Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností uzatvorená podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov a § 19 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov v spojení s § 8 ods. 2 vyhl. Národného Bezpečnostného Úradu (ďalej len „NBÚ) č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení v platnom znení (ďalej len „Zmluva")

Contract for the Provision of Security Measures and Notification Obligations concluded in accordance with § 269 para. 2 of Act No. 513/1991 Coll., Commercial Code, as amended by later regulations, and § 19 para. 2 of Act No. 69/2018 Coll. on Cybersecurity and on amendments to certain laws, as amended by later regulations, in conjunction with § 8 para. 2 of Regulation No. 362/2018 Coll. of the National Security Authority (hereinafter referred to as the "NSA"), determining the content of security measures, the content and structure of security documentation, and the scope of general security measures in the current wording (hereinafter referred to as the "Contract").

---

medzi

1. **Prevádzkovateľom základnej služby**
   Názov: Univerzitná nemocnica Martin
   Sídlo: Kollárova 2 , 036 59 Martin,
   Štatutárny orgán:
   MUDr. Peter Durný, PhD. MPH, riaditeľ

   IČO: 00365327
   DIČ: 2020598019

(ďalej len „Prevádzkovateľ základnej služby a/alebo Odberateľ")

a

2. **Dodávateľom na výkon činností**
   Obchodné meno: AZmed, A simplified joint-stock company
   Sídlo: 6, rue Leonard da Vinci, 53000 Laval France

   Oprávnená osoba : Julien Vidal .....

   (ďalej ako Dodávateľ)

Odberateľ a Dodávateľ spolu ďalej ako „Zmluvné strany" a každý samostatne ako „Zmluvná strana"

Preambula

Zmluvné strany uzatvárajú túto Zmluvu za účelom špecifikácie plnenia bezpečnostných opatrení a notifikačných povinností v nadväznosti na ***Zmluvu o výpožičke*** *zo dňa* ***17.11.2024*** *uzavretú medzi Dodávateľom a Prevádzkovateľom základnej služby (ďalej v tomto texte len „Osobitná zmluva").*

between

1. **The Operator of the essential service**
   Name: University Hospital Martin
   Registered office: Kollárova 2, 036 59 Martin
   Legal representative:
   MUDr. Peter Durný, PhD. MPH, Director

   ID: 00365327
   Tax ID: 2020598019

   (hereinafter referred to as the "Operator of the essential service and/or Customer")

and

2. **The Supplier for the performance of activities**
   Name: AZmed, A simplified joint-stock company
   Registered office: 6, rue Leonard da Vinci, 53000 Laval, France

   Authorized representative: Julien Vidal .....

   (hereinafter referred to as the "Supplier")

The Customer and the Supplier collectively hereinafter referred to as the "Contracting Parties," and each individually as a "Contracting Party".

Preamble

The Contracting Parties enter into this Agreement for the purpose of specifying the implementation of security measures and notification obligations in connection with the **Loan Agreement** dated **November 17, 2024**, concluded between the Supplier and the Operator of the essential service (hereinafter referred to in this document as the "Separate agreement").

Článok 1
Úvodné ustanovenia

1. Odberateľ je prevádzkovateľom základnej služby v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších zmien (ďalej ako „zákon o kybernetickej bezpečnosti").
2. Odberateľ vyhlasuje, že si je vedomý svojich zmluvných a zákonných povinností, prijal všetky potrebné bezpečnostné opatrenia, ktoré bude počas platnosti tejto zmluvy udržiavať, má zodpovedajúce materiálne, technické a personálne vybavenie a zaväzuje sa poskytnúť Dodávateľovi potrebnú súčinnosť a informácie, aby mohol efektívne napĺňať účel a predmet tejto Zmluvy.
3. Dodávateľ prehlasuje, že sa detailne oboznámil s rozsahom a povahou požadovaných bezpečnostných opatrení a notifikačných povinností podľa tejto Zmluvy a že disponuje technickým vybavením, kapacitami a odbornými znalosťami, ktoré sú potrebné pre zaistenie požiadaviek podľa tejto Zmluvy.
4. Dodávateľ sa zaväzuje vykonávať všetky činnosti definované v tejto Zmluve v súlade s všeobecne záväznými právnymi predpismi. Zmluvné strany zhodne prehlasujú, že nič v tejto zmluve nezbavuje zmluvné strany zodpovednosti za plnenie vlastných povinností, ktoré im vyplývajú z právnych predpisov vydaných v súlade so zákonom o kybernetickej bezpečnosti a zo zákona o kybernetickej bezpečnosti.
5. Pojmy uvedené v tejto zmluve sa zhodujú s pojmami definovanými zákonom o kybernetickej bezpečnosti a v prípade ich slovnej nezhody sa použijú ustanovenia zákona o kybernetickej bezpečnosti, ktoré sú im významom najbližšie.
6. Práva a povinnosti Zmluvných strán neupravené v tejto Zmluve sa riadia príslušnými ustanoveniami Obchodného zákonníka, Osobitnou zmluvou, zákonom o kybernetickej bezpečnosti vyhl. NBÚ č. 362/2018 Z.z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení a inými všeobecne záväznými právnymi predpismi.
7. Zmluva stanovuje základné úlohy a princípy spolupráce Zmluvných strán s cieľom zabezpečiť kybernetickú bezpečnosť sietí a informačných systémov Odberateľa počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom, ktoré by sa mohli dotknúť sietí a informačných systémov Odberateľa a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby zo

Article 1
Introductory Provisions

1. The Customer is the operator of an essential service in accordance with Act No. 69/2018 Coll. on Cybersecurity and on amendments to certain laws, as amended by later regulations (hereinafter referred to as the "Cybersecurity Act").
2. The Customer declares that it is aware of its contractual and legal obligations, has adopted all necessary security measures, which it will maintain during the validity of this agreement, possesses appropriate material, technical, and personnel resources, and undertakes to provide the Supplier with the necessary cooperation and information to effectively fulfil the purpose and subject matter of this Agreement.
3. The Supplier declares that it has thoroughly familiarized itself with the scope and nature of the required security measures and notification obligations under this Agreement and possesses the technical equipment, capacities, and professional knowledge necessary to ensure compliance with the requirements of this Agreement.
4. The Supplier undertakes to perform all activities defined in this Agreement in accordance with generally binding legal regulations. The Contracting Parties jointly declare that nothing in this agreement relieves the Contracting Parties of the responsibility for fulfilling their own obligations arising from legal regulations issued in accordance with the Cybersecurity Act and the Act on Cybersecurity.
5. Terms defined in this Agreement correspond to the definitions in the Cybersecurity Act, and in case of any discrepancy in wording, the provisions of the Cybersecurity Act that are closest in meaning shall apply.
6. Rights and obligations of the Contracting Parties not regulated in this Agreement shall be governed by the relevant provisions of the Commercial Code, the Separate Agreement, the Cybersecurity Act, Regulation of the National Security Authority No. 362/2018 Coll., determining the content of security measures, the content and structure of security documentation, and the scope of general security measures, and other generally binding legal regulations.
7. The Agreement establishes the basic tasks and principles of cooperation between the Contracting Parties with the aim of ensuring the cybersecurity of the networks and information systems of the Customer throughout their life cycle, preventing cybersecurity incidents that could affect the networks and information systems of the Customer, and minimizing the impact of cybersecurity incidents on the continuity of the provision of essential services by the Customer (hereinafter referred to as the "purpose"), including in collaboration with the Supplier.

strany Odberateľa (ďalej len „účel"), a to aj v spolupráci s Dodávateľom.

Článok 2
Predmet zmluvy

1. Predmetom tejto Zmluvy je určenie práv a povinností Zmluvných strán pri plnení bezpečnostných opatrení a notifikačných povinností v zmysle zákona o kybernetickej bezpečnosti realizovaných v nadväznosti na Osobitnú zmluvu.
2. Dodávateľ sa zaväzuje zaistiť pri poskytovaní služieb Odberateľovi dodržiavanie bezpečnostných požiadaviek, ktoré sú kladené na tretie strany v zmysle § 19 zákona o kybernetickej bezpečnosti a Vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška NBÚ").
3. Dodávateľ sa zároveň zaväzuje zachovávať mlčanlivosť a dôvernosť dôverných informácií, ak mu budú zo strany Odberateľa poskytnuté a poskytovať im náležitú ochranu, aby nedošlo k ich prezradeniu tretím osobám alebo k ich sprístupneniu verejnosti, k ich zneužitiu alebo k akejkoľvek neoprávnenej manipulácii s nimi.
4. Miestom plnenia tejto Zmluvy sú najmä pracovisko alebo sídlo Odberateľa, pracovisko alebo sídlo Dodávateľa, alebo pracoviská a sídla subdodávateľov v zmysle Osobitnej zmluvy. V prípade zmeny alebo doplnenia sídla alebo pracoviska zo strany Zmluvných strán, vykonajú tak Zmluvné strany oznamom zaslaným e-mailom na kontaktné osoby uvedené v záhlaví tejto Zmluvy najneskôr do 30 dní od vykonania tejto zmeny.
5. Bezpečnostné opatrenia a notifikačné povinnosti sa Dodávateľ zaväzuje plniť od okamihu nadobudnutia účinnosti tejto Zmluvy až do skončenia platnosti Osobitnej zmluvy, pokiaľ z právnych predpisov uvedených v tejto Zmluve alebo z tejto Zmluvy nevyplývajú určité povinnosti pre Dodávateľa aj po skončení platnosti Osobitnej zmluvy.

Článok 3
Práva a povinnosti Dodávateľa

1. Odberateľ je povinný bezodkladne po uzavretí Zmluvy oboznámiť Dodávateľa s bezpečnostnou politikou informačných systémov upravenou v aktuálnych vnútorných predpisoch Odberateľa. Dodávateľ sa zaväzuje oboznámiť sa a dodržiavať bezpečnostnú politiku informačných systémov Odberateľa v časti, v ktorej je služba Dodávateľa pripojená k sieti základnej služby alebo

Article 2
Subject of the Agreement

1. The subject of this Agreement is to determine the rights and obligations of the Contracting Parties in the implementation of security measures and fulfilment of notification obligations in accordance with the Cybersecurity Act, carried out in connection with the Separate Agreement.
2. The Supplier undertakes to ensure compliance with security requirements placed on third parties in accordance with § 19 of the Cybersecurity Act and Regulation No. 362/2018 Coll. of the National Security Authority, determining the content of security measures, the content and structure of security documentation, and the scope of general security measures (hereinafter referred to as "NSA regulation").
3. The Supplier also commits to maintaining confidentiality and secrecy of confidential information provided by the Customer, ensuring their proper protection to prevent their disclosure to third parties or their public release, misuse, or any unauthorized manipulation.
4. The place of performance of this Agreement is primarily the workplace or registered office of the Customer, the workplace or registered office of the Supplier, or the workplaces and registered offices of subcontractors in accordance with the Separate Agreement. In the event of a change or amendment to the registered office or workplace by the Contracting Parties, the Parties shall notify each other by email to the contact persons specified in the header of this Agreement no later than 30 days from the date of such change.
5. The Supplier undertakes to fulfill security measures and notification obligations from the effective date of this Agreement until the expiration of the Separate Agreement, unless legal regulations specified in this Agreement or arising from this Agreement impose certain obligations on the Supplier even after the expiration of the Separate Agreement.

Article 3
Rights and Obligations of the Supplier

1. The Customer is obligated, immediately after the conclusion of the Agreement, to inform the Supplier about the security policy of information systems regulated in the current internal regulations of the Customer. The Supplier undertakes to familiarize itself with and adhere to the security policy of the Customer's information systems in the part where the service of the Supplier is connected to the network of the essential service or

informačného systému základnej služby (ďalej ako „bezpečnostná politika") a súčasne s ňou Dodávateľ vyjadruje svoj súhlas. O oboznámení sa s bezpečnostnou politikou a vyjadrení súhlasu s ňou si Zmluvné strany vydajú písomné potvrdenie.

2. Dodávateľ súhlasí s tým, že bezpečnostná politika Odberateľa sa môže priebežne meniť a dopĺňať tak, aby zodpovedala aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov Odberateľa a aktuálnym hrozbám dotýkajúcim sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Odberateľa. Odberateľ je povinný bezodkladne oboznámiť Dodávateľa s aktualizovanou bezpečnostnou politikou s dôrazom na zmeny v nej uvedené, pričom Dodávateľ následne písomne potvrdí, že sa so zmenami bezpečnostnej politiky oboznámil a súhlasí s nimi.
3. Dodávateľ sa zaväzuje chrániť všetky informácie poskytnuté Odberateľom, najmä chrániť ich integritu, dostupnosť a dôvernosť pri ich spracovaní a nakladaní s nimi v prostredí Dodávateľa.
4. Dodávateľ sa zaväzuje hlásiť všetky potrebné informácie požadované Odberateľom pri zabezpečovaní požiadaviek kladených na Odberateľa podľa zákona o kybernetickej bezpečnosti alebo vyhlášky NBÚ, a to zaslaním e-mailu na kontaktnú osobu Odberateľa uvedenú v tejto Zmluve a to bezodkladne.
5. Dodávateľ sa zaväzuje hlásiť všetky informácie, ktoré majú vplyv na túto Zmluvu zaslaním e-mailu na kontaktnú osobu Odberateľa uvedenú v tejto Zmluve, a to bezodkladne.
6. V oblasti technických zraniteľností systémov a zariadení realizuje Dodávateľ opatrenia podľa § 9 vyhlášky NBÚ, najmä identifikuje technické zraniteľnosti informačných systémov, ktoré využíva pri poskytovaní služieb Odberateľovi a ktoré toto poskytovanie služieb Odberateľovi ovplyvňujú, napríklad prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľným účinkom:

a. Zavedenie a prevádzka nástroja alebo mechanizmu určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí, ak sú súčasťou poskytovaných služieb.
b. Zavedenie a prevádzka nástroja alebo mechanizmu určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí, ak sú súčasťou poskytovaných služieb.
c. Využitie verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.

7. Dodávateľ je ďalej povinný :

the information system of the essential service (hereinafter referred to as the "security policy") and concurrently expresses its consent to it.

2. The Supplier agrees that the Customer's security policy may be continuously changed and supplemented to align with current security measures, the current state of the Customer's networks and information systems, and current threats affecting the Supplier that could potentially have an adverse impact on the essential service of the Customer. The Customer is obligated to promptly inform the Supplier of the updated security policy, with an emphasis on the changes therein, and the Supplier subsequently confirms in writing that it has familiarized itself with the changes to the security policy and agrees to them.

3. The Supplier undertakes to protect all information provided by the Customer, especially ensuring their integrity, availability, and confidentiality during processing and handling in the Supplier's environment.

4. The Supplier commits to reporting all necessary information requested by the Customer in fulfilling the requirements imposed on the Customer by the Cybersecurity Act or the NSA regulation. This shall be done by sending an email to the Customer's designated contact person specified in this Agreement promptly.

5. The Supplier commits to report all information that may impact this Agreement by sending an email to the Customer's designated contact person specified in this Agreement promptly.

6. In the field of technical vulnerabilities of systems and devices, the Supplier implements measures according to § 9 of the NSA regulation, particularly identifying technical vulnerabilities in information systems that it exploits while providing services to the Customer and that impact the provision of services to the Customer. This includes measures defined in the following points or measures with comparable effects:

a. Implementation and operation of a tool or mechanism designed to detect existing vulnerabilities in software tools and their components if they are part of the provided services.
b. Implementation and operation of a tool or mechanism designed to detect existing vulnerabilities in technical means and their components if they are part of the provided services.
c. Utilization of publicly available lists provided by manufacturers that describe vulnerabilities in software and technical devices..

7. The supplier is further obligated:

a. zabezpečiť vlastnú kybernetickú bezpečnosť, aby cez Dodávateľa nebolo možné zasiahnuť siete a informačné systémy Odberateľa,
b. vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení tejto Zmluvy alebo budú mať prístup k informáciám Odberateľa,
c. sledovať hrozby dotýkajúce sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Odberateľa („incidenty"),
d. predchádzať vzniku incidentov,
e. systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o incidentoch,
f. prijímať od Odberateľa varovania a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potencionálny nepriaznivý vplyv na základnú službu Odberateľa,
g. zasielať Odberateľovi včasné varovania pred incidentmi, o ktorých sa dozvie z vlastnej činnosti podľa tejto zmluvy alebo inak, a to bezodkladne,
h. spolupracovať s Odberateľom pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov Odberateľa,
i. po ukončení zmluvného vzťahu vrátiť, previesť alebo aj zničiť všetky informácie, ku ktorým má Dodávateľ počas trvania Osobitnej zmluvy s Odberateľom prístup. Rovnakú povinnosť má Dodávateľ aj v prípade skončenia účelu spracúvania týchto informácií, ak o to požiada Odberateľ, a to bezodkladne, prípadne v lehote určenej Odberateľom,
j. okrem už uvedeného prijať a dodržiavať bezpečnostné opatrenia minimálne v oblastiach podľa § 20 ods. 3 písm. d), e), f), g) h), j), k) a m) zákona o kybernetickej bezpečnosti v rozsahu podľa § 8, 10, 12, 14 a 15 vyhlášky NBÚ, a v rozsahu špecifikovanom v bezpečnostnej politike Odberateľa,
k. spolupracovať s Odberateľom v oblasti kybernetickej bezpečnosti tak, aby nedošlo ku kybernetickým incidentom a/alebo iným situáciám, ktoré by mohli mať vplyv na bezpečnosť a/alebo poskytovanie služieb
l. s poukazom na ust. § 8 ods. 2 písm. p) vyhlášky NBÚ po ukončení tejto Zmluvy udeliť, poskytnúť, previesť alebo postúpiť všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby na Odberateľa; tento záväzok Dodávateľa ostáva v platnosti po dobu najmenej piatich rokov po ukončení tejto Zmluvy.

a. ensure its own cybersecurity to prevent any interference with the networks and information systems of the Customer through the Supplier,
b. create and enhance the security awareness of its employees who will be involved in the fulfilment of this Agreement or will have access to the Customer's information,
c. monitor threats affecting the Supplier that could potentially have an adverse impact on the fundamental service of the Customer ("incidents"),
d. prevent the occurrence of incidents,
e. systematically obtain (monitor and detect), concentrate (record), analyze, and evaluate information about incidents,
f. receive warnings from the Customer and take preventive measures necessary to avert threats that could potentially have an adverse impact on the fundamental service of the Customer,
g. promptly send warnings to the Customer about incidents learned through its own activities under this agreement or otherwise,
h. collaborate with the Customer in ensuring the cybersecurity of the Customer's networks and information systems,
i. after the termination of the contractual relationship, return, transfer, or destroy all information to which the Supplier has access during the duration of the Separate Agreement with the Customer. The Supplier has the same obligation in case of the termination of the purpose of processing this information, if requested by the Customer, immediately or within the deadline specified by the Customer,
j. in addition to the above, accept and adhere to security measures at least in the areas according to § 20 para. 3 letters d), e), f), g), h), j), k), and m) of the Cybersecurity Act, to the extent specified in § 8, 10, 12, 14, and 15 of the NSA regulation, and in the scope specified in the Customer's security policy,
k. collaborate with the Customer in the field of cybersecurity to prevent cybersecurity incidents and/or other situations that could affect the security and/or provision of services,
l. with reference to § 8 para. 2 letter p) of the NSA regulation, after the termination of this Agreement, grant, provide, transfer, or assign all necessary licenses, rights, or consents to ensure the continuity of the operated fundamental service to the Customer. This Supplier's commitment remains valid for at least five years after the termination of this Agreement.

8. Dodávateľ sa zaväzuje, že všetky činnosti a plnenia podľa tejto Zmluvy zabezpečí riadne a včas spravidla vlastnými kapacitami. Dodávateľ môže zapojiť do poskytovania služieb podľa tejto Zmluvy ďalšieho dodávateľa (ďalej len „subdodávateľ"), ak mu to vyplýva z ustanovení Osobitnej zmluvy. Ak Dodávateľ zapojí do poskytovanie služieb subdodávateľa, vzťahujú sa na neho rovnaké podmienky ako na samotného Dodávateľa. Za plnenie povinností svojich subdodávateľov podľa tejto Zmluvy zodpovedá priamo Dodávateľ tak, ako by ich poskytoval sám.
9. Dodávateľ sa zaväzuje dokumentovať svoju činnosť podľa tejto Zmluvy (vrátane evidovania incidentov a dokumentovania školení svojich zamestnancov) a na žiadosť Odberateľa mu predložiť uvedenú dokumentáciu na nahliadnutie a zhotovenie kópií.
10. Zoznam pracovných rolí Dodávateľa a zoznam jeho zamestnancov, ktorí majú mať prístup k informáciám a údajom Odberateľa, s ktorými prídu do styku v súvislosti s plnením tejto Zmluvy, je uvedený v prílohe č. 1, ktorá je neoddeliteľnou súčasťou tejto Zmluvy. Dodávateľ je povinný písomne oznámiť Odberateľovi každú zmenu v personálnom obsadení; na platnosť takejto zmeny sa nevyžaduje uzatvorenie dodatku k tejto Zmluve. Dodávateľ je povinný zaviazať povinnosťou mlčanlivosti podľa ust. § 12 zákona o kybernetickej bezpečnosti osoby, ktoré sa budú podieľať na plnení tejto Zmluvy.
11. Dodávateľ sa zaväzuje, že bez písomného súhlasu Odberateľa nepostúpi svoje peňažné pohľadávky, ktoré vzniknú z tejto Zmluvy iným tretím osobám. Postúpenie pohľadávky zo strany Dodávateľa tretej osobe bez súhlasu Odberateľa je neplatné. Súhlas Odberateľa je platný len za podmienky, že bol na takýto úkon udelený predchádzajúci súhlas MZ SR. V prípade porušenia tejto povinnosti je Dodávateľ povinný uhradiť Odberateľovi zmluvnú pokutu vo výške 2 % z istiny pohľadávky. Uvedené sa neuplatní, ak osobitný právny predpis vzťahujúci sa na pohľadávku vyplývajúcu z takejto Zmluvy vylučuje možnosť podmieniť postúpenie pohľadávky súhlasom Odberateľa ako dlžníka.
12. Zmluvné strany sa dohodli, že Dodávateľ neprijme vyhlásenie podľa § 303 a nasl. Obchodného zákonníka. V prípade porušenia tejto povinnosti je Dodávateľ povinný uhradiť Odberateľovi zmluvnú pokutu vo výške 2 % z istiny pohľadávky. Uvedené sa neuplatní, ak osobitný právny predpis vylučuje uzavretie dohody podľa predchádzajúcej vety.

Článok 4

Riešenie kybernetických bezpečnostných incidentov

8. The Supplier undertakes to ensure all activities and fulfilments under this Agreement properly and on time, usually with its own capacities. The Supplier may involve another provider ("subcontractor") in providing services under this Agreement if it arises from the provisions of the Separate Agreement. If the Supplier involves a subcontractor in providing services, the same conditions apply to the subcontractor as to the Supplier itself. The Supplier is directly responsible for the fulfilment of the obligations of its subcontractors under this Agreement, as if the Supplier were providing them itself.

9. The Supplier undertakes to document its activities under this Agreement (including incident recording and documentation of its employees' training) and, upon the Customer's request, provide the documentation for inspection and copying.

10. The list of the Supplier's job roles and the list of its employees who will have access to the Customer's information and data in connection with the fulfilment of this Agreement are provided in Annex No. 1, which is an integral part of this Agreement. The Supplier is obligated to inform the Customer in writing of any changes in personnel; the validity of such changes does not require the signing of an amendment to this Agreement. The Supplier is obliged to bind individuals participating in the fulfilment of this Agreement to confidentiality under § 12 of the Cybersecurity Act.

11. The Supplier undertakes not to assign its monetary claims arising from this Agreement to third parties without the written consent of the Customer. The assignment of the Supplier's claim to a third party without the Customer's consent is invalid. The Customer's consent is valid only if the prior consent of the Ministry of Health of the Slovak Republic (MZ SR) has been obtained. In case of breach of this obligation, the Supplier is obliged to pay the Customer a contractual penalty in the amount of 2% of the principal claim. This provision does not apply if a special legal regulation relating to the claim arising from this Agreement excludes the possibility of conditioning the assignment of the claim on the consent of the Customer as the debtor.

12. The Parties agree that the Supplier will not accept a declaration under § 303 et seq. of the Commercial Code. In case of a breach of this obligation, the Supplier is obliged to pay the Customer a contractual penalty in the amount of 2% of the principal claim. This provision does not apply if a special legal regulation excludes the conclusion of an agreement according to the preceding sentence.

Article 4

Management of Cybersecurity Incidents

1. Dodávateľ sa zaväzuje postupovať tak, aby pri jeho činnosti nedošlo k vzniku kybernetického bezpečnostného incidentu (ďalej len „incident").
2. Dodávateľ je povinný bezodkladne, najneskôr do 24 hodín nahlásiť Odberateľovi každý incident, o ktorom sa dozvie, a to spôsobom určeným touto zmluvou. Dodávateľ následne určí závažnosť incidentu.
3. Ak v čase hlásenia incidentu stále trvajú prejavy incidentu, Dodávateľ odošle Odberateľovi neúplné hlásenie aj s odkazom, že ide o neúplné hlásenie. Dodávateľ neúplné hlásenie bez zbytočného odkladu doplní po obnove riadnej a úplnej prevádzky siete a všetkých informačných systémov Odberateľa.
4. Najčastejšími spôsobmi riešenia incidentov, ktoré Dodávateľ využíva, sú:
    a. odozva,
    b. označenie incidentov a ich účinkov,
    c. náprava nepriaznivých dopadov incidentov,
    d. iné vhodné činnosti spojené s nápravou incidentov (ďalej len „Reakčné opatrenia"), a to ako na výzvu Odberateľa, tak aj bez jeho výzvy, ak sa o incidente dozvie.
5. Dodávateľ pri reakciách na incidenty spolupracuje s Odberateľom, NBÚ a inými príslušnými orgánmi a za týmto účelom poskytuje súčinnosť a zdieľa všetky získané informácie, ktoré nie sú dôvernými informáciami, a ktoré by mohli mať vplyv na implementáciu Reakčných opatrení v budúcnosti.
6. Dodávateľ sa zaväzuje v čase incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní a poskytnúť ho Odberateľovi. Dodávateľ sa zaväzuje oznámiť Odberateľovi skutočnosti, že v súvislosti s incidentom mohlo dôjsť k spáchaniu trestného činu.
7. Dodávateľ bez zbytočného odkladu oznámi Odberateľovi implementáciu Reakčných opatrení. Ak o to Odberateľ požiada, po úspešnej implementácii Reakčného opatrenia Dodávateľ predloží návrh bezpečnostných opatrení a postupov, ktoré zabezpečia, že nedôjde k opakovaniu, pokračovaniu či šíreniu incidentu (ďalej len „Ochranné opatrenie"). Ak Dodávateľ Ochranné opatrenie nenavrhne alebo ak Ochranné opatrenie neprinesie požadovaný efekt, Dodávateľ vypracuje a predloží iné Ochranné opatrenie. S povolením Odberateľa Dodávateľ implementuje Ochranné opatrenie, preverí jeho účinnosť a spíše záznam o efektívnosti jeho implementácie.

Článok 5
Zodpovednosť Dodávateľa

1. The Supplier undertakes to act in such a way that its activities do not lead to the occurrence of a cybersecurity incident (hereinafter referred to as "incident").
2. The Supplier is obligated to immediately, no later than within 24 hours, report to the Customer each incident it becomes aware of, in a manner specified by this agreement. The Supplier will then determine the severity of the incident.
3. If manifestations of the incident persist at the time of reporting, the Supplier will send an incomplete report to the Customer, with a reference that it is an incomplete report. The Supplier will promptly complete the incomplete report after the restoration of normal and complete operation of the network and all information systems of the Customer.
4. The most common ways the Supplier uses to resolve incidents are:
    a. Response,
    b. Identification of incidents and their effects,
    c. Remediation of adverse impacts of incidents,
    d. Other appropriate activities related to incident remediation (hereinafter referred to as "Response Measures"), both at the Customer's request and without it if the Supplier becomes aware of the incident.
5. The Supplier collaborates with the Customer, NSA (National Security Authority), and other relevant authorities in responding to incidents, providing cooperation, and sharing all non-confidential information that may impact the implementation of Response Measures in the future.
6. The Supplier undertakes, during an incident, to secure evidence or a means of evidence that can be used in criminal proceedings and provide it to the Customer. The Supplier commits to notify the Customer of the fact that a criminal offense may have been committed in connection with the incident.
7. The Supplier will promptly inform the Customer of the implementation of Response Measures. Upon the Customer's request, after the successful implementation of Response Measures, the Supplier will submit a proposal for security measures and procedures to ensure that the incident is not repeated, continued, or spread (hereinafter referred to as "Protective Measure"). If the Supplier does not propose a Protective Measure or if the Protective Measure does not achieve the desired effect, the Supplier will develop and submit another Protective Measure. With the Customer's permission, the Supplier will implement the Protective Measure, verify its effectiveness, and record the effectiveness of its implementation.

Article 5
Supplier's Responsibility

1. Dodávateľ berie na vedomie, že neplnenie jeho povinností podľa tejto Zmluvy môže spôsobiť Odberateľovi škody, pričom v prípade škôd ako dôsledkov incidentov, ktoré by sa pri riadnom a včasnom plnení povinností Dodávateľa podľa tejto zmluvy neprejavili alebo by sa prejavili v menšej intenzite, zodpovedá Odberateľovi v plnom rozsahu (zodpovednosť za výsledok).
2. Ak Odberateľ v súvislosti s preukázateľným porušením povinností Dodávateľa podľa tejto Zmluvy dostane pokutu, zaväzuje sa Dodávateľ nahradiť vzniknutú škodu v celom rozsahu, či poskytnúť primerané (peňažné) zadosťučinenie. Dodávateľ sa zároveň zaväzuje v súlade s § 725 zákona č. 513/1991 Zb. Obchodný zákonník, odškodniť Odberateľa v plnej výške udelenej pokuty, uloženej náhrady škody či primeraného (peňažného) zadosťučinenia.

Článok 6
Audit kybernetickej bezpečnosti

1. Odberateľ je oprávnený vykonať u Dodávateľa audit kybernetickej bezpečnosti (ďalej len „audit") zameraný na overenie plnenia povinností Dodávateľa podľa tejto Zmluvy a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia Dodávateľa na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti u Dodávateľa pre plnenie cieľov tejto Zmluvy. Výdavky Odberateľa spojené s vykonaním auditu znáša Odberateľ.
2. Odberateľ môže audit u Dodávateľa vykonať sám alebo prostredníctvom poverenej tretej osoby; v takom prípade práva a povinnosti Odberateľa pri výkone auditu realizuje Odberateľom poverená tretia osoba, ktorá je povinná zachovávať povinnosť mlčanlivosti o všetkých skutočnostiach zistených pri audite vo vzťahu k tretím osobám.
3. Dodávateľ sa zaväzuje, že Odberateľovi umožní kedykoľvek vykonať audit, ktorým si Odberateľ overí mieru a efektívnosť plnenia povinností Dodávateľom uvedených v bode 1 tohto článku, pričom tento audit bude zameraný najmä na kontrolu technického, technologického a personálneho vybavenia a procesných postupov, ktoré Dodávateľ využíva pri plnení svojich povinností v oblasti kybernetickej bezpečnosti a tiež bude zameraný na overenie nastavenia a efektívnosti procesov a technológií v organizačnej a technickej oblasti Dodávateľa.
4. Akékoľvek nedostatky alebo pochybenia zistené auditom je Dodávateľ povinný odstrániť bezodkladne, avšak najneskôr do 60 (slovom:

1. The Supplier acknowledges that the non-fulfillment of its obligations under this Agreement may cause damages to the Customer. In the case of damages resulting from incidents that would not have manifested or would have manifested with less intensity under the proper and timely fulfillment of the Supplier's obligations under this agreement, the Supplier is fully responsible to the Customer (liability for results).
2. If the Customer incurs a fine in connection with a demonstrable breach of the Supplier's obligations under this Agreement, the Supplier undertakes to compensate for the incurred damage in full or provide appropriate (monetary) satisfaction. The Supplier also commits, in accordance with § 725 of Act No. 513/1991 Coll., Commercial Code, to indemnify the Customer in full for the imposed fine, compensation for damages, or appropriate (monetary) satisfaction.

Article 6
Cybersecurity Audit

1. The Customer is entitled to conduct a cybersecurity audit (hereinafter referred to as "audit") at the Supplier's premises aimed at verifying the Supplier's compliance with the obligations under this Agreement and the effectiveness of their fulfilment. The audit will particularly focus on verifying the technical, technological, and personnel equipment of the Supplier for performing tasks in the field of cybersecurity, as well as the setup of processes, roles, and technologies in the organizational, personnel, and technical areas of the Supplier for achieving the goals of this Agreement. The Customer bears the expenses associated with conducting the audit.
2. The Customer may conduct the audit at the Supplier's premises either by itself or through an authorized third party. In such a case, the rights, and obligations of the Customer in conducting the audit are carried out by the third party authorized by the Customer, which is obliged to maintain confidentiality about all facts discovered during the audit in relation to third parties.
3. The Supplier undertakes to allow the Customer to conduct an audit at any time to verify the extent and effectiveness of the Supplier's fulfillment of the obligations mentioned in point 1 of this article. This audit will primarily focus on checking the technical, technological, and personnel equipment and procedural processes that the Supplier uses in fulfilling its obligations in the field of cybersecurity. It will also aim to verify the setup and effectiveness of processes and technologies in the organizational and technical areas of the Supplier.
4. Any deficiencies or errors identified during the audit must be promptly rectified by the Supplier, but no later than within 60 (sixty) days from the date of the audit days based on the severity of the deficiency or error.

šesťdesiatich) kalendárnych dní, ak to na základe závažnosti nedostatku alebo pochybenia je možné.

5. Dodávateľ je povinný pri audite spolupracovať s Odberateľom a v prípade potreby mu umožniť voľný vstup do svojich priestorov, zabezpečiť mu dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto Zmluvy na nahliadnutie. Audit sa vykonáva výlučne prostredníctvom, alebo za prítomnosti poverenej osoby alebo osôb Dodávateľa.
6. Odberateľ je povinný oznámiť Dodávateľovi najmenej 10 (slovom: desať) pracovných dní vopred, že chce u Dodávateľa vykonať audit. Vykonanie alebo nevykonanie auditu Odberateľom nezbavuje Dodávateľa zodpovednosti za plnenie povinností Dodávateľa vyplývajúcich z tejto Zmluvy. Ak Dodávateľ neumožní vykonanie auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto Zmluvy. Termín auditu musí byť odobrený oboma Zmluvnými stranami, tak aby nezasahoval do bežného chodu ani jeden zo Zmluvných strán.
7. Odberateľ je povinný zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe. Odberateľ a jeho zamestnanci pri návšteve priestorov Dodávateľa v rámci výkonu auditu musia dodržiavať pokyny Dodávateľa týkajúce sa uvedených priestorov na úseku bezpečnosti a ochrany zdravia pri práci (ďalej len „BOZP") a ochrany pred požiarmi na účely predchádzania vzniku požiarov a zabezpečenia podmienok na účinné zdolávanie požiarov (ďalej len „PO"), s ktorými boli oboznámení podľa štvrtej vety tohto odseku, pričom zodpovednosť za to, že tieto osoby budú dodržiavať uvedené pokyny, nesie Odberateľ. Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov Dodávateľa na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne Dodávateľ. Dodávateľ je povinný preukázateľne informovať zamestnancov Odberateľa o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch Dodávateľa môžu vyskytnúť, a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal Dodávateľ na zaistenie BOZP a PO, o opatreniach a postupe v prípade poškodenia zdravia vrátane poskytnutia prvej pomoci, ako aj o opatreniach a postupe v prípade zdolávania požiaru, záchranných prác a evakuácie, a preukázateľne ich poučiť o pokynoch na zaistenie BOZP a PO platných pre priestory Dodávateľa.

Článok 7

Dôvernosť informácií a mlčanlivosť

5. The Supplier is obligated to cooperate with the Customer during the audit and, if necessary, allow free access to its premises, provide documentation, and allow inspection of technical and technological equipment related to the fulfilment of tasks in the field of cybersecurity under this Agreement. The audit is carried out exclusively through or in the presence of the authorized person or persons of the Supplier.
6. The Customer is obliged to notify the Supplier at least 10 (ten) working days in advance that it intends to conduct an audit at the Supplier's premises. The performance or non-performance of the audit by the Customer does not exempt the Supplier from the responsibility for fulfilling the obligations arising from this Agreement. If the Supplier does not allow the audit, it is considered that it is not fulfilling the tasks in the field of cybersecurity under this Agreement. The audit date must be mutually approved by both Contracting Parties to avoid disrupting the normal operation of either of the Contracting Parties.
7. The Customer is obliged to maintain confidentiality about the circumstances learned during the audit that are not publicly known. The Customer and its employees, during visits to the Supplier's premises as part of the audit, must adhere to the Supplier's instructions regarding security and occupational safety and health (hereinafter referred to as "OSH") and fire protection to prevent the occurrence of fires and ensure conditions for effective fire extinguishing (hereinafter referred to as "FP"). The responsibility for ensuring that these individuals comply with the instructions lies with the Customer. The Supplier is fully and exclusively responsible for creating conditions to ensure OSH and FP, as well as securing and equipping the premises for the safe conduct of the audit. The Supplier is obligated to inform the Customer's employees about the dangers and risks that may arise during the audit in the Supplier's premises and about the results of the risk assessment, preventive measures, and protective measures taken by the Supplier to ensure OSH and FP. The Supplier must also provide information on measures and procedures in case of health damage, including first aid, as well as measures and procedures in case of firefighting, rescue work, and evacuation, and demonstrably instruct them on OSH and FP instructions applicable to the Supplier's premises.

Article 7

Confidentiality of Information and Non-Disclosure

1. Zmluvné strany, nimi poverené osoby, subdodávatelia, ako aj zamestnanci oboch Zmluvných strán sú povinní zachovávať v tajnosti všetky dôverné informácie, ktoré sú uvedené v tejto Zmluve alebo ktoré budú uvedené v jej dodatkoch a prílohách alebo ktoré im boli poskytnuté, alebo ktoré inak získali v súvislosti so Zmluvou alebo s ktorými sa oboznámili počas plnenia Zmluvy, resp. ktoré súvisia s predmetom plnenia, s údajmi, ktoré podliehajú ochrane, s údajmi o klientoch a obchodných partneroch Zmluvných strán, údajmi z informačných systémov ktorejkoľvek Zmluvnej strany a predzmluvnými rokovaniami s ňou súvisiacimi, s výnimkou nasledujúcich prípadov:
    a. ak je poskytnutie informácie od dotknutej Zmluvnej strany uložené na základe všeobecne záväzných právnych predpisov alebo na základe povinnosti uloženej postupom podľa všeobecne záväzných právnych predpisov (napr. zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov),
    b. ak je informácia verejne dostupná z iného dôvodu, ako je porušenie povinnosti mlčanlivosti dotknutou Zmluvnou stranou, informácie, ktoré už sú v deň podpisu Zmluvy verejne známe alebo ktoré je možné už v deň podpisu tejto Zmluvy získať z bežne dostupných informačných prostriedkov,
    c. informácie, ktoré sa stanú po podpise Zmluvy verejne známymi alebo ktoré možno po tomto dni získať z bežne dostupných informačných prostriedkov,
    d. ak je informácia poskytnutá odborným poradcom dotknutej Zmluvnej strany (vrátane právnych, účtovných, daňových a iných poradcov), ktorí sú buď viazaní všeobecnou profesionálnou povinnosťou mlčanlivosti alebo ak sa voči dotknutej Zmluvnej strane zaviazali povinnosťou mlčanlivosti,
    e. pre účely akéhokoľvek súdneho, rozhodcovského, správneho alebo iného konania, ktorého je dotknutá Zmluvná strana účastníkom,
    f. ak je informácia poskytnutá so súhlasom druhej Zmluvnej strany.

2. Zmluvné strany sú povinné zachovať mlčanlivosť o všetkých dôverných informáciách, ibaže by z tejto Zmluvy alebo z príslušných všeobecne záväzných právnych predpisov vyplývalo inak. Tento záväzok

1. Contracting parties, their authorized representatives, subcontractors, as well as employees of both contracting parties, are obliged to maintain confidentiality regarding all confidential information specified in this Agreement or in its appendices and amendments, or that has been provided to them or otherwise acquired in connection with the Agreement, or that is related to the subject matter of the performance, including data subject to protection, information about clients and business partners of the contracting parties, data from information systems of any contracting party, and pre-contractual negotiations with it, with the exception of the following cases:
    a. If the provision of information by the affected contracting party is mandated by generally binding legal regulations or by an obligation imposed through a procedure pursuant to generally binding legal regulations (e.g., Act No. 211/2000 Coll. on Free Access to Information and on Amendments to Some Acts, as amended),
    b. If the information is publicly available for reasons other than a breach of the obligation of confidentiality by the affected contracting party; information that is already publicly known on the day of signing this Agreement or that can be obtained on the day of signing this Agreement from generally accessible information sources,
    c. Information that becomes publicly known after the signing of the Agreement or that can be obtained from generally accessible information sources after that date,
    d. If the information is provided by professional advisors of the affected contracting party (including legal, accounting, tax, and other advisors) who are either bound by a general professional obligation of confidentiality or who have committed to confidentiality towards the affected contracting party,
    e. For the purposes of any judicial, arbitration, administrative, or other proceedings in which the affected contracting party is a participant,
    f. If the information is provided with the consent of the other contracting party.

2. Contracting parties are obliged to maintain confidentiality regarding all confidential information unless otherwise stipulated by this Agreement or the relevant applicable legal regulations. This commitment

trvá aj po ukončení platnosti a účinnosti tejto Zmluvy.

3. Zmluvné strany sa zaväzujú, že dôverné informácie bez predchádzajúceho písomného súhlasu druhej Zmluvnej strany nepoužijú pre seba alebo pre tretie osoby, neposkytnú tretím osobám a ani neumožnia prístup tretích osôb k dôverným informáciám. Za tretie osoby sa nepokladajú členovia orgánov Zmluvných strán, audítori alebo právni poradcovia Zmluvných strán, ktorí sú ohľadne im sprístupnených informácií viazaní povinnosťou mlčanlivosti na základe všeobecne záväzných právnych predpisov.
4. Zmluvné strany sa zaväzujú, že všetky zúčastnené osoby a subjekty budú s takto poskytnutými informáciami a zistenými skutočnosťami nakladať ako s dôvernými informáciami.
5. Zmluvné strany sa zaväzujú, že upovedomia druhú Zmluvnú stranu o porušení povinnosti mlčanlivosti bez zbytočného odkladu po tom, ako sa o takomto porušení dozvedeli a zároveň sa zaväzujú vyvinúť maximálne úsilie na to, aby sa odstránili následky takéhoto porušenia, a aby sa zabránilo ďalšiemu porušeniu povinnosti mlčanlivosti a tiež aby sa zabezpečili a obnovili všetky opatrenia potrebné na ochranu dôverných informácií.
6. Zmluvné strany sa zaväzujú, že budú ochraňovať dôverné informácie druhej Zmluvnej strany s rovnakou starostlivosťou ako ochraňujú vlastné dôverné informácie rovnakého druhu, vždy však najmenej v rozsahu primeranej odbornej starostlivosti a zachovávania ochrany a dôvernosti údajov v súlade s právnym poriadkom SR.
7. Zmluvné strany sa zaväzujú zachovávať mlčanlivosť o podmienkach spolupráce podľa tejto Zmluvy, ako aj o všetkých skutočnostiach týkajúcich sa druhej Zmluvnej strany (najmä, nie však výlučne obchodnej povahy), ktoré im boli sprístupnené počas trvania tejto Zmluvy alebo ktoré sa im stali iným spôsobom známe. Uvedené sa týka najmä skutočností týkajúcich sa kybernetickej bezpečnosti a osobných údajov zamestnancov. Povinnosť mlčanlivosti trvá aj po skončení tejto Zmluvy alebo Osobitnej zmluvy bez časového obmedzenia.
8. Výnimky z povinností podľa tohto článku tejto Zmluvy upravujú najmä Zákon o kybernetickej bezpečnosti a iné príslušné právny predpisy.

Článok 8

Oznámenia a kontaktné osoby

1. Dodávateľ je povinný komunikovať pri plnení povinností podľa tejto zmluvy s Odberateľom, ako aj oznamovať všetky informácie, ktoré môžu mať vplyv na túto Zmluvu alebo súvisia s touto Zmluvou, e-mailom na kontaktné údaje Zmluvných strán

persists even after the termination of the validity and effectiveness of this Agreement.

3. The contracting parties undertake not to use confidential information for themselves or third parties, disclose it to third parties, or allow third parties access to confidential information without the prior written consent of the other contracting party. Members of the bodies of the contracting parties, auditors, or legal advisors of the contracting parties, who are bound by confidentiality obligations based on generally binding legal regulations regarding the information made available to them, are not considered third parties.
4. The contracting parties commit that all involved individuals and entities will treat such provided information and identified facts as confidential.
5. The contracting parties undertake to notify the other contracting party of any breach of the confidentiality obligation without undue delay after becoming aware of such a breach. They also commit to making maximum efforts to remedy the consequences of such a breach, prevent further breaches of confidentiality, and ensure the protection and restoration of all measures necessary to safeguard confidential information.
6. The contracting parties commit to protecting the confidential information of the other contracting party with the same care as they protect their own confidential information of a similar nature, always at least to the extent of reasonable professional care and compliance with data protection laws in the Slovak Republic.
7. The contracting parties undertake to maintain confidentiality about the terms of cooperation under this Agreement, as well as all facts related to the other contracting party (especially, but not exclusively, of a commercial nature) that were made available to them during the term of this Agreement or became known to them in any other way. This applies particularly to facts related to cybersecurity and personal data of employees. The obligation of confidentiality persists after the termination of this Agreement or the Specific Agreement without time limitations.
8. Exceptions to the obligations under this article of this Agreement are regulated, especially by the Cybersecurity Act and other relevant legal regulations.

Article 8

Notifications and Contact Persons

1. The Supplier is obligated to communicate during the fulfilment of obligations under this agreement with the Customer and to notify of all information that may impact this Agreement or is related to this Agreement, either by email to the contact details of the Contracting Parties

uvedené v tejto Zmluve alebo doporučenou poštou alebo prostredníctvom kuriéra na adresy uvedené v záhlaví tejto Zmluvy, pričom vo všetkých prípadoch musí byť prenos informácií uskutočnený za podmienok umožňujúcich chránený prenos informácií.

2. Odberateľ určuje nasledovnú kontaktnú osobu pre komunikáciu s Dodávateľom na úseku kybernetickej bezpečnosti:

   meno: Pavol VRABEC, MBA, CISM

   Telefonický kontakt: 00421 907 852 280

   Adresa elektronickej pošty: pavol.vrabec@unm.sk, mkb@unm.sk

3. Dodávateľ určuje nasledovnú kontaktnú osobu pre komunikáciu alebo sprostredkovanie potrebných informácií na úseku kybernetickej bezpečnosti.
   Meno: Alexandre Attia .....

4. Kontaktná osoba Dodávateľa plní úlohy pri zabezpečovaní reaktivity podľa čl. 4 tejto Zmluvy. Kontaktná osoba plní notifikačné povinnosti prostredníctvom na to povereného organizačného útvaru Dodávateľa.
5. Kontaktné osoby podľa odsekov 2 a 3 tohto článku môže príslušná zmluvná strana zmeniť, ak oznámi novú kontaktnú osobu druhej zmluvnej strane v písomnej forme spôsobom podľa ods. 6 článku 9 tejto Zmluvy. V prípade, ak kontaktné osoby majú prístup k informáciám a údajom Odberateľa sú povinné zachovávať mlčanlivosť podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti.

Článok 9

Doba trvania a zánik Zmluvy

1. Táto zmluva sa uzatvára na dobu určitú, a to do ukončenia Osobitnej zmluvy .
2. Pred uplynutím dohodnutej doby trvania môžu Zmluvné strany zmluvný vzťah ukončiť:
   a. písomnou dohodou Zmluvných strán,
   b. odstúpením Odberateľa od Zmluvy pri porušení zmluvných povinností Dodávateľom podľa ods. 4 tohto článku,
   c. odstúpením Dodávateľa od Zmluvy pri porušení zmluvných povinností Odberateľom podľa ods. 5 tohto článku,
   d. písomnou výpoveďou Odberateľa, aj bez uvedenia dôvodu, pričom výpovedná lehota je jeden mesiac a začína plynúť prvým dňom mesiaca nasledujúceho po mesiaci, v ktorom bola výpoveď Dodávateľovi doručená.

specified in this Agreement or by registered mail or through a courier to the addresses specified in the heading of this Agreement, with the condition that, in all cases, the transfer of information must be conducted under conditions allowing for secure information transmission.

2. The Customer designates the following contact person for communication with the Supplier in the field of cybersecurity:

   Name: Pavol VRABEC, MBA, CISM

   Phone contact: 00421 907 852 280

   Email address: pavol.vrabec@unm.sk, mkb@unm.sk

3. The Supplier designates the following contact person for communication or provision of necessary information in the field of cybersecurity:
   Name: Alexandre Attia .....

4. The Supplier's contact person performs tasks related to ensuring reactivity according to Article 4 of this Agreement. The contact person fulfills notification obligations through the organizational unit authorized for this purpose within the Supplier's organization.
5. The relevant contracting party may change the contact persons according to paragraphs 2 and 3 of this articles by notifying the other contracting party of the new contact person in writing, in accordance with paragraph 6 of Article 9 of this Agreement. If contact persons have access to information and data of the Customer, they are obliged to maintain confidentiality in accordance with § 12 para. 1 of the Cybersecurity Act.

Article 9

Duration and Termination of the Agreement

1. This agreement is concluded for a fixed term until the termination of the Separate Agreement.
2. Prior to the expiration of the agreed term, the Contracting Parties may terminate the contractual relationship:
   a. by written agreement of the Contracting Parties,
   b. by the Customer's withdrawal from the Agreement in the event of a breach of contractual obligations by the Supplier according to paragraph 4 of this article,
   c. c. by the Supplier's withdrawal from the Agreement in the event of a breach of contractual obligations by the Customer according to paragraph 5 of this article,
   d. d. by the written notice of the Customer, even without specifying a reason, with a notice period of one month, commencing on the first day of the month following the month in which the notice was delivered to the Supplier.

3. Ukončenie tejto Zmluvy sa netýka tých ustanovení, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie majú trvať aj po ukončení tejto Zmluvy, ďalej záväzkov na náhradu škody spôsobenej porušením povinností podľa tejto Zmluvy.
4. Odberateľ je oprávnený odstúpiť od tejto Zmluvy v prípade:
    a. porušenia aplikovateľných právnych predpisov ohľadom kybernetickej bezpečnosti,
    b. porušenia zmluvných ustanovení o kybernetickej bezpečnosti v Zmluve alebo v Osobitnej zmluve,
    c. ak Dodávateľ opakovane koná v rozpore s touto Zmluvou alebo všeobecne záväznými právnymi predpismi a na výzvu Odberateľa toto konanie a jeho následky v primeranej lehote určenej Odberateľom neodstránil,
    d. ak Dodávateľ pri svojej činnosti nedodržiava bezpečnostnú politiku informačných systémov Odberateľa,
    e. ak Dodávateľ poruší záväzok mlčanlivosti a/alebo ochrany informácií vyplývajúcu z tejto Zmluvy,
    f. ak Dodávateľ bezodkladne nenahlási Odberateľovi incident, o ktorom sa dozvie alebo ho nahlási v rozpore s touto Zmluvou,
    g. ak Dodávateľ neumožní Odberateľovi vykonať audit aj napriek predošlému oznámeniu o vykonaní auditu v lehote podľa tejto Zmluvy alebo nespolupracuje s Odberateľom pri vykonávaní auditu,
    h. ak Dodávateľ neodstránil nedostatky alebo pochybenia zistené auditom v lehote určenej podľa tejto Zmluvy,
    i. ak Dodávateľ neposkytne potrebnú súčinnosť v zmysle tejto Zmluvy,
    j. ak je na Dodávateľa vyhlásený konkurz alebo bola povolená reštrukturalizácia alebo ak bol návrh na vyhlásenie konkurzu odmietnutý alebo konkurz zrušený pre nedostatok majetku,
    k. ak je Dodávateľ v likvidácii.
5. Dodávateľ je oprávnený odstúpiť od tejto Zmluvy, ak:
    a. Odberateľ opakovane koná v rozpore s touto Zmluvou alebo všeobecne záväznými právnymi predpismi,

3. The termination of this Agreement does not affect provisions that, due to their nature or explicit wording, are intended to survive the termination of this Agreement, including obligations to compensate for damages caused by a breach of obligations under this Agreement.
4. The Customer is entitled to terminate this Agreement in the following cases:
    a. Violation of applicable legal regulations regarding cybersecurity.
    b. Breach of contractual provisions on cybersecurity in the Agreement or in the Separate Agreement.
    c. If the Supplier repeatedly acts in contradiction to this Agreement or generally binding legal regulations, and, upon the Customer's request, fails to rectify such actions and their consequences within a reasonable period determined by the Customer.
    d. If the Supplier, in its activities, fails to comply with the information systems security policy of the Customer.
    e. If the Supplier violates the obligation of confidentiality and/or information protection arising from this Agreement.
    f. If the Supplier fails to promptly report an incident to the Customer, which it learns about or reports in violation of this Agreement.
    g. If the Supplier does not allow the Customer to conduct an audit, despite prior notice of the audit within the period specified in this Agreement or does not cooperate with the Customer in conducting the audit.
    h. If the Supplier does not rectify deficiencies or errors identified during the audit within the period specified in this Agreement.
    i. If the Supplier does not provide the necessary cooperation as per this Agreement.
    j. If bankruptcy proceedings are initiated against the Supplier or if restructuring has been approved, or if a petition for bankruptcy has been rejected or bankruptcy has been cancelled due to lack of assets.
    k. If the Supplier is in liquidation.
5. The Supplier is entitled to terminate this Agreement if:
    a. The Customer repeatedly acts in contradiction to this Agreement or generally binding legal regulations,

b. Odberateľ neoznámi Dodávateľovi najmenej 10 (slovom: desať) pracovných dní vopred, že chce u Dodávateľa vykonať audit,

c. Odberateľ poruší svoju povinnosť zachovávať mlčanlivosť vyplývajúcu z tejto Zmluvy.

6. Odstúpenie od Zmluvy musí byť oznámené písomne, pričom musí byť uvedený dôvod, pre ktorý Zmluvná strana od Zmluvy odstupuje. Odstúpenie od Zmluvy sa považuje za doručené v deň, kedy druhá Zmluvná strana prevzala zásielku obsahujúcu odstúpenie a v prípade, že toto odstúpenie odmietla prevziať alebo jej nebolo doručené z iného dôvodu, považuje sa odstúpenie za doručené v deň, kedy sa zásielka vrátila odosielajúcej Zmluvnej strane za podmienky, že bola odoslaná na adresu druhej Zmluvnej strany uvedenú v Zmluve alebo v príslušnom verejnom registri (t.j. v príslušnom obchodnom alebo živnostenskom registri). Uvedené ustanovenie o doručení odstúpenia sa rovnako vzťahuje na doručovanie akýchkoľvek oznámení, výziev, upomienok, výpovedí a iných písomných prejavov vôle medzi zmluvnými stranami.

Článok 10
Záverečné ustanovenia

1. Táto Zmluva nadobúda platnosť dňom jej podpísania oprávnenými zástupcami oboch zmluvných strán a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv Úradu vlády SR.
2. Túto Zmluvu je možné meniť len písomnými dodatkami odsúhlasenými a podpísanými obidvomi Zmluvnými stranami.
3. Zmluvné strany sa zaväzujú, že všetky spory, ktoré vzniknú z tejto Zmluvy alebo v súvislosti s ňou budú riešené zmierom. Ak nedôjde k vyriešeniu sporu zmierom, spor rozhodne vecne a miestne príslušný súd určený podľa procesných právnych predpisov Slovenskej republiky. Zmluvné strany sa dohodli, že v prípade potreby je rozhodným právom právo Slovenskej republiky.
4. Pokiaľ niektoré z ustanovení tejto Zmluvy je neplatné alebo neúčinné alebo nevynútiteľné, nemá to vplyv na platnosť, účinnosť alebo vynútiteľnosť jej ostatných ustanovení. V prípade, že niektoré z ustanovení tejto zmluvy je neplatné, alebo sa stane neskôr neplatným alebo neúčinným, zaväzujú sa Zmluvné strany, že ho nahradia ustanovením, ktoré najviac zodpovedá ich pôvodnej vôli.
5. Zmluva je vyhotovená v dvoch rovnopisoch, pre každú Zmluvnú stranu po jednom rovnopise.

b. The Customer fails to notify the Supplier at least 10 (in words: ten) business days in advance that they intend to conduct an audit at the Supplier's premises.

c. c. The Customer breaches their obligation to maintain confidentiality arising from this Agreement.

6. Termination of the Agreement must be communicated in writing, stating the reason for the termination. Termination of the Agreement is considered delivered on the day when the other Party received the shipment containing the termination. In the event of refusal to accept the termination or if it was not delivered for any other reason, the termination is considered delivered on the day the shipment is returned to the sending Party, provided it was sent to the address of the other Party as specified in the Agreement or in the relevant public register (i.e., in the respective commercial or trade register). This provision on the delivery of termination equally applies to the delivery of any notices, demands, reminders, terminations, and other written expressions of will between the contracting parties.

Article 10
Final Provisions

1. This Agreement becomes effective on the day of its signing by authorized representatives of both contracting parties and is enforceable from the day following its publication in the Central Registry of Contracts of the Government Office of the Slovak Republic.
2. This Agreement may only be amended by written amendments agreed upon and signed by both contracting parties.
3. The contracting parties undertake that all disputes arising from this Agreement or in connection with it will be resolved amicably. If a dispute is not resolved amicably, it shall be decided by a competent court determined in terms of subject matter and locality according to the procedural legal regulations of the Slovak Republic. The contracting parties have agreed that, if necessary, the governing law is the law of the Slovak Republic.
4. If any provision of this Agreement is invalid, ineffective, or unenforceable, it does not affect the validity, effectiveness, or enforceability of its other provisions. In case any provision of this Agreement is invalid or becomes invalid or ineffective later, the contracting parties undertake to replace it with a provision that most closely corresponds to their original intent.
5. The Agreement is drawn up in two identical copies, one for each contracting party.

6. Zmluvné strany vyhlasujú, že sú plne spôsobilé na právne úkony, že ich zmluvná voľnosť nie je ničím obmedzená, že túto Zmluvu neuzavreli ani v tiesni, ani za nápadne nevýhodných podmienok, že si obsah Zmluvy dôkladne prečítali a že tento im je jasný, zrozumiteľný a vyjadrujúci ich slobodnú, vážnu a spoločnú vôľu, a na znak súhlasu ju podpisujú.

Príloha č. 1: Zoznam pracovných rolí Dodávateľa a zoznam zamestnancov Dodávateľa

V Martine dňa 21. FEB. 2024

eľ

...temocnica Martin
Kollárova 2, 036 59 Martin

Paris 12/02/2024
V ..... dňa .....

Julien VIDAL, CEO, AZMED

6. The contracting parties declare that they are fully capable of legal acts, that their contractual freedom is not restricted by anything, that they have not entered into this Agreement under duress or under conspicuously disadvantageous conditions, that they have thoroughly read the content of the Agreement, that it is clear, understandable, and expresses their free, serious, and joint will, and they sign it as a sign of consent.

Attachment No. 1: List of Supplier's job roles and list of Supplier's employees

In Martin, date 21. FEB. 2024

...nocnica Martin
...36 59 Martin

Julien VIDAL, CEO, AZMED

Príloha č. 1: Zoznam pracovných rolí Dodávateľa

Attachment No. 1:
List of Supplier's job roles and list of Supplier's employees

Meno/Name	Pracovná Rola/Job role	Email	Kontakt/Contact phone
Alexandre Garot	Support engineer		
Pierre Riché	Support engineer		
Oscar Poels	Support engineer		