výkonom praktického vyučovania.*

2. TYPES OF PERSONAL *DATA / TIPY OSOBNÝCH ÚDAJOV SPOLOČNOSTI*

a. Common personal data of students (especially: name, surname, attendance, field of study, phone number, date of birth, class, evaluation)

a. *Bežné osobné údaje (najmä: meno, priezvisko, dochádzka, rok narodenia, telefónne číslo, trieda, študijný odbor, hodnotenie)*

3. CATEGORIES OF DATA SUBJESTS CONCERNED / *KATEGÓRIE DOTKNUTÝCH OSÔB*

(a) Students in practise

(a) *Žiaci na praxi*

4. LIST OF AUTHORIZED OPERATION/ZOZNAM POVOLENÝCH SPRACOVATEĽSKÝCH ČINNOSTÍ

collection, recording, organize, retrieval, consultation, use, store, blocking, liquidate; processing operation can only be performed in connection with the fulfillment of duties and obligation of Main contract an Agreement

získavanie, zaznamenávanie, usporadúvanie, vyhľadávanie, prehliadanie,využívanie,uchovávanie, blokovanie,vymazanie; spracovateľské činnosti sa môžu vykonávať iba v súvislosti s plnením práv a povinností podľa Hlavnej zmluvy a Zmluvy.

Osobné údaje budú spracúvané čiastočne automatizovanými prostriedkami, t.j. kombináciou ľudského faktora a technológie.

ANNEX 3.2 - DATA SECURITY STANDARDS / PRÍLOHA 2 – *ŠTANDARDY ZABEZPEČENIA ÚDAJOV*

Technical and Organizational Security Measures
Technické a organizačné bezpečnostné opatrenia

1. Physical access control / Kontrola fyzického prístupu

1.1 Physical access control / Kontrola fyzického prístupu

- Access to vulnerable building areas and rooms is controlled and documented. The implementation of physical access control measures is implemented through internal documentation.
- There are mechanical access control systems for monitoring the entry to the building/building areas.
- Details on the administration and maintenance of mechanical access control systems are included in the documentation for the access control system.
- Entries to the building or individual areas and the respective exits are logged.
- The access log data are evaluated regularly and/or on specific occasions.
- The recording of entries and exits to and from the building are used exclusively in accordance with the purpose of data protection control.
- The security system for access control is not breached by the delivery of data media, documents, lists or other media.
- A security plan for the building that also contains information on access capabilities exists.
- Security zone classifications are included in the IT security plan or security plan for the building.
- Distribution rooms (electricity, water, gas, telephone, alarm systems, etc.) are protected against unauthorized access.
- The building has continuous exterior protection.
- There are reasonable, non-mechanical access control measures for the building.
- Access logs are retained only as long as required for their intended permitted purpose.
- The Evaluation of access logs is compliant with data protection regulations.

Prístup do „citlivých" oblastí budov a miestností je kontrolovaný a zadokumentovaný. Implementácia opatrení na kontrolu fyzického prístupu je obsiahnutá v internej dokumentácii.
Pre účely monitorovania vstupu so budovy/priestorov sú zavedené mechanické systémy kontroly prístupu.
Podrobnosti o správe a údržbe mechanických systémov kontroly vstupu sú zahrnuté v dokumentácii k systému kontroly prístupu.
Zaznamenávajú sa vstupy a odchody do/z budovy alebo do jednotlivých priestorov.
Údaje o prístupoch sú vyhodnocované pravidelne alebo v prípade potreby.
Záznamy o vstupoch a odchodoch z a do budovy sú použité výlučne v súlade s účelom, dodržiavajúc zásady ochrany osobných údajov.
Doručenie nosičov dát, dokumentov, listov alebo iných médií nie je porušením bezpečnostného systému kontroly prístupu.
Informácie o možnostiach prístupu sú obsiahnuté aj v bezpečnostnom pláne budovy.
Klasifikácie bezpečnostných zón sú zahrnuté v IT bezpečnostnom pláne alebo bezpečnostnom pláne pre danú budovu.
Rozvodné miestnosti (elektrina, voda, plyn, telefón, poplašný systém atd.) sú chránené pred neoprávneným prístupom.
Budova má zabezpečenú nepretržitú externú kontrolu.
Pre budovu sú zavedené primerané, iné ako mechanické opatrenia na zabezpečenie kontroly prístupu.
Záznamy o prístupoch sa uchovávajú len tak dlho, ako je to nevyhnutné pre ich zamýšľaný dovolený účel.
Hodnotenie záznamov o prístupoch je v súlade s právnymi predpismi o ochrane osobných údajov.

1.2 Organizational access controls / Systém kontroly prístupu

- Identification is mandatory for external individuals by means of a visibly displayed visitor's pass in case it is determined by internal documentation.
- Code or ID cards that are issued to external individuals have a strictly limited period of validity

determined on the basis of the purpose of the visit.

- Visitor and company identifications are allocated in a revisable manner.
- Visitor identification is revoked daily.
- Personal details of company visitors are recorded in a visitor log/visitor list.

Ak je to zakotvené vo vnútorných predpisoch, návštevníci musia byť označení pomocou preukazu návštevníka upevneného na viditeľnom mieste.

Kód alebo preukaz vydaný návštevníkom má striktne obmedzenú dobu platnosti v závislosti od účelu návštevy.

Identifikácie návštevníkov a spoločností sú prideľované spôsobom, ktorý je možné revidovať.

Identifikácia návštevníkov má jednodňovú platnosť.

Osobné údaje návštevníkov spoločnosti sú evidované v knihe návštev / zozname návštevníkov.

1.3 Server rooms ("Closed shop" operation) / Serverovne (operácia „zavretého obchodu")

- Entries to the computer room are reduced to a low number to allow a safe control of accesses and exits.
- Measures for room surveillance of server rooms are implemented.
- The Service provider's servers operate in a closed and access-controlled area.
- Only qualified employees – classified based on explicit criteria - have access to the server rooms.
- Network components are located in dedicated, access-controlled areas.
- Maintenance and cleaning personnel shall undergo applicable access control tests for the server rooms.
- Maintenance and cleaning personnel can only move within previously defined areas.
- Regular inspection of security measures for their effectiveness is conducted.

Prístup do počítačových miestností je obmedzený na takú úroveň, aby bolo možné kontrolovať príchody a odchody.

Sú zavedené opatrenia na monitorovanie priestorov serverovien.

Servery Poskytovateľa služieb sa nachádzajú v uzatvorenej oblasti s kontrolovaným prístupom.

Do serverovien majú prístup len kvalifikovaní zamestnanci, ktorí spĺňajú presne zadefinované kritériá.

Sieťové súčasti sú umiestnené vo vyhradených priestoroch s obmedzeným prístupom.

Zamestnanci obsluhy a údržby majú prístup do serverovien len po tom, ako podstúpia príslušné kontrolné prístupové testy.

Zamestnanci obsluhy a údržby sa môžu pohybovať len vo vopred vymedzených priestoroch.

Vykonáva sa pravidelná previerka bezpečnostných opatrení s cieľom posúdiť ich účinnosť.

2. Logical access control / IT kontrola prístupu

2.1 Logical access control measures / Opatrenia na zabezpečenie IT kontroly prístupu

- A description of logical access control is available.
- Information systems and services have a formal user registration and de-registration process for granting and withdrawing/cancelling access authorizations.
- The complexity of passwords and PINs is subject to minimum requirements that meet the current state of the art.
- The procedure with passwords (e.g., prohibition of disclosure, storage) is regulated in written form.

Je k dispozícii popis IT prístupového kontrolného systému.

Informačné systémy a služby sú zabezpečené procesom formálnej užívateľskej registrácie a jej zrušenia na zabezpečenie a zamietnutie/zrušenie prístupovej autorizácie.

Komplexnosť hesiel a PIN kódov podlieha minimálnym požiadavkám vzhľadom na súčasný technický stav.

Postup na zachádzanie s heslami (napr. zákaz zverejnenia, uchovávanie) je predmetom písomnej regulácie.

2.2 Network access protection / Ochrana sieťového prístupu

- External access to the network is provided over a secure connection (e.g., VPN, certificate).
- It is ensured that only authorized persons have logical access to network components.
- There is a formal approval procedure that systems and applications involving personal data must follow before obtaining network access.
- It is ensured that only authorized devices obtain logical access to the organization's network.

- For applications that are accessible via Internet, there exists both a multistage IT architecture and a demilitarized zone (DMZ). Network segments are segregated from each other into various levels based on their security requirements to prevent data traffic between different vulnerable segments.

  Prístup do externej siete sa uskutočňuje prostredníctvom chráneného pripojenia (napr. VPN, certifikát).

  Len osoby s potrebným oprávnením majú prístup k sieťovým súčastiam.

  Systémy a žiadosti (formuláre) obsahujúce osobné údaje musia prejsť formálnym schvaľovacím procesom, než získajú prístup k sieti.

  Len tie zariadenia, ktoré získajú autorizáciu, majú prístup do siete Poskytovateľa služieb.Pre aplikácie prístupné cez internet existuje viacstupňová IT architektúra a demilitarizovaná zóna (DMZ). Sieťové súčasti sú od seba oddelené a zaradené do rôznych úrovní vzhľadom na ich bezpečnostné požiadavky za účelom zabránenia prenosu dát medzi viacerými citlivými súčasťami.

2.3 Maintenance access protection / Údržba ochrany prístupu

- For remote maintenance, a person that is an employee/authorized person of the Service provider sets up the call, i.e. the call setup takes place within the network.
- Software modifications by external personnel as part of (remote) service calls are approved by the responsible area and subsequently monitored.

  Za účelom výkonu diaľkovej údržby, osoba ktorá je zamestnancom/osobou poverenou Poskytovateľom služieb nastaví servisnú linku, t.j. linku fungujúcu v rámci siete.

  Úpravy softwaru vykonávané externými zamestnancami ako súčasť (diaľkových) servisných liniek, sú schvaľované zodpovednými osobami a následne monitorované.

3. Data access controls / Kontroly prístupu k údajom

3.1 Data access protection measures / Opatrenia na ochranu prístupu k údajom

- An authorization concept regulates the granting and withdrawal of rights.
- There is a validation process for the authorization process and the authorizations granted, and the respective documentation is available.
- Authorization processes ensure at all times that only specifically authorized persons hold admittance, access and entry authorizations to relevant installations for the provision of services (buildings, rooms, systems, network, applications) (need-to-know principle).
- All modifications to the authorizations are documented revisable to allow tracking of which authorizations were granted at which time to which persons.
- The users ensure that their DP equipment is appropriately protected when it is unattended.
- The "clean desk" and "clear screen" principles are actively implemented.
- Special security software of an external manufacturer is installed for guaranteeing data and access protection.

  Autorizačný postup reguluje poskytovanie a odvolanie práv.

  V procese autorizácie je zavedený proces potvrdenia platnosti a priznania autorizácie, k čomu je k dispozícii príslušná dokumentácia.

  Autorizačný proces v každom okamihu zaisťuje, že len osoby so špeciálnym povolením majú vstupné a prístupové oprávnenia k významným inštaláciám potrebným na zabezpečovanie servisu (budovy, miestnosti, systémy, siete, žiadosti) (princíp nevyhnutných znalostí).

  Všetky zmeny oprávnení sa evidujú, aby mohli byť preskúmané a bolo možné zistiť, akej osobe bolo aké oprávnenie v akom čase poskytnuté.

  Užívatelia dbajú na to, aby ich DP zariadenia boli v čase, keď ich nevyužívajú, vhodne chránené.

  Zaviedli sa princípy „prázdneho stolu" a „prázdnej obrazovky".

  Za účelom ochrany údajov a prístupu je nainštalovaný špeciálny bezpečnostný software od externého výrobcu.

3.2 Secure disposal or subsequent use of data media/secure deletion of documents / Bezpečná likvidácia a následné použití nosičov dát/bezpečné zmazanie dokumentov

- There are clear instructions for handling data mediums that are no longer required. This includes paper that has been written on or printed documents.
- There is a clear instruction for the disposal or subsequent use of devices equipped with storage mediums.
- Documents and data mediums whose legal, contractual or regulatory storage period has expired are being destroyed.

Sú dané jasné pokyny pre manipuláciu s nosičmi dát obsahujúcimi údaje, ktoré už nie sú potrebné. To zahŕňa aj popísaný papier alebo vytlačené dokumenty.

Sú dané jasné pokyny pre likvidáciu alebo následné použitie zariadení vybavených nosičmi dát.

Dokumenty a nosiče dát, u ktorých uplynula zákonná, zmluvná či kontrolná lehota na ich uchovávanie, sú zničené.

4. Transfer control / Kontrola prenosu

4.1 Employee requirement for data secrecy / Požiadavka na utajeniu údajov zo strany zamestnanca

- All personnel that process personal data by means of an automated process are obligated to comply with data protection regulations.
- New employees receive data protection information for the handling of personal data.
- All parties involved are aware of data security and data protection issues.
- Individuals processing personal data are trained on data protection behavior in the workplace.
- There are specific rules for the treatment of departing, especially dismissed, employees.

Všetci zamestnanci, ktorí spracovávajú osobné údaje prostredníctvom automatizovaného procesu sú povinní konať v súlade s právnymi predpismi na ochranu osobných údajov.

Noví zamestnanci obdržia informácie (pokyny) o ochrane osobných údajov pri nakladaní s osobnými údajmi.

Všetky zainteresované subjekty sú si vedomé problematiky zaistenia bezpečnosti a ochrany údajov.

Osoby, ktoré spracovávajú osobné údaje sú vyškolené, aby dodržiavali zásady bezpečného správania sa na pracovisku pri spracovávaní osobných údajov.

Vo vzťahu ku zamestnancom, ktorí z Poskytovateľa služieb *odchádzajú, špeciálne ktorí boli prepustení, sú definované špeciálne pravidlá zaobchádzania.*

4.2 Guidelines and procedures for the classification of data / Predpisy a postupy pre klasifikáciu údajov

- There is a company-wide guideline for the classification of data.

Poskytovateľ služieb *má vnútorný predpis pre klasifikáciu údajov.*

4.3 Physical data transfer / Fyzický prenos údajov

- The service provider is aware of all processes for which transfer control is required.
- Suitable security measures are implemented for the physical transport of data mediums (including paper/documents).
- The service provider has implemented appropriate security measures for the transfer of data mediums for maintenance or error analysis.
- Data transfer takes place only by verification (receipt).
- The service provider ensures that data are transmitted only to the correct addressee indicated by the company or based on the intended purposes.

Poskytovateľ služieb si je vedomý všetkých postupov, pri ktorých sa vyžaduje kontrola prenosu.

Sú zavedené vhodné bezpečnostné opatrenia pre fyzický prenos nosičov dát (vrátane papiera/ dokumentov).

Poskytovateľ služieb zaviedol príslušné bezpečnostné opatrenia pre presun nosičov dát obsahujúcich údaje pre údržbu alebo analýzu chýb.

Prenos údajov sa uskutočňuje len po odsúhlasení (o čom bude vystavený doklad).

Poskytovateľ služieb zabezpečuje, že údaje sú prenášané výlučne správnemu adresátovi, ktorého určí spoločnosť, alebo vzhľadom na zamýšľaný účel.

4.4 Electronic data transfer / Elektronický prenos údajov

- The service provider maintains a summary/list of places at which transfers can be performed under program control.
- Spec for the programs installed for automated transfers is available.
- The electronic transfer of personal data is logged in terms of involved processes, recipients of personal data, the personal data processed, date and time.

Poskytovateľ služieb vedie zoznam miest, na ktoré môže byť uskutočnený prenos pod kontrolou programu.

Pre programy inštalované na automatizované prenosy je k dispozícii špecifikácia.

Elektronický prenos osobných údajov je zaznamenávaný z hľadiska zapojených procesov, príjemcov osobných údajov, spracovávaných osobných údajov, dátumu a času.

5. Input control / Vstupná kontrola

5.1 Logs / Záznamy

- Logs indicate at the user level which applications or services a specific user has used within a defined period.
- The programs and tools used for the evaluation of input logs are documented. This also applies to used filter criteria.
- Log data for input control are protected against unauthorized viewing or manipulation.
- Clear deletion periods are set for the storage of log files for input control.
- The data for input control are subject to a strict purpose limitation and used solely for the purpose of data protection control. No behavior and performance monitoring of employees is conducted through evaluation of the log files without a specific reason.
- A Service provide's guideline/policy that contains processes for the evaluation of log files when there is suspicion of a security breach or after a security breach is available.
- The data protection officer/person authorized for personal data protection monitors the compliance with logging guidelines/policies for input control on a random basis.

Záznamy z prihlásenia ukazujú, ktoré aplikácie či služby použil konkrétny užívateľ na používateľskej úrovni v určitom období.

Programy a nástroje použité na vyhodnocovanie záznamov z prihlásenia sú zadokumentované. To platí aj pre použité filtračné kritériá.

Údaje o záznamoch z prihlásenia zo vstupnej kontroly sú chránené pred neoprávnených nazeraním alebo manipuláciou.

Pre uchovávanie súborov prihlásenia pre vstupnú kontrolu sú stanovené obdobia, kedy dochádza k ich úplnému zmazaniu.

Údaje pre vstupnú kontrolu podliehajú striktnému obmedzeniu účelu a sú použiteľné len na účel kontroly ochrany osobných údajov. Bez konkrétneho dôvodu nie je možné vykonávať použitím záznamov z prihlásenia monitoring správania sa a činnosti zamestnancov.

Poskytovateľ služieb *má k dispozícii vnútorný predpis/smernicu obsahujúce procesy hodnotenia súborov prihlásenia pri podozrení na porušenie bezpečnosti alebo procesy nastupujúce po porušení bezpečnosti.*

Zodpovedná osoba/osoba poverená ochranou osobných údajov náhodne monitoruje súlad vnútorného predpisu/smernice pre vstupnú kontrolu s právnymi predpismi.

6. Order control / Poriadková kontrola

6.1 Data protection officer (Article 37 to 39 GDPR & national law) / Zodpovedná osoba (Článok 37 až 39 nariadenia GDPR a národný predpis)

- A data protection officer is designated.
- Data protection officers shall have no conflict of interests.
- The data protection officer possesses the qualifications and reliability required for the specific company.
- The data protection officer has been designated in writing.
- The management supports the data protection officer.
- The data protection officer is directly subordinated to the management and reports directly to it.
- The data protection officer is informed and involved in the planning of new processes or the modification of existing processes on a timely basis.
- In case the service provider is not obliged to nominate the Data Protection Officer another person who will manage personal data protection must be nominated and the provisions above will be applied similarly.

V Poskytovateľovi služieb je určená zodpovedná osoba.

U zodpovednej osoby nesmie existovať žiadny konflikt záujmov.

Zodpovedná osoba je kvalifikovaná a spoľahlivá osoba podľa požiadaviek konkrétnej spoločnosti.

Zodpovedná osoba je vymenovaná písomne.

Vedenie Poskytovateľa služieb zodpovednú osobu podporuje.

Zodpovedná osoba je priamo podriadená vedeniu Poskytovateľa služieb a hlásenia podáva priamo tomuto vedeniu.

Zodpovedná osoba je včas informovaná a zapojená do plánovania nových procesov alebo zmeny existujúcich procesov.

Ak nemá Poskytovateľ služieb povinnosť menovať zodpovednú osobu, je povinný zaistiť, aby u neho bola vymenovaná iná osoba, ktorá bude zodpovedná za ochranu osobných údajov a na

ktorú sa budú aplikovať všetky vyššie uvedené ustanovenia.

6.2 The data protection officer actively participates in process design. Contractual requirement / Zodpovedná osoba se aktívne zúčastňuje tvorby procesov. Smluvná požiadavka

- All contractors in terms of processors of personal data are contractually bound by the data controller.
- The written order complies with the listing of requirements under Article 28, section 3 of the GDPR.

Všetci dodávatelia sú z hľadiska sprostredkovateľa zmluvne zviazaní s prevádzkovateľom.

Písomná objednávka musí byť v súlade s požiadavkami zakotvenými v článku 28, odd. 3 nariadenia GDPR.

6.3 Selection of contractors / Výber dodávateľov

- The company was provided with significant information on data protection and the technical and organizational measures of the service provider prior to assigning the contract.
- The decision and the reasons for the selection of the service provider were documented by the company.
- The service provider checks the compliance of the subcontractor with data protection regulations for those areas that are not confirmed by certification before the start of the processing, and monitors the subcontractor on a regular basis thereafter.

Pred uzatvorením zmluvy sú zo strany Poskytovateľa služieb, Spoločnosti poskytnuté podstatné informácie týkajúce sa ochrany osobných údajov a technických a organizačných opatrení.

Rozhodnutie a dôvody výberu Poskytovateľa služieb sú zadokumentované Spoločnosťou.

Poskytovateľ služieb ešte pred začatím spracovávania údajov a neskôr v pravidelných intervaloch kontroluje, či jeho subdodávateľ postupuje v súlade s predpismi na ochranu osobných údajov v tých oblastiach, ktoré nie sú potvrdené certifikátom.

6.4 Instructions / Pokyny

- The company appoints persons authorized to issue instructions to the service provider.
- The service provider makes a list of authorized recipients of instructions available to the company.
- Instructions are provided in writing.
- The service provider checks the identity of the issuer of instructions.

Spoločnosť vymenuje osobu oprávnenú udeľovať Poskytovateľovi služieb pokyny.

Poskytovateľ služieb vytvorí zoznam osôb, ktoré sú oprávnené tieto pokyny prijímať.

Pokyny majú písomnú formu.

Poskytovateľ služieb preverí identitu zadávateľa pokynov.

6.5 Data protection management system / Systém riadenia ochrany údajov

- With regard to the processing of personal data, risk analysis is conducted based on established and transparent criteria, and information security and data protection risks are identified, evaluated and properly handled in a compulsorily established and continuous process based on these criteria.
- There are data protection and data security plans in place specifically for the physical security of company-operated data centers and platform-specific characteristics. These can be made available on request.
- All documents that are to be made available are issued in a way as to make it possible for informed third parties to review the respective information security implemented and the data security measures executed. The documentation is kept up to date. Documentation with modified contents is made available on request.
- Sufficient resources are made available for establishing, implementing, executing, monitoring, reviewing, maintaining and improving the data management system and proof of the availability exists.
- It is guaranteed that only personnel that have sufficient skills to comprehend the assigned tasks are involved in operating the data protection management system. This is ensured by instruction and other training measures.
- Continuous improvement of Data Protection Management System is based on the Plan-Do-Check-Act Cycle, under which the company becomes aware on request of the Plan phase.
- Data protection measures are based on defined protection requirements for IT applications, IT systems and networks (as defined by the responsible area).
- Security indicators that threaten the processing of personal data are monitored so that

incidents (e.g., virus or malware incidents, abuse of root rights, hacker attacks, etc.) can be reacted against quickly.

- Processes have been established that ensure the implementation of rights of affected individuals. These include:
- Information regarding personal data processed and provision of a copy of those data
  - Rectification and completion of personal data
  - Erasure of personal data on request
  - Restriction of personal data
  - Data portability/transfer
  - Right to object
  - Data protection by design and default (Privacy by Design and Default)
- A process protects the data subjects rights to a data protection impact assessment (risk analysis process) if the processing is likely to result in a high risk to the rights and freedoms of natural persons based on the nature, scope, context and purposes of the processing.
- Hardware and software products are obtained from acknowledged and responsible sources. There is reliable technical support and a traceable supply chain.
- The institution and use of administrative access is subject to formal procedures that describe how roles, accounts, access rights and privileges for administrative access are set up, regularly reviewed, modified, disabled and deleted. Administrative access to systems is limited to a minimum number of administrators and protected by double authentication or a similar security measure, and always recorded.
- Information regarding technical weaknesses of data systems in use is obtained on a timely basis, the vulnerability of the organization to exploitation of such weaknesses is evaluated and appropriate measures for dealing with the resultant risk are implemented. The patch roll-out is agreed upon with the company.
- It is ensured that resource use is monitored and agreed upon with the company to ensure the contractually agreed adequate systems performance. Agreed capacities may not be directed to other users without agreement of the company.
- Personal data on hardware that is to be discarded is irretrievably deleted to the highest possible state of the art, or the hardware is completely destroyed securely.
- Subcontractors are required to comply at least with the requirements agreed upon with the company. Implementation and monitoring of reasonable measures are ensured by the subcontractors.

S poukazom na ochranu osobných údajov sa vykonáva analýza rizík založená na transparentných a zadefinovaných kritériách, v rámci ktorej sú identifikované riziká informačnej bezpečnosti a ochrany dát, následne sú vyhodnotené a riešené v povinne zavedenom a pokračujúcom procese založenom na týchto kritériách.

Sú zavedené plány ochrany a bezpečnosti údajov, špeciálne fyzickej ochrany dátových centier Poskytovateľa služieb *a platformových charakteristík. Tieto je možné dať na vyžiadanie k dispozícii.*

Všetky dokumenty, ktoré majú byť k dispozícii sú vydávané tak, aby boli dostupné informovaným tretím stranám na preskúmanie bezpečnostných informácií a opatrení prijatých na zabezpečenej údajov. Dokumentácia sa neustále aktualizuje. Upravená dokumentácia je na vyžiadanie k dispozícii.

K dispozícii sú dostatočné zdroje na zavedenie, vykonávanie, aplikovanie, monitorovanie, modifikovanie, udržiavanie a zlepšovanie systému riadenia ochrany dát a existuje dôkaz o ich dostupnosti.

Je zaručené, že len zamestnanci s dostatočnými schopnosťami pre splnenie zadaných úloh sú zahrnutí do systému riadenia ochrany údajov. To sa zaisťuje pokynmi a inými školiacimi opatreniami.

Neustále zlepšovanie systému riadenia ochrany údajov je založené na PDCA cykle, o ktorého fáze plánovania je Spoločnosť na vyžiadanie informovaná.

Opatrenia na ochranu údajov sú založené na zadefinovaných bezpečnostných požiadavkách pre IT aplikácie, IT systémy a siete (podľa zadefinovanej oblasti zodpovednosti).

Bezpečnostné identifikátory, ktoré ohrozujú spracovanie osobných údajov sú monitorované, takže na incidenty (napr. vírusy, malware, zneužitie základných práv, hackerské útoky) je možné rýchlo zareagovať.

Sú zavedené procesy, ktoré zaisťujú vykonávanie práv dotknutých osôb. Tieto zahŕňajú :

- *Informácie týkajúce sa spracúvania osobných údajov a poskytnutie kópie týchto údajov.*
- *Oprava a doplnenie osobných údajov.*
- *Výmaz osobných údajov na základe žiadosti.*
- *Obmedzenie spracúvania osobných údajov.*

- *Prenosnosť údajov.*
- *Právo namietať.*
- *Špecificky navrhnutá a štandardná ochrana údajov (Špecifické a štandardné súkromie).*

Ak je pravdepodobné, že spracovávanie údajov bude viesť k vysokému riziku ohrozenia práv a slobôd fyzických osôb vzhľadom na povahu, rozsah, obsah a účel spracovania, je zadefinovaný proces ochrany práv dotknutých osôb a posúdenie dopadu ochrany údajov (proces analýzy rizík).

Hardware a software sú získavané len z overených a dôveryhodných zdrojov. Je zavedená spoľahlivá technická podpora a vysledovateľná dodávateľská línia.

Zavedenie a použitie administratívneho prístupu je predmetom formálneho procesu, ktorý popisuje, ako sú nastavené úlohy, účty, prístupové práva a výhody administratívneho prístupu. Tento proces je pravidelne revidovaný, upravovaný, vyradený a vymazaný. Administratívny prístup do systému je limitovaný pre minimálne množstvo administrátorov a chránený dvojitým overením alebo obdobným bezpečnostným opatrením, a je vždy nahrávaný.

Informácie o slabých miestach používaných dátových systémov sú pravidelne získavané, zraniteľnosť spoločnosti v dôsledku týchto slabých stránok je vyhodnocovaná a sú prijímané opatrenia na zaobchádzanie s výslednými rizikami. Riešenia sú prijímané so súhlasom Spoločnosti.

Je zabezpečené, že použitie zdrojov je monitorované a odsúhlasené spoločnosťou, tak aby bol zabezpečený zmluvne dohodnutý výkon. Dohodnuté kapacity nesmú byť prenesené na iných užívateľov bez súhlasu spoločnosti.

Osobné údaje na hardware, ktoré majú byť neobnoviteľne vymazané sa zmažú spôsobom uskutočniteľným vzhľadom na súčasný stav techniky, prípadne bude zničený celý hardware.

Subdodávatelia musia konať minimálne v súlade s požiadavkami spoločnosti. Subdodávatelia zabezpečia zavedenie a monitorovanie primeraných opatrení.

7. Availability checks / Kontroly dostupnosti

7.1 Risk and vulnerability analysis / Analýza rizika a citlivosti

- A risk and vulnerability analysis that also includes consideration of risk factors to maintaining the DP operation is available.
- Vulnerabilities are eliminated or a plan of action for remedying noted vulnerabilities and risks is created.

K dispozícii je tiež analýza rizika a zraniteľnosti, ktorá zahŕňa zváženie rizikových faktorov pri udržiavaní DP operácií.

Zraniteľné miesta sú odstránené a je vytvorený akčný plán pre odstránenie známych zraniteľných miest a rizík.

7.2 Disaster preparedness and IT emergency plan / Príprava na krízové situácie a núdzový IT plán

- All potential disasters such as strikes, absenteeism, property damage, fire, explosion, earthquake, flood, etc. are taken into consideration.
- Alternative space is available for the operation.
- A backup server center is provided.
- An IT security officer is appointed for the Service provider.
- Written specifications and documents exist for recovery of the IT systems after a disaster.
- Emergency drills are held regularly.

Do úvahy boli brané všetky možné krízové situácie, ako je napr. štrajk, pracovné absencie, škoda na majetku, požiar, požiar, výbuch, zemetrasenie či povodeň.

Na mimoriadne operácie je dostupný alternatívny priestor.

K dispozícii je tiež záložný server.

Poskytovateľ služieb *má vymenovaného IT bezpečnostného referenta.*

Pre obnovenie IT systémov po katastrofe sú zavedené písomné špecifikácie a dokumenty.

Pravidelne sa konajú nácviky núdzových situácií.

7.3 Backup concept / Záložný koncept

- Accurate documentation exists in terms of the requirements of a backup concept.
- Backup media are adequately protected against theft and destruction.
- The company has approved processes for data protection available and they are documented in operating instructions.
- The individuals competent and responsible for data protection are designated by name. Their responsibilities are documented.

- Capacity planning for data protection is available.
- The restoration and integrity of available backups is tested regularly.

Existuje presná dokumentácia vzhľadom na požiadavky na záložný koncept.

Záložné médiá sú adekvátne chránené proti krádeži a zničeniu.

Poskytovateľ služieb *má k dispozícii schválené procesy pre ochranu údajov a sú zadokumentované v návodoch na použitie.*

Osoby zodpovedné za ochranu osobných údajov sú vymenovaní. Ich zodpovednosť je zadokumentovaná.

Pre ochranu osobných údajov sú naplánované kapacity.

Obnovenie a integrita dostupných záložných systémov sa pravidelne testuje.

7.4 Storage of business documents / Uchovávanie obchodných dokumentov

- Only the most necessary personnel have access to the archive areas. Access authorizations are documented in the archive regulations.
- An archivist is appointed for the archive.
- Data mediums and documents are issued and stored only by authorized archive personnel.

Do archívov má prístup len nevyhnutný počet zamestnancov. Prístupové autorizácie sú zadokumentované v archívnom poriadku.

Pre archív je vymenovaný archivár.

Nosiče údajov a dokumenty sú spravované a skladované len autorizovaným archívnym personálom.

7.5 Other security measures / Ostatné bezpečnostné opatrenia

- Written service instructions for all security measures are available.
- Whether employees are observing the security measures that apply to them is checked on a regular basis.
- Employees are regularly trained in the handling of security devices and compliance with security instructions.

Pre všetky bezpečnostné opatrenia sú k dispozícii písomné služobné pokyny.

Pravidelne sa vykonávajú kontroly za účelom posúdenia dodržiavania bezpečnostných opatrení zamestnancami.

Zamestnanci sú pravidelne školení v oblasti nakladania s bezpečnostnými zariadeniami a v oblasti dodržiavania bezpečnostných pokynov.

8. Segregation control / Kontrola oddeľovania

- Office, development, testing and production systems are operated (at least logically) in clearly separated grid segments.
- Exclusively test data are used for testing and development purposes.
- There is a concept for the creation and implementation of test data.

Kancelárie, vývoj, testovanie a výrobné systémy sa sú prevádzkované v jasne oddelených sieťových segmentoch.

Testovacie údaje sú používané výlučne na účely testovania a vývoja.

Je zavedený koncept pre vytváranie a zavádzanie testovacích údajov.

Gbeľany, date 26.8.2018 *Gbeľany, dňa 26.8.2018*	Gbeľany, date 26.8.2018 *Gbeľany, dňa 26.8.2018*
IČ DPH: SK2021787768 On behalf of Company/controller *Za Spoločnosť/prevádzkovateľa* Younghwa Kim, CEO/ konateľ	On behalf of: Electrotechnical high school (SOŠE), Komenského 50, 010 01 Žilina *Menom: Stredná odborná škola elektrotechnická, Komenského 50, 010 01 Žilina* Ing. Ľubomír Králik, director/riaditeľ