

ZMLUVA O SPOLUPRÁCI č. 4/2025/111

uzatvorená v súlade so . zákona č. 513/1991 Z.z. Obchodný zákonník v znení neskorších predpisov a
v súlade s ust. §65 a nasl. zákona č. 185/2015 Z.z. Autorský zákon v znení neskorších predpisov
(Ďalej len : „ Zmluva“)

1. Zmluvná strana

Obchodné meno:	Pôdohospodárska platobná agentúra
Sídlo:	Hraničná 12, 815 26 Bratislava, Slovenská republika
IČO:	30 794 323
Bankové spojenie:	Štátna pokladnica Bratislava
IBAN:	
Štatutárny zástupca:	Ing. Marek Čepko, generálny riaditeľ
Rozpočtová organizácia:	zriadená zákonom č. 473/2003 Z. z. v znení neskorších predpisov, s pôsobnosťou podľa zákona č. 280/2017 Z. z. a o zmene a doplnení niektorých zákonov

(ďalej len: "Strana 1")

a

2. Zmluvná strana

Obchodné meno:	AXASOFT, a.s.
Sídlo:	Panenská 7, 811 03 Bratislava Slovenská republika
V mene ktorej koná:	Ing. Mgr. Peter Čaniga, predseda predstavenstva
IČO:	35 738 219
IČ DPH:	SK2020269691
Spoločnosť zapísaná:	v obchodnom registri Mestského súdu Bratislava III, vložka č.: 1627/B, Oddiel:
Sa	

(ďalej len: "Strana 2")

(ďalej spoločne označované ako "Zmluvné strany")

Označenie: **4/2025/111**

Článok I

Predmet Zmluvy

1. Predmetom tejto Zmluvy o spolupráci je spolupráca medzi zmluvnými stranami za účelom poskytovania súčinnosti pri kontrole kvality aplikačnej, technickej a prevádzkovej dokumentácie k dielu a zlepšovaní kvality konfiguračných nastavení a podpory prevádzky počítačového programu Agrárny informačný systém (ďalej len „AGIS“) nasadenom na testovacom prostredí.
2. Zmluvné strany sa vzájomne zaväzujú spoločne participovať na zabezpečení kontroly kvality a zlepšovaní aktuálnosti aplikačnej, technickej a prevádzkovej dokumentácie k dielu IS AGIS v rozsahu podľa platnej Vyhlášky 401/2023 Zz vo vzťahu k aktuálne nasadenému dielu IS AGIS na testovacom prostredí.

3. Strany si budú vzájomne poskytovať potrebnú súčinnosť, informácie a podporu pre naplnenie cieľov uvedených v tejto Zmluve.

Článok II

Oblasti spolupráce

1. Zmluvné strany sa dohodli spolupracovať najmä v týchto oblastiach:
 - a) Zabezpečenie kontroly kvality aplikačnej, technickej a prevádzkovej dokumentácie pre IS AGIS („Systém“) ako celku a ako aj pre všetky moduly samostatne voči aktuálne nasadenej verzii informačného systému na testovacom prostredí
 - b) Navrhovanie zlepšovania konfiguračných nastavení a podpory prevádzky počítačového programu Agrárny informačný systém (ďalej len „AGIS“) nasadenom na testovacom prostredí.
 - c) Navrhovanie zlepšení servisných služieb IS AGIS a jeho modulov, komponentov a rozhraní
2. Strany môžu spoločne definovať ďalšie oblasti spolupráce formou písomných dodatkov k tejto Zmluve.

Článok III

Dĺžka trvania a ukončenie

1. Táto Zmluva nadobúda účinnosť dňom jeho podpísania oboma Zmluvnými stranami a zostáva v platnosti do 31.12.2026
2. Ktorákoľvek zo Zmluvných strán môže vypovedať Zmluvu písomným oznámením doručením druhej Zmluvnej strane najmenej 20 pracovných dní pred požadovaným dňom ukončenia.

Článok IV

Cena a platobné podmienky

1. Táto Zmluva sa uzatvára bezodplatne.

Článok V

Osobitné protikorupčné ustanovenia

1. Pri plnení tejto zmluvy sa Strana 2 zaväzuje dodržiavať platné a účinné právne predpisy vzťahujúce sa ku korupcii a korupčnému správaniu.
2. Strana 2 podpisom tejto Zmluvy vyhlasuje, že sa oboznámila s Protikorupčnou politikou Pôdohospodárskej platobnej agentúry, ktorá je zverejnená na webovom sídle Objednávateľa, jej obsahu porozumel a zaväzuje sa ju rešpektovať a dodržiavať.
3. Strana 2 podpisom tejto zmluvy zároveň vyhlasuje, že:
 - a) pozná znaky korupcie a korupčného správania,
 - b) zdrží sa akejkoľvek formy korupcie a korupčného správania v súvislosti s plnením záväzkov vyplývajúcich z tejto Zmluvy,
 - c) poskytne súčinnosť v prípade posudzovania podozrenia z korupcie alebo korupčného správania,

- d) zdrží sa akýchkoľvek foriem korupcie súvisiacich s plnením predmetu Zmluvy alebo záväzkov vyplývajúcich z tejto Zmluvy,
 - e) bezodkladne oznámi Objednávateľovi na emailovú adresu akékoľvek podozrenie z korupcie alebo porušenie ktoréhokoľvek ustanovenia tohto článku Zmluvy a poskytne súčinnosť pri preskúšaní tohto oznámenia,
 - f) nie je v konflikte záujmov vo vzťahu k zamestnancom Strany 1, ktorý by mohol ovplyvniť realizáciu predmetu tejto Zmluvy.
4. V prípade, ak Strana 2 poruší akékoľvek ustanovenie tohto článku Zmluvy alebo jeho časť je Strana 1 oprávnená aj bez predchádzajúceho upozornenia odstúpiť od tejto Zmluvy s okamžitou platnosťou bez toho, aby Strane 2 vznikol akýkoľvek nárok zo zodpovednosti za odstúpenie Strany 1 od Zmluvy, pričom odstúpenie je účinné dňom doručenia oznámenia o odstúpení od zmluvy Strane 2 resp. ak sa takéto oznámenie dostane do dispozičnej sféry Strany 2 a/alebo v jeho mene konajúcej osoby.
-

Článok VI

Pravidlá riadenia informačnej bezpečnosti

1. Strana 2 je povinná:
 - a) rešpektovať operatívne pokyny Strany 1 počas plnenia predmetu tejto Zmluvy,
 - b) dodržiavať bezpečnostné opatrenia uvedené v tejto Zmluve a v príslušnej bezpečnostnej dokumentácii Strany 1,
 - c) poskytnúť potrebnú súčinnosť oprávneným orgánom vykonávajúcim kontrolu/audit, ak súvisí s plnením predmetu tejto Zmluvy,
 - d) poskytnúť potrebnú súčinnosť Strane 1 pre kontrolu/audit svojich IT,
 - e) dodržiavať platné všeobecne záväzné právne predpisy SR, ale najmä zákon č. 452/2021 Z. z. o elektronických komunikáciách v znení neskorších predpisov (ďalej len „zákon č. 452/2021 Z. z.“), zákon o ITVS, zákon č. 69/2018 Z. z., zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 18/2018 Z. z.“) a príslušné vyhlášky k uvedeným zákonom súvisiace s plnením predmetu tejto dohody,
 - f) používať vzdialený prístup do IT Strany 1, len na účel potrebný k plneniu Zmluvy
 - g) predkladať požiadavky v súvislosti so vzdialeným prístupom do IS Strany 1 výhradne prostredníctvom Oprávneného zamestnanca Strany 1.
2. Strana 2 sa zaväzuje, že zabezpečí, aby jeho zamestnanci konajúci v mene Strany 2 pri vzdialenom prístupe do IS Strany 1 dodržiavali všetky podmienky a povinnosti uvedené v tejto Zmluve, všeobecne záväzné právne predpisy SR súvisiace s plnením predmetu tejto Zmluvy vzťahujúce sa k vzdialenému prístupu do IS Strany 1 a súčasne dodržiavali bezpečnostnú dokumentáciu Strany 1.
3. Strana 1 je oprávnená vykonávať u Strany 2 audit vo vzťahu k predmetu tejto Zmluvy.

Bezpečnostné opatrenia pri vzdialenom prístupe do informačných technológií Strany 1

1. Strana 2 je povinný pri vykonávaní činností v IT Strany 1:
 - b) zachovávať mlčanlivosť o všetkých údajoch Strany 1. s ktorými prišiel do styku pri prístupe do IT Strany 1, a to aj po ukončení tejto Zmluvy, pracovného, resp. služobného pomeru,
 - c) rešpektovať operatívne pokyny Strany 1,
 - d) všetky činnosti v IT Strany 1 vykonávať v súlade so všeobecne záväznými právnymi predpismi SR ale najmä zákonom o ITVS, zákonom č. 69/2018 Z. z., zákonom č. 452/2021 Z. z., zákonom č. 18/2018 Z. z. a príslušných vyhlášok k uvedeným zákonom,

- e) prihlasovať sa do IT Strany 1 pod svojim prihlasovacím menom a prihlasovacím heslom na prístup do IT Strany 1, zdieľanie prihlasovacích účtov viacerými používateľmi je zakázané,
- f) zmeniť pri prvom prihlásení do IT Strany 1 prvé heslo na prístup do IT Strany 1, ktoré mu bolo pridelené Stranou 1,
- g) zabezpečiť dôvernosť a ochranu svojho prihlasovacieho mena a prihlasovacieho hesla, pričom zodpovedá za všetky udalosti, zásahy a transakcie, ktoré sa uskutočnili v IT Strane 1 s použitím jeho prihlasovacieho účtu do IT Strany 1,
- h) v prípade podozrenia na prezradenie hesla, resp. v prípade jeho samotného prezradenia, o danej skutočnosti okamžite informovať Oprávneného zamestnanca Strany 1 a nahlásiť udalosť ako BI.
- i) počas vzdialeného prístupu neopustiť pripojený technický prostriedok do IT Strany 1, nedovoliť iným osobám prístup k tomuto technickému prostriedku alebo sledovanie jeho aktívnej obrazovky,
- j) po ukončení vykonávania činností v IT Strane 1 odhlásiť sa z VPN a tak znemožniť prístup k IT Strany 1, ktorý by mohol byť zneužitý k neoprávnenému prístupu do IT Strany 1,
- k) vykonávať činnosti v IT Strany 1 tak, aby pri ňom nedošlo k poškodeniu alebo zničeniu IT Strany 1 alebo k neočakávanému prerušeniu prevádzky IT Strany ,
- l) náležite zdokumentovať všetky zásahy do IS (aký zásah bol vykonaný, kedy bol vykonaný, kto ho vykonal, zdôvodnenie zásahu, popis nového stavu, prípadné obmedzenie pre IS, vzniknuté problémy).

Pri práci s heslom je Strana 2 povinná dodržiavať nasledovné zásady:

1. Heslá pre účty s administrátorskými oprávneniami musia spĺňať minimálne požiadavky:
 - b) Dĺžka hesla minimálne 14 znakov
 - c) Heslá musia obsahovať:
 - i. minimálne jedno veľké písmeno
 - ii. minimálne jedno malé písmeno
 - iii. minimálne jednu číslicu
 - iv. minimálne jeden špeciálny znak
 - d) Zmena hesla
 - i. minimálne raz za 3 mesiace,
 - ii. zmenené heslá musia mať od pôvodného hesla editačnú vzdialenosť minimálne 7, t.j. počet operácií vymazania, vloženia alebo prepísania znaku, ktorými sa z pôvodného hesla dá získať nové,
 - iii. zmenené heslo nesmie byť jedným z posledných 24 hesiel v histórii hesiel pre daný účet,
 - iv. heslo je možné meniť najviac raz za 1 deň
2. Heslá pre účty s privilegovaným prístupom musia spĺňať minimálne požiadavky:
 - a) Dĺžka hesla minimálne 12 znakov (20 znakov pre systémové a technické účty)
 - b) Heslá musia obsahovať:
 - i. minimálne jedno veľké písmeno
 - ii. minimálne jedno malé písmeno
 - iii. minimálne jednu číslicu
 - iv. minimálne jeden špeciálny znak
 - c) Zmena hesla
 - i. minimálne raz za 3 mesiace
 - ii. zmenené heslá musia mať zmenené viac ako polovicu znakov oproti pôvodnému heslu
 - iii. zmenené heslo nesmie byť jedným z posledných 24 hesiel v histórii hesiel pre daný účet
3. Pripájanie technických prostriedkov Zhotoviteľa do IT Strany 1:
 - a) technické prostriedky Strana 2 (najmä osobné počítače, pamäťové nosiče údajov, meracie zariadenia, mobilné telefóny, tablety, sondy a pod.) v súvislosti s vykonávaním Plnenia v IT Strana 1 je možné pripojiť do IT Strana 1 len na základe písomného súhlasu Oprávneného zamestnanca Strany 1,

- b) ak sa do IT Strany 1 bude pripájať technický prostriedok Strany 2, ktorý nie je schválený, je potrebné aby Strana 2 predložila údaje o technickom prostriedku Strane 1 na jeho posúdenie a schválenie,
 - c) technický prostriedok Strany 1 sa pripája k IT Strany 2 len na nevyhnutne potrebný čas, na základe výsledkov antivírusovej kontroly, ktorá potvrdí bezpečnosť technického prostriedku,
 - d) počas doby pripojenia technického prostriedku Strany k IT Strany 1 je prítomný Oprávnený zamestnanec Strany 1.
4. Strana 2 má zakázané:
- a) používať vzdialený prístup do IT Strany 1 na iný účel, ako bol uvedený v žiadosti,
 - b) poskytovať, sprístupňovať alebo zdieľať prístupové údaje do IT Strany 1,
 - c) ukladať prístupové údaje do IT Strany 1 na ľahko dostupné médiá a miesta (papier, diár, nezabezpečený počítačový súbor/program, stôl, monitor a pod.),
 - d) vzdialene sa prihlasovať do IT Strany 1 sa v iných časoch ako na to určených, okrem vopred dohodnutých a schválených konkrétnych prípadov,
 - e) nechávať vzdialene prihlásený technický prostriedok do IT Strany 1 bez dozoru
 - f) ostávať vzdialene prihlásený do IT Strany 1 a počas inej vykonávanej činnosti, ako činnosti súvisiacej s plnením predmetu Zmluvy,
 - g) pristupovať k iným častiam alebo komponentom IT Strany 1, ktoré nie sú predmetom tejto Zmluvy,
 - h) inštalovať v IT Strany 1 akýkoľvek počítačový program alebo technický prostriedok,
 - i) na bežné činnosti v IT Strany 1 súvisiace s plnením predmetu Zmluvy používať privilegované prístupové oprávnenia vzhľadom na používateľskú rolu,
 - j) vzdialene sa prihlasovať do IT Strany 1 technickými prostriedkami, ktoré neboli Stranou 1 schválené v súlade s touto Zmluvou,
 - k) poskytovať údaje, ktoré získali alebo s ktorými prišli do styku počas vzdialeného prístupu do IT Strany 1 tretím osobám.
5. Strana 2 zodpovedá za dôvernosť a ochranu svojich hesiel a zodpovedá za všetky udalosti a transakcie, ktoré sa uskutočnili v IT Strany 1 s použitím prihlasovacieho účtu Strany 2.
6. Ak Strana 1 zistí, že Strana 2 mala pokus o prístup k iným častiam alebo komponentom IT Strany 1, ktoré neboli zo strany Strany 1 odsúhlasené, bude okamžite Strane 2 zablokovaný vzdialený prístup do IT Strany 2 zo strany Strany 1.
7. Strana 2 bude automaticky odhlásená zo vzdialeného prístupu do IT Strany 1 po identifikovaní nečinnosti v IT Strany 1 viac ako 15 minút.
8. Strana 1 má právo na okamžité blokovanie vzdialených prístupov do IT Strany 1 v prípade:
- a) pri zistení BI alebo podozrení na BI ako aj o iných zistených skutočnostiach majúcich vplyv na zabezpečovanie informačnej a kybernetickej bezpečnosti prevádzkovaných IT Strany 1,
 - b) pri podozrení na pristupovanie do iných častí IT Strany 1 ako tých, ktoré súvisia s predmetom plnenia Zmluvy,
 - c) pri podozrení na pristupovanie do IT Strany 1 neschváleným technickým prostriedkom.
9. V objekte Strany 1 vykonáva Strana 2 činnosti súvisiace s predmetom plnenia vždy pod dozorom Oprávneného zamestnanca Strany 1.
10. Strana 2 vyhlasuje, že súhlasí s bezpečnostnými opatreniami podľa tejto Zmluvy a zaväzuje sa ich dodržiavať.
11. Strana 2 zabezpečí do 10 pracovných dní po podpise tejto Zmluvy súhlas s bezpečnostnými opatreniami podľa tejto Zmluvy a záväzok ich dodržiavať od Pracovníkov Strany 2.

12. Strana 2 je povinná dodržiavať bezpečnostnú dokumentáciu Strany 1, ktorú mu Strana 1 sprístupnil na naštudovanie pred podpisom tejto Zmluvy. Bezpečnostnou dokumentáciou sa pre potreby tejto Zmluvy rozumie najmä interné riadiace akty alebo iné záväzné dokumenty Strany 1 vydané za účelom prijímania, realizácie, udržiavania, riadenia a kontroly bezpečnostných požiadaviek pre ochranu IS Strany 1.
13. Strana 2 je povinná prijímať primerané bezpečnostné opatrenia pri vzdialenom prístupe do IS Strany 1 minimálne v rozsahu ako má stanovené Strana 1 ako sú definované v tejto Zmluve.

Riadenia Bezpečnostných incidentov

1. Strana 2 je povinná pri zistení bezpečnostného incidentu alebo podozrení na bezpečnostný incident ako aj o iných zistených skutočnostiach majúcich vplyv na zabezpečovanie informačnej a kybernetickej bezpečnosti prevádzkovaných IT Strany 1 (všetko spolu ďalej len „BI“) bezodkladne nahlásiť túto skutočnosť na určené kontaktné miesto, a to na elektronickú adresu Strany 1
2. Predmetom tejto Zmluvy nie je riešenie BI týkajúcich sa činnosti súvisiacich s predmetom plnenia.
3. BI musí byť konkrétne, nezameniteľne a zrozumiteľne špecifikovaný. Hlásenie vykonáva Strana 2.
4. Hlásenie o BI obsahuje minimálne:
 - a) kontaktné údaje Pracovníka Strany 2, ktorý identifikoval BI alebo podozrenie na BI,
 - b) časové údaje zistenia a/alebo vzniku BI alebo podozrenia na BI,
 - c) popis vykonávaných činností v IT Strany 1 pri identifikovaní BI alebo podozrenia na BI,
 - d) detailný opis priebehu BI a jeho prvotnú identifikáciu alebo podozrenie (prejavy, správanie sa IT Strany 1, ktoré naznačili/jednoznačne identifikovali BI),
 - e) zoznam zasiahnutých alebo potencionálne zasiahnutých častí/komponentov/aktív IT Strany 1 BI (hostname, MAC adresu, IP @u, identifikačné údaje zariadení, identifikácia IS a pod.), zoznam údajov zasiahnutých alebo potencionálne zasiahnutých BI, zúčastnených osôb, dátum a čas manipulácie s údajmi, vymedzenie miesta ich uloženia,
 - f) informáciu o vykonaných opatreniach smerujúcich k zmierneniu dopadov BI, vrátane dátumu a času realizácie opatrení.
5. Pracovníci Strany 2, vykonávajúci činnosti v IT Strany 1 prostredníctvom vzdialeného prístupu sú povinní pri vyšetrovaní BI, ktorý súvisí s plnením tejto dohody, zamestnancom Strany 1 alebo iným príslušným orgánom, poskytnúť potrebnú súčinnosť.
6. Po vzniku BI alebo podozrenia na BI nesmie Strana 2 vykonávajúca činnosti v IT Strany 1 prostredníctvom vzdialeného prístupu vykonávať akékoľvek aktivity, ktoré by mohli viesť k znehodnoteniu dôkazov alebo k zhoršeniu dôsledkov BI.
7. Strana 1 rieši nahlásený BI v rámci svojich kapacít v súlade so zákonom o ITVS a zákonom č. 95/2019 Z. z. a príslušných vyhlášok k uvedeným zákonom.
8. Za dočasné vyriešenie BI sa považuje i náhradný spôsob vyriešenia BI s cieľom zabezpečiť prevádzkyschopnosť IS Strany 1, a to až do doby definitívneho vyriešenia BI alebo odstránenia dôsledkov BI.

9. Ak zistený BI bude mať za následok narušenie integrity, dostupnosti a dôvernosti služieb poskytovaných Stranou 2, všetky povinnosti vyplývajúce prevádzkovateľovi základnej služby zo zákona č. 69/2018 Z. z. a/alebo 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 znáša Strana 1.
10. Strana 2 eviduje všetky BI súvisiace so vzdialeným prístupom do IT Strany 1 identifikovaného pri vykonávaní činností súvisiacich predmetom plnenia, ich prešetrenie, riešenie a uzatvorenie a aj prípadné nápravné opatrenia.
11. Strana 2 informuje Stranu 1 o vyriešení BI súvisiaceho so vzdialeným prístupom do IT Strany 1 pre činnosti súvisiace s predmetom plnenia. Strana 1 je povinná v súvislosti so vzdialeným prístupom do IT Strany 1 na základe pokynov Strany 2 prijať nápravné opatrenia, ktoré boli schválené Stranou 1 pri riešení BI a súvisia s plnením predmetu tejto Zmluvy. Bezpečnostné opatrenia KIB
12. Zmluvné strany berú na vedomie, že prístupom k zmluve budú dodržiavať ustanovenia vyhlášky č. 362/2018 Z.z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

Článok VII

Mlčanlivosť

1. Zmluvné strany potvrdzujú, že pre účely tejto Zmluvy Dôvernými informáciami, ak nie je ďalej dohodnuté inak, sú všetky informácie, ktoré Strana 1 poskytne a/alebo sprístupní Strane 2 v súvislosti s touto Zmluvou, tzn. v súvislosti s vývojom a dodaním Diela, ak boli Strane 1 ako dôverné označené alebo ide o informácie, ktoré nie je potrebné takto označovať podľa bodu 10.4 tohto článku nižšie.
2. Za Dôverné informácie sa považujú najmä (ale nie bezvýhradne):
 - a) akékoľvek informácie, ktoré sa Strana 2 dozvie v súvislosti vzájomnej spolupráce, na základe tejto Zmluvy, ktoré nie sú v obchodných kruhoch bežne dostupné a poskytnutie a/alebo sprístupnenie ktorých môže spôsobiť Strane 1 majetkovú, nemajetkovú alebo inú ujmu/škodu,
 - b) akákoľvek dokumentácia poskytnutá Stranou 2 Strane 1,
 - c) vzájomná komunikácia zmluvných strán akoukoľvek formou, vrátane obsahu tejto Zmluvy,
 - d) know how Strany 1,
 - e) akékoľvek informácie týkajúce sa IT systémov, softvérových nástrojov, ako aj dát Strany 1,
 - f) vnútorné predpisy Strany 1, vrátane nastavených procesov, postupov,
 - g) ďalšie podklady a/alebo informácie, ktoré sú takto označené.
3. Strana 2 sa zaväzuje, že všetky informácie poskytnuté Stranou 1 použije len na účely priamo súvisiace so spolupracou na základe tejto Zmluvy, nebude ich ďalej rozširovať, zverejňovať, reprodukovat' a/alebo inak sprístupňovať, a ani ich akýmkoľvek spôsobom neposkytne tretím stranám bez preukázateľného písomného súhlasu Strany 1.
4. Informácie je Strana 2 oprávnená sprístupniť v nevyhnutnom rozsahu a výlučne v rámci spolupráce na základe tejto Zmluvy svojim štatutárom, zamestnancom, pričom títo všetci musia byť viazaní povinnosťou mlčanlivosti, a to minimálne v rozsahu tejto Zmluvy. Strana 1 týmto zároveň udeľuje súhlas Strane 2 so sprístupnením informácií Strane 2 a jej subdodávateľom a to v nevyhnutnom rozsahu a len v zmysle spolupráce na základe tejto Zmluvy.

5. Porušením ktorejkoľvek povinností týkajúcej sa ochrany informácií uvedenej v tomto článku Zmluvy zo Strany 2 vzniká Strane1 voči Strane 2 nárok na zaplatenie zmluvnej pokuty vo výške 10.000,- EUR (slovom: desaťtisíc EUR) za každé takéto porušenie a nárok na náhradu škody vo výške prevyšujúcej zmluvnú pokutu.

Článok VIII

Záverečné ustanovenia

6. Táto Zmluva predstavuje vyjadrenie vzájomnej vôle spolupracovať a jej obsah môže byť menený alebo dopĺňaný len formou písomných dodatkov podpísaných oboma Zmluvnými stranami.
7. Táto Zmluva je vyhotovená v dvoch rovnopisoch, po jednom pre každú Stranu.

V Bratislave, dňa

V Bratislave, dňa

Pôdohospodárska platobná agentúra

Ing. Marek Čepko
generálny riaditeľ

AXASOFT a.s.

Ing. Mgr. Peter Čaniga
predseda predstavenstva