2023-0109-116420

COLONNADE
A FAIRFAX COMPANY

Originál

Poistná zmluva č. 8-803-014595

Poisťovňa / poistiteľ	**Colonnade Insurance S.A.** so sídlom Rue Jean Piret 1, L-2350 Luxemburg, Luxembursko zapísaná v Obchodnom registri Luxemburg pod č. B 61605
	konajúca prostredníctvom
	Colonnade Insurance S.A., pobočka poisťovne z iného členského štátu zapísaná v Obchodnom registri Okresného súdu Košice I, oddiel Po, vložka číslo 591/V
Sídlo pobočky	Moldavská cesta 8 B, 042 80 Košice, Slovenská republika
IČO **IČ DPH**	50 013 602 SK4120026471
V zastúpení	Ing. Ivan Hollý, underwriter senior konajúci na základe poverenia Ing. Ján Šajban, senior underwriter konajúci na základe poverenia
	a
Poistník / Poistený	**Slovenská elektrizačná prenosová sústava, a.s.** zapísaná v Obchodnom registri Okresného súdu Bratislava I, Oddiel: Sa, Vložka číslo: 2906/B ďalej len ako „**poistník**“ alebo „**poistený**“ alebo „**klient**“
Sídlo	Mlynské nivy 59/A, Bratislava 824 84, Slovenská republika
IČO **IČ DPH**	35 829 141 SK2020261342
Bankové spojenie	Tatra banka, a. s. SK30 1100 0000 0026 2019 1900; TATRSKBX
V zastúpení	Ing. Peter Dovhun, predseda predstavenstva Marián Širanec, MBA, člen predstavenstva

uzatvárajú v zmysle všeobecne záväzných právnych predpisov túto poistnú zmluvu na:

POISTENIE ZODPOVEDNOSTI ZA ŠKODU

Táto poistná zmluva, osobitné zmluvné dojednania, všeobecné poistné podmienky, dotazník vyplnený poistníkom a prílohy tvoria spolu jeden neoddeliteľný dokument, ďalej len „poistná zmluva“. Akékoľvek slovo alebo výraz, ktorému sa prikladá špecifický význam, bude mať tento význam v celej poistnej zmluve.

Poistiteľ sa zaväzuje poskytovať poistenému / poisteným poistnú ochranu v súlade s podmienkami tejto zmluvy a poistník sa zaväzuje zaplatiť poistiteľovi poistné v súlade s podmienkami tejto poistnej zmluvy.

Sprostredkovateľ poistenia	**Marsh s.r.o.** **Nikola Zachař; nikola.zachar@marsh.com**

UW: Ing. Ivan Hollý

Poistná zmluva č. 8-803-014595

Druh poistenia:	**Poistenie zodpovednosti za škodu súvisiacu s ochranou osobných údajov / Poistenie kybernetických rizík Colonnade Insurance S.A.**
Doba trvania poistenia (Poistná doba):	**1 rok (12 mesiacov) od dátumu účinnosti v zmysle osobitných zmluvných dojednaní;** na **dobu určitú**
Retroaktívny dátum:	**dátum účinnosti v zmysle osobitných zmluvných dojednaní**
Činnosť poisteného na ktorú sa poistenie vzťahuje:	**Prenos elektriny**
Teritoriálny rozsah poistného krytia:	**Európa**
Čistý obrat spoločnosti za posledné ukončené účtovné obdobie:	**431 495 738,- EUR**
Referenčná hodnota obratu spoločnosti:	**440 000 000,- EUR**

Rozsah / druh poistenia v zmysle Všeobecných poistných podmienok poistenia kybernetických rizík (CI 1002/22/12):

Neoprávnené nakladanie s údajmi (bod A. VPP):	**kryté poistením**
Porušenie administratívnych a regulačných povinností (bod B. VPP):	**kryté poistením**
Náklady na odborné služby (bod C. VPP):	**kryté poistením**
Zverejnenie digitálneho obsahu v multimédiách (bod D. VPP):	**kryté poistením**
	kryté poistením
Prerušenie prevádzky siete (bod F. VPP):	**kryté poistením**

Limit poistného plnenia (Poistná suma):	**5 000 000,- EUR** na jednu a spolu na všetky poistné udalosti počas doby trvania poistenia
Sublimity poistného plnenia	
• **B.1 - Sublimit poistného plnenia pre Náklady spojené s Konaním dozorného orgánu:**	**Sublimit 100% z limitu poistného plnenia** na jednu a spolu na všetky poistné udalosti počas doby trvania poistenia
• **B.2 - Sublimit poistného plnenia pre Pokuty uložené Dozorným orgánom:**	**Sublimit 100% z limitu poistného plnenia** na jednu a spolu na všetky poistné udalosti počas doby trvania poistenia

COLONNADE
A FAIRFAX COMPANY

Poistná zmluva č. 8-803-014595

• **C.1 - Sublimit poistného plnenia pre Náklady za forenzné služby v oblasti kybernetickej bezpečnosti:**	**Sublimit 100% z limitu poistného plnenia** na jednu a spolu na všetky poistné udalosti počas doby trvania poistenia
• **C.2 - Sublimit poistného plnenia pre Náklady na nápravu dobrého mena Spoločnosti:**	**Sublimit 100% z limitu poistného plnenia** na jednu a spolu na všetky poistné udalosti počas doby trvania poistenia
• **C.3 - Sublimit poistného plnenia pre Náklady na nápravu dobrého mena osoby / jednotlivca:**	**Sublimit 100% z limitu poistného plnenia** na jednu a spolu na všetky poistné udalosti počas doby trvania poistenia
• **C.4 - Sublimit poistného plnenia pre Náklady na oznámenie Dotknutej osobe**	**Sublimit 100% z limitu poistného plnenia** na jednu a spolu na všetky poistné udalosti počas doby trvania poistenia
• **C.5 - Sublimit poistného plnenia pre Náklady na obnovu elektronických dát:**	**Sublimit 100% z limitu poistného plnenia** na jednu a spolu na všetky poistné udalosti počas doby trvania poistenia
Doplnkové Poistenie:	
• **D. - Sublimit poistného plnenia pre Zverejnenie digitálneho obsahu v multimédiách:**	**Sublimit 100% z limitu poistného plnenia** na jednu a spolu na všetky poistné udalosti počas doby trvania poistenia **Sublimit 50% z limitu poistného plnenia maximálne však 2 500 000,- EUR** na jednu a spolu na všetky poistné udalosti počas doby trvania poistenia
• **F. - Sublimit poistného plnenia pre Prerušenie prevádzky siete:**	**Sublimit 25% z limitu poistného plnenia maximálne však 1 250 000,- EUR** na jednu a spolu na všetky poistné udalosti počas doby trvania poistenia Sublimity poistného plnenia nie sú doplnkovými limitmi k limitu poistného plnenia a nijakým spôsobom nezvyšujú limit poistného plnenia.
Spoluúčasť:	**250 000,- EUR** pre jednu a každú poistnú udalosť s výnimkou nižšie uvedeného **20% zo škody minimálne 250 000,- EUR**
• **Spoluúčasť pre Prerušenie prevádzky siete:**	**vo výške škody spôsobenej za 48 hodín prerušenia prevádzky siete minimálne však 250 000,- EUR**
Poistné za dobu trvania poistenia:	**250 000,- EUR**
Bankové údaje:	peňažný ústav: **Citibank Europe plc, pobočka zahr. banky** IBAN: **SK16 8130 0000 0011 0210 0306** BIC (SWIFT): **CITISKBA** variabilný symbol: **číslo poistnej zmluvy bez pomlčiek** konštantný symbol: **3558**

Poistná zmluva č. 8-803-014595

Splatnosť poistného za jednotlivé poistné obdobie:	**deň účinnosti poistnej zmluvy** v zmysle bankových údajov Poistiteľ má právo posunúť dátum splatnosti poistného za konkrétne poistné obdobie na neskorší dátum, pričom v takom prípade platí dátum splatnosti uvedený na faktúre vystavenej poisťovňou.
Kontaktné telefónne číslo asistenčnej služby pre prípad poistnej / kybernetickej udalosti:	**+421 918 453 149**

Osobitné zmluvné dojednania

1. Poistnou udalosťou sa v zmysle tejto zmluvy rozumie taká nepredvídateľná udalosť, s ktorou je spojený vznik povinnosti poisťovne plniť a ktorá bola po prvýkrát písomne uplatnená voči poistenému (v prípade, ak ide o poistenie zodpovednosti za škodu) a poisťovni nahlásená počas doby trvania poistenia. Retroaktívny dátum je dátum stanovený v poistnej zmluve, ktorý predchádza vzniku poistenia, a ktorý určuje začiatok plynutia doby, počas ktorej mohlo dôjsť k porušeniu povinností majúcich za následok vznik škody krytej touto poistnou zmluvou. Retroaktívny dátum sa vzťahuje k poisteniu zodpovednosti za škodu a znamená dátum, kedy najskôr v minulosti mohlo dôjsť k porušeniu povinností majúcich za následok vznik škody krytej touto poistnou zmluvou, aby takéto porušenie povinností mohlo byť považované za príčinu vzniku povinnosti poisťovne poskytnúť poistné plnenie. Podmienkou platnosti poistnej zmluvy je, že poistený nemal v čase jej uzatvorenia vedomosť o porušení takejto povinnosti.

2. Zmluvné strany sa dohodli, že poistenie sa vzťahuje výlučne na poistníka / poisteného t.j. spoločnosť Slovenská elektrizačná prenosová sústava, a.s..

3. Neoddeliteľnou súčasťou tejto poistnej zmluvy je poistníkom kompletne vyplnený a oprávnenou osobou poistníka podpísané dotazníky „QUESTIONNAIRE FOR CYBER RISKS INSURANCE" a „Cyber Risk Assessment Questionnaire Endorsement ICS and OT", ktoré sa vzťahujú bez rozdielu na všetkých poistených v rozsahu tejto poistnej zmluvy.

4. Poistné za poistné obdobie je stanovené ako minimálne poistné (prináleží poistiteľovi vždy) na základe žiadateľom deklarovaného čistého obratu žiadateľa (v zmysle účtovnej závierky) za posledné ukončené účtovné obdobie vo výške uvedenej v tejto poistnej zmluve, ktorý je v rozmedzí do referenčnej hodnoty obratu uvedenej v tejto poistnej zmluve.

5. Akékoľvek straty, náklady, škody alebo výdavky spôsobené alebo vyplývajúce zo zraniteľnosti známej ako "Log4j" alebo "Log4shell" (CVE-2021-44228) a akýchkoľvek následných zraniteľností založených na tejto zraniteľnosti sú vylúčené z krytia.

6. Poistením nie sú kryté škody ani akékoľvek asociované náklady vyplývajúce z a / alebo spojené s nedostatočným šifrovaním osobných údajov a dôverných informácií poisteným v prípade, ak poistnému takáto povinnosť šifrovania vyplýva zo zákona alebo zmlúv uzatvorených s obchodnými partnermi poisteného.

7. Zmluvné strany sa dohodli, že bod F. Prerušenie prevádzky siete, časť F.2 Definície, odsek „Prerušenie prevádzky siete" Všeobecných poistných podmienok poistenia kybernetických rizík (CI 1002/22/12) (ďalej len „VPP") sa nahrádza nasledovným znením:
„Strata spôsobená prerušením prevádzky siete
znamená zníženie čistého zisku **Spoločnosti** v období od uplynutia **Čakacej doby** do obnovenia prevádzky **Počítačového systému** (maximálne však do uplynutia 120. dňa po začatí **Prerušenia prevádzky siete**), ktorý by **Spoločnosť** dosiahla nebyť **Prerušenia prevádzky siete** (a ktorá predstavuje ušlý zisk) pred zaplatením dane z príjmu a po započítaní úspor a nákladov na zmiernenie dopadov. Škoda spôsobená **Prerušením prevádzky siete** v tomto kontexte zahŕňa iba zníženie výnosov **Spoločnosti** v dôsledku zmluvného zníženia platieb za služby (ako napríklad prenos, systémové služby, krytie strát pri prenose, a výnosy z medzinárodnej predvádzky prenosovej sústavy, Market Coupling - MC, Inter TSO compensation - ITC) **Spoločnosti;** nezahŕňa škodu vyplývajúcu z **Nárokov Tretích osôb** z akéhokoľvek dôvodu."

8. Nakoľko spoločnosť Slovenská elektrizačná prenosová sústava, a.s. je povinnou osobou v zmysle zákona č. 211/2000 Z.z. o slobodnom prístupe k informáciám v platnom znení (ďalej aj ako „Zákon o slobode informácií"), Zmluvné strany sú oboznámené s tým, že Zmluva a daňové doklady súvisiace so Zmluvou budú zverejnené takým spôsobom, ktorý

Poistná zmluva č. 8-803-014595

pre povinne zverejňované zmluvy, objednávky a faktúry ukladá zákon o slobodnom prístupe k informáciám vo svojom ust. § 5a a § 5b.

9. Všetky ustanovenia tejto poistnej zmluvy sú samostatnými podmienkami poistnej zmluvy. V prípade, že je niektoré ustanovenie vyhlásené za neplatné, zakázané alebo nevynútiteľné súdom alebo iným príslušným orgánom z akéhokoľvek dôvodu, okrem prípadu, že je jeho výklad zúžený, táto poistná zmluva sa bude vykladať tak, ako keby toto neplatné, zakázané alebo nevynútiteľné ustanovenie bolo dohodnuté vo význame, ktorý nie je neplatný, zakázaný alebo nevynútiteľný; pričom však platnosť, zákonnosť a vynútiteľnosť ostatných ustanovení tejto poistnej zmluvy nebude nijakým spôsobom dotknutá alebo ohrozená.

10. Zmluvné strany sa dohodli, že pre prípad vrátenia akéhokoľvek nespotrebovaného poistného (tzv. vratka poistného) z tejto poistnej zmluvy / dodatku k poistnej zmluve bude takéto poistné vrátené poistiteľom výlučne na účet poistníka, z ktorého bolo pôvodne zaplatené poistné za dobu trvania poistenia resp. príslušné poistné obdobie.

11. Poistné za jednotlivé poistné obdobie bolo stanovené bez ohľadu na dĺžku jednotlivého poistného obdobia. Toto ustanovenie sa nevzťahuje na prípady zániku poistenia v zmysle jednotlivých ustanovení tejto poistnej zmluvy / dodatku k poistnej zmluve ako aj ustanovení príslušných právnych noriem.

12. Táto Zmluva nadobúda platnosť dňom podpísania obidvoma Zmluvnými stranami a účinnosť dňom nasledujúcim po dni zverejnenia tejto Zmluvy v súlade s ust. § 47a ods. 1 Občianskeho zákonníka.

13. Poistné je splatné na účet poistiteľa v zmysle ustanovení tejto poistnej zmluvy. Za dátum úhrady poistného / 1. splátky poistného bude považovaný dátum, kedy bolo poistné pripísané na účet poistiteľa.

14. Poistná zmluva je vyhotovená v dvoch originálnoch, pričom každá zo zmluvných strán obdrží jeden obomi stranami podpísaný originál poistnej zmluvy.

PREHLÁSENIE POISTNÍKA

Prehlasujem / potvrdzujem v mene všetkých poistených, že:

- všetky údaje uvedené v tejto poistnej zmluve a priloženom dotazníku zodpovedajú skutočnosti;
- ako odpoveď na písomnú otázku poistiteľa „Uveďte škody, ktoré Vaša spoločnosť spôsobila za predchádzajúcich 5 rokov." uvádzam, že v čase uzatvárania poistnej zmluvy nemám žiadnu vedomosť, že by som za obdobie predchádzajúcich 5 rokov spôsobil (s výnimkou škôd uvedených v dotazníku, ktorý je súčasťou tejto poistnej zmluvy) ja alebo jednotliví poistení akúkoľvek škodu tretím osobám v rozsahu tejto poistnej zmluvy, na základe čoho by si tretia osoba uplatnila voči mne alebo jednotlivým poisteným nárok na náhradu škody. Zároveň prehlasujem, že mi v čase uzavretia tejto poistnej zmluvy nie je známa žiadna ďalšia skutočnosť, na základe ktorej by mohol byť vznesený voči mne alebo jednotlivým poisteným oprávnený nárok na náhradu škody;
- ako odpoveď na písomnú otázku poistiteľa „Uveďte škody, ktoré ste utrpeli ku dňu podpisu poistnej zmluvy" uvádzam, že som neutrpel žiadnu škodu v rozsahu krytia tejto poistnej zmluvy (s výnimkou škôd uvedených v dotazníku, ktorý je súčasťou tejto poistnej zmluvy);
- nevstúpil som akýmkoľvek spôsobom, či už priamo alebo nepriamo, od momentu, kedy som ja alebo mnou poverená osoba, najmä sprostredkovateľ poistenia, začal rokovania s poistiteľom ohľadom uzavretia tejto poistnej zmluvy alebo dodatku k poistnej zmluve do interakcie s krajinami alebo oblasťami, na ktoré sa vzťahujú sankcie vlády Slovenskej republiky, Európskej únie, Organizácie spojených národov, Organizácie pre správu zahraničných aktív (OFAC) alebo vlády USA resp. s osobami, ktoré sú na sankčných zoznamoch vyššie uvedených vlád alebo organizácií. Zároveň prehlasujem, že mi v čase uzavretia tejto poistnej zmluvy resp. dodatku k poistnej zmluve nie je známa žiadna ďalšia skutočnosť, na základe ktorej by mohol byť vznesený voči mne nárok na náhradu škody alebo by som si mohol uplatňovať náhradu škody v súvislosti s vyššie uvedeným;
- bol som oboznámený so Všeobecnými poistnými podmienkami a Osobitnými zmluvnými dojednaniami;
- odpoveďou na všetky písomné otázky poistiteľa uvedené v prílohe „Doplňujúce otázky k činnosti poisteného" je „Nie";
- v čase uzatvárania tejto poistnej zmluvy odpovedám „áno" na všetky v tomto odseku nižšie uvedené body v úvodzovkách;

  „Žiadateľ preveril svoje procesy a identifikoval oblasti, ktoré by mohli byť v rozpore s dodržiavaním pravidiel nariadenia GDPR a / alebo jeho lokálnej právnej úpravy (ďalej len „GDPR") a urobil potrebné kroky na to, aby bol v súlade s GDPR riadne zdokumentovaným spôsobom, najmä s odkazom na nasledovné oblasti:

1. Žiadateľ preukázateľne zdokumentoval, aké osobné údaje má k dispozícii, odkiaľ pochádzajú, s kým ich zdieľa a zároveň vedie záznamy o svojich činnostiach spracovania údajov;

2. Žiadateľ preukázateľne identifikoval legislatívny rámec svojich aktivít spracovania údajov a prehodnotil svoje súčasné upozornenia o ochrane osobných údajov a v prípade potreby vykonal potrebné zmeny podľa požiadaviek GDPR;

3. Žiadateľ preukázateľne preskúmal a v prípade potreby aktualizoval svoje interné postupy tak, aby zabezpečí, že garantuje všetky práva, ktoré majú jednotlivci v zmysle GPPR (vrátane, ale nie výlučne, z hľadiska vymazania osobných údajov, poskytnutia údajov elektronicky, všeobecne používaného formátu a prístupu k údajom);

4. Žiadateľ preukázateľne preskúmal, ako hľadá, zaznamenáva, spravuje súhlas na spracovávanie dát a či je prípadne potrebné vykonať akékoľvek zmeny. Zároveň či obnovil potrebný súhlas, ak nespĺňa štandard GDPR;

5. Žiadateľ preukázateľne preskúmal alebo stanovil svoje interné postupy na odhaľovanie, oznamovanie a vyšetrovanie porušenia ochrany osobných údajov a má vedomosť o spôsobe informovania orgánu ochrany údajov (a prípadne aj niektorých ďalších orgánov) v prípade porušenia ochrany osobných údajov.

6. Pokiaľ sa to v zmysle GDPR vzťahuje na žiadateľa, vykonal zároveň posúdenie vplyvu ochrany údajov;

7. Pokiaľ sa to v zmysle GDPR vzťahuje na žiadateľa, určil osobu pre ochranu údajov (tzv. Data Protection Officer „DPO"), interného zamestnanca alebo externého poradcu pre ochranu údajov, ktorý preberá zodpovednosť za dodržiavanie ochrany údajov v zmysle GDPR a má vedomosti, podporu a právomoci efektívne vykonávať svoju úlohu DPO;

8. Žiadateľ potvrdzuje, že nevykonáva žiadne činnosti v nasledujúcich odvetviach:
   - zdravotnícke služby;
   - telekomunikácie (vrátane internetu, prevádzkovania webových stránok, poskytovanie cloudových riešení, atď.) okrem podpornej činnosti v rámci prenosu telekomunikačných dát medzi technickými zariadeniami prenosovej sústavy;
   - call centrá;
   - telemarketingové služby;
   - služby spracovania dát (outsourcing pre tretie strany);
   - poskytovanie akýchkoľvek finančných, bankových a / alebo platobných služieb;
   - poisťovacie služby a sprostredkovanie poistenia;
   - verejná správa (štátne a miestne orgány, úrady a spoločnosti, v ktorých majú vlastnícky podiel);
   - letecké spoločnosti;
   - prevádzkovanie hazardných hier.

9. Žiadateľ vykonáva pravidelné, automatické zálohovanie alebo postupy obnovenia kritických systémov, údajov a informácií.

10. Žiadateľ má medzi internou a externou sieťou tzv. firewall a používa antivírusovú ochranu pred škodlivým softvérom, ochranu proti tzv. spyware alebo malware a má prístup do vlastného systému chránený minimálne prístupovým menom a heslom."

- nezbieram, nearchivujem, nedistribuujem ani iným spôsobom nespracúvam, alebo nie sú pre mňa treťou stranou spracúvané akékoľvek údaje o platobných alebo bankových kartách tretích osôb;

- nepoužívam systémy, ktoré ich výrobca / vývojár už nepodporuje v žiadnom kritickom systéme (s výnimkou prípadov, kde boli zo strany žiadateľa prijaté tzv. kompenzačné opatrenia, ktoré znižujú mieru rizika, ktoré vychádza z neaplikovania záplat, ktoré sa obecne riadia internou smernicou pre riadenie procesu ošetrovania zraniteľností - SM 05/2023 Manažment zraniteľností) a v spoločnosti existuje systém riadenia opravy platných systémov tzv. „patch management proces" pre kritické systémy a aplikácie;

- vykonávam pravidelné, automatické zálohovanie alebo postupy obnovenia kritických systémov, údajov a informácií;

- rozumiem všetkým ustanoveniam tejto poistnej zmluvy a súhlasím s nimi.

COLONNADE
A FAIRFAX COMPANY

Poistná zmluva č. 8-803-014595

Zároveň prehlasujem, že mi boli poskytnuté Informácie o spracúvaní osobných údajov podľa článkov 13 a 14 nariadenia Európskeho parlamentu a Rady 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktoré sú prístupné aj na webovom sídle poistiteľa www.colonnade.sk .

Neoddeliteľné prílohy tejto poistnej zmluvy:

1. Všeobecné poistné podmienky poistenia kybernetických rizík (CI 1002/22/12)
2. Dotazníky „QUESTIONNAIRE FOR CYBER RISKS INSURANCE" a „Cyber Risk Assessment Questionnaire Endorsement ICS and OT" – kompletne vyplnené a podpísané oprávnenou osobou poistníka
3. Výpis z obchodného registra poistníka
4. Informácie o spracúvaní osobných údajov (CI Info GDPR/22/11)
5. Doplňujúce otázky k činnosti poisteného

V Bratislave, dňa .....

V Bratislave, dňa 2

Ing. Peter Dovhun
predseda predstavenstva
Slovenská elektrizačná prenosová sústava, a.s.

Ing. Ivan Holly
underwriter senior konajúci na základe poverenia
Colonnade Insurance S.A.,
pobočka poisťovne z iného členského štátu

Marián Širanec, MBA
člen predstavenstva
Slovenská elektrizačná prenosová sústava, a.s.

Ing. Ján Šajban
senior underwriter konajúci na základe poverenia
Colonnade Insurance S.A.,
pobočka poisťovne z iného členského štátu

COLONNADE
A FAIRFAX COMPANY

Všeobecné poistné podmienky poistenia kybernetických rizík (CI 1002/22/12)
(ďalej len „**VPP**")

1. Rozsah Poistenia, Poistná udalosť, Poistné riziko

Toto **Poistenie** sa dojednáva primárne pre prípad zodpovednosti za **Škodu** spôsobenú **Poisteným Tretím osobám** v súvislosti so **Spracúvaním osobných údajov** a pre prípad vzniku iných **Poistných udalostí** bližšie špecifikovaných v týchto **VPP**.

Pri dodržaní všetkých príslušných ustanovení **Poistnej zmluvy** a týchto **VPP**, z tohto **Poistenia** majú **Poistení** právo, aby v prípade vzniku **Poistnej udalosti** za nich **Poisťovňa** nahradila **Škodu**, za ktorú **Poistení** zodpovedajú, a ktorá je krytá príslušnou **Poistnou zmluvou** a týmito **VPP** za podmienky, že ku všetkým **Poistným udalostiam** dôjde alebo budú oznámené v dobe podľa článku 5.1 nižšie.

Poisťovňa poskytne **Poistné plnenie** podľa týchto **VPP** výlučne vo forme finančného plnenia.

A. Neoprávnené nakladanie s údajmi

A.1 Neoprávnené nakladanie s osobnými údajmi
Poisťovňa uhradí za **Poisteného** akékoľvek **Škody** a **Náklady právneho zastúpenia** vyplývajúce z **Nároku** vzneseného proti **Poistenému Dotknutou osobou** z dôvodu skutočného alebo údajného **Neoprávneného nakladania s osobnými údajmi.**

A.2 Neoprávnené nakladanie s dôvernými informáciami
Poisťovňa uhradí za **Poisteného** akékoľvek **Škody** a **Náklady právneho zastúpenia** vyplývajúce z **Nároku** vzneseného proti **Poistenému Treťou osobou** z dôvodu skutočného alebo údajného **Neoprávneného nakladania s dôvernými informáciami.**

A.3 Subdodávatelia
Poisťovňa uhradí za **Spoločnosť** akékoľvek **Škody** a **Náklady právneho zastúpenia** v súvislosti s **Nárokmi Tretích osôb voči Subdodávateľovi** (ak je Spoločnosť zmluvne zaviazaná poskytnúť za neho odškodnenie), ktoré vznikli z dôvodu skutočného alebo údajného porušenia povinností Subdodávateľa v súvislosti so spracúvaním **Osobných údajov** a/alebo **Dôverných informácií** v mene **Spoločnosti**, za ktoré je **Spoločnosť** zodpovedná.

A.4 Sieťová bezpečnosť
Poisťovňa uhradí za **Poisteného** akékoľvek **Škody** a **Náklady právneho zastúpenia** vyplývajúce z **Nároku** vzneseného proti **Poistenému Treťou osobou** z dôvodu akéhokoľvek konania, chyby alebo opomenutia **Poisteného** v súvislosti so spracúvaním **Osobných údajov** a **Dôverných informácií,** ktoré viedlo k:
(a) inštalácii akéhokoľvek nelegálneho softvéru, počítačového kódu alebo vírusu do **Dát tretej osoby** uložených v **Počítačových systémoch Spoločnosti,** pokiaľ bol taký softvér, počítačový kód alebo vírus špeciálne vytvorený za účelom narušenia prevádzky **Počítačových systémov Spoločnosti** alebo poškodenia softvéru alebo dát nahratých alebo zaznamenaných v **Počítačových systémoch Spoločnosti**;
(b) neoprávnenému odmietnutiu prístupu oprávnenej **Tretej osobe** k **Dátam tretej osoby**;
(c) neoprávnenému získaniu sieťového prístupového kódu (Network Access Code) od **Spoločnosti**;
(d) zničeniu, zmene, skresleniu, znehodnoteniu, poškodeniu, likvidácii alebo vymazaniu **Dát tretej osoby** uložených v akomkoľvek **Počítačovom systéme**;
(e) fyzickému odcudzeniu **IT vybavenia Spoločnosti Treťou osobou** alebo fyzickou stratou **IT vybavenia Spoločnosti** (s výnimkou ustanovení podľa odseku 4.2 (b) nižšie; alebo
(f) neoprávnenému sprístupneniu **Dát tretej osoby** v zmysle **Príslušného právneho predpisu o ochrane osobných údajov** prostredníctvom **Zamestnanca Spoločnosti**.

B. Porušenie administratívnych a regulačných povinností

B.1 Náklady spojené s Konaním dozorného orgánu
Poisťovňa uhradí **Poistenému** alebo za **Poisteného** akékoľvek **Náklady na odborné služby** (maximálne do výšky príslušného limitu uvedeného v **Poistnej zmluve**) vynaložené na právnu pomoc a právne zastúpenie v súvislosti s akýmkoľvek **Konaním dozorného orgánu**.

B.2 **Pokuty uložené Dozorným orgánom**
Poisťovňa uhradí **Poistenému** alebo za **Poisteného** akékoľvek **Pokuty** uložené **Dozorným orgánom** (maximálne do výšky príslušného limitu uvedeného v **Poistnej zmluve**), ktoré je **Poistený** povinný zaplatiť na základe rozhodnutia právoplatne ukončeného **Konania dozorného orgánu** vyplývajúceho z porušenia **Príslušného právneho predpisu o ochrane osobných údajov**.

C. Náklady na odborné služby

C.1 **Náklady za forenzné služby v oblasti kybernetickej bezpečnosti**
Poisťovňa uhradí **Spoločnosti** alebo za **Spoločnosť** akékoľvek **Náklady na odborné služby** (maximálne do výšky príslušného limitu uvedeného v **Poistnej zmluve**) vynaložené na nezávislé poradenstvo v oblasti kybernetickej bezpečnosti, v prípade, ak existuje dôvodné podozrenie, že došlo alebo dochádza k **Neoprávnenému prístupu do systému,** za účelom zistenia jeho príčiny a odporučenia opatrení za účelom zamedzenia alebo zmiernenia jeho nepriaznivých dôsledkov.
Tieto **Náklady na odborné služby** budú uhradené najskôr odo dňa doručenia oznámenia **Poisťovni** v súlade s článkom 5.1 nižšie.

C.2 **Náklady na nápravu dobrého mena Spoločnosti**
Poisťovňa uhradí **Spoločnosti** alebo za **Spoločnosť** akékoľvek **Náklady na odborné služby** (maximálne do výšky príslušného limitu uvedeného v **Poistnej zmluve**) vynaložené na poradenstvo poskytnuté nezávislými Tretími osobami (vrátane právneho poradenstva v oblasti mediálnej stratégie, krízového poradenstva a PR služieb) za účelom riadenia primeraných opatrení na zamedzenie alebo zmiernenie potenciálnych nepriaznivých dôsledkov **Mediálne významnej udalosti**, vrátane vytvorenia a implementácie komunikačnej stratégie.
Tieto **Náklady na odborné služby** budú uhradené za obdobie odo dňa ich oznámenia **Poisťovni** v súlade s článkom 5.1 nižšie do uplynutia 185 dní. Uvedená lehota začína plynúť deň po vykonaní oznámenia podľa predchádzajúcej vety.

C.3 **Náklady na nápravu dobrého mena osoby / jednotlivca**
Poisťovňa uhradí štatutárnemu orgánu **Spoločnosti** alebo jeho členovi a **Zamestnancovi zodpovednému za compliance (dodržiavanie právnych predpisov),** vedúcemu právneho oddelenia Spoločnosti alebo za tieto osoby / týchto jednotlivcov akékoľvek **Náklady na odborné služby** (maximálne do výšky príslušného limitu uvedeného v **Poistnej zmluve**) vynaložené na nezávislé poradenstvo v oblasti public relations za účelom zamedzenia alebo zmiernenia potenciálnych nepriaznivých dôsledkov (osobných aj pracovných) na dobré meno týchto osôb / jednotlivcov z dôvodu skutočného alebo údajného **Neoprávneného prístupu do systému** alebo porušenia **Príslušného právneho predpisu o ochrane osobných údajov**. Osoby uvedené v tomto odseku sú povinné vopred odkonzultovať vynaloženie Nákladov na odborné služby v zmysle tohto odseku s Poisťovňou, pričom Poisťovňa tieto Náklady na odborné služby uhradí len v prípade, ak ich vynaloženie vopred písomne odsúhlasila.
Náklady na odborné služby v zmysle tohto odseku budú uhradené za obdobie odo dňa ich oznámenia **Poisťovni** v súlade s článkom 5.1 nižšie do uplynutia 185 dní. Uvedená lehota začína plynúť deň po vykonaní oznámenia podľa predchádzajúcej vety.

C.4 **Náklady na oznámenie Dotknutej osobe**
Poisťovňa uhradí **Poistenému** alebo za **Poisteného** akékoľvek **Náklady na odborné služby** (maximálne do výšky príslušného limitu uvedeného v **Poistnej zmluve**) vynaložené na vyšetrovanie, zhromažďovanie informácií, prípravu a oznámenie **Dotknutej osobe** a / alebo ktorémukoľvek príslušnému **Dozornému orgánu** v súvislosti s akýmkoľvek skutočným alebo údajným **Neoprávneným prístupom do systému** alebo porušením **Príslušného právneho predpisu o ochrane osobných údajov** za podmienky, že **Poistený** je povinný vykonať takéto oznámenie podľa **Príslušného právneho predpisu o ochrane osobných údajov**.

C.5 **Náklady na obnovu elektronických dát**
Poisťovňa uhradí **Spoločnosti** alebo za **Spoločnosť** akékoľvek **Náklady na odborné služby** (maximálne do výšky príslušného limitu uvedeného v **Poistnej zmluve**) vynaložené na:
(a) zistenie, či **Dáta**, ktoré **Spoločnosť** spracúva, je alebo nie je možné obnoviť, znovu zhromaždiť alebo znovu vytvoriť; a
(b) znovu-vytvorenie alebo znovu-zhromaždenie **Dát**, ktoré **Spoločnosť** spracúva, v prípade ak záložný systém na úschovu dát takéto dáta nezachoval, alebo v prípade ak sú **Dáta** poškodené alebo zničené v dôsledku technického zlyhania alebo nedbalosti alebo nekonania osoby, ktorá vykonáva spracovanie **Dát** v mene **Spoločnosti** (bez ohľadu na to, či sa jedná o **Zamestnanca** alebo **Subdodávateľa**).

2. Doplnkové Poistenie

Pokiaľ je to explicitne uvedené v **Poistnej zmluve**, vzťahuje sa toto **Poistenie** aj na poistné riziká uvedené v tomto článku, a to za podmienok uvedených v **Poistnej zmluve** a týchto **VPP** vrátane osobitných poistných podmienok uvedených iba v tejto časti týchto **VPP**.

COLONNADE
A FAIRFAX COMPANY

D. Zverejnenie digitálneho obsahu v multimédiách

D.1 Zverejnenie digitálneho obsahu v multimédiách

Poisťovňa uhradí **Spoločnosti** alebo za **Spoločnosť** akékoľvek **Škody** a **Náklady právneho zastúpenia** (maximálne do výšky príslušného limitu uvedeného v **Poistnej zmluve**) vyplývajúce z **Nároku** vzneseného proti **Spoločnosti** **Treťou osobou** z dôvodu nasledujúcich porušení povinností súvisiacich so **Zverejnením digitálneho obsahu** alebo prípadne opomenutia **Zverejnenia digitálneho obsahu:**

(a) zásah do dobrej povesti, vrátane, ale nie výlučne, ohovárania, urážky na cti, osočovania, zľahčovania aj vo vzťahu k akejkoľvek fyzickej alebo právnickej osobe, alebo spôsobenia nemajetkovej ujmy s takýmto zásahom spojenej;

(b) nedbanlivostné porušenie autorského práva, práva k označeniu, práva k ochrannej známke, práva k obchodnému menu, firemnej identite, práva k doméne, a to vo forme vloženia webového linku na určitý element web stránky (deep-linking) alebo súbežného zobrazovania viacerých web stránok alebo v inej forme (framing);

(c) plagiátorstvo, pirátstvo alebo neoprávnené privlastnenie si či krádeži nápadov a informácií;

(d) porušenie alebo iný zásah do práva na súkromie, neoprávnené zverejnenie súkromných informácií, zneužitie alebo komerčné privlastnenie si mena, osobnosti alebo podoby;

(e) nekalá súťaž (ale len v súvislosti s niektorým z úkonov podľa písmena a) až d) vyššie);

(f) zodpovednosť vyplývajúcej z nedbanlivosti **Poisteného** vo vzťahu k akémukoľvek obsahu digitálneho média.

D.2 Definícia

Zverejnenie digitálneho obsahu

znamená zverejnenie alebo vysielanie obsahu napĺňajúceho charakteristiku uvedenú v článku D.1 prostredníctvom akéhokoľvek digitálneho média.

D.3 Výluky

Špecifikácia produktu

Doplnkové poistenie podľa tohto ustanovenia sa nevzťahuje na **Straty** vyplývajúce z, založené na alebo pripísateľné skutočnému alebo údajnému nepresnému, nesprávnemu alebo neúplnému oceneniu tovaru, výrobkov, služieb a všetkých cenových záruk, cenových vyhlásení, odhadov zmluvných cien, pravosti akýchkoľvek tovarov, výrobkov alebo služieb, alebo tomu, že akékoľvek tovary alebo služby nie sú v súlade s deklarovanou kvalitou alebo výkonnostnými parametrami / štandardmi. Okrem tejto výluky sa na toto **Doplnkové poistenie** vzťahujú primerane aj všeobecné výluky uvedené v článku 4 týchto **VPP**.

Účtovné údaje

Doplnkové poistenie sa nevzťahuje na **Straty** spôsobené chybami v akýchkoľvek účtovných alebo iných finančných záznamoch zverejnených **Spoločnosťou**, vrátane výročnej správy **Spoločnosti**, jej účtovnej závierky alebo akýchkoľvek informáciách poskytnutých akciovému alebo finančnému trhu.

COLONNADE
A FAIRFAX COMPANY

F. Prerušenie prevádzky siete

F.1 Prerušenie prevádzky siete

Poisťovňa uhradí **Poistenému** akúkoľvek **Stratu spôsobenú prerušením prevádzky siete** (maximálne do výšky príslušného limitu uvedeného v **Poistnej zmluve**), ktorá **Poistenému** vznikne v dôsledku **Prerušenia prevádzky siete**; táto **Strata spôsobená prerušením prevádzky siete** bude uhradená za dobu po uplynutí **Čakacej doby** a výhradne v dôsledku **Bezpečnostného zlyhania.**

F.2 Definície

Prerušenie prevádzky siete
znamená akékoľvek závažné prerušenie alebo pozastavenie služby poskytovanej **Počítačovým systémom** priamo spôsobené **Bezpečnostným zlyhaním**.

Strata spôsobená prerušením prevádzky siete
znamená zníženie čistého zisku **Spoločnosti** v období od uplynutia **Čakacej doby** do obnovenia prevádzky **Počítačového systému** (maximálne však do uplynutia 120. dňa po začatí **Prerušenia prevádzky siete**), ktorý by **Spoločnosť** dosiahla nebyť **Prerušenia prevádzky siete** (a ktorá predstavuje ušlý zisk) pred zaplatením dane z príjmu a po započítaní úspor a nákladov na zmiernenie dopadov. Škoda spôsobená **Prerušením prevádzky siete** v tomto kontexte zahŕňa iba zníženie výnosov **Spoločnosti** v dôsledku zmluvného zníženia platieb za služby **Spoločnosti;** nezahŕňa škodu vyplývajúcu z **Nárokov Tretích osôb** z akéhokoľvek dôvodu.

Bezpečnostné zlyhanie
znamená neoprávnenú infiltráciu do **Počítačového systému**, vrátane, nie však výlučne takú, ktorá vedie k Neoprávnenému prístupu do, neoprávnenému použitiu, zabráneniu prístupu do **Počítačového systému** alebo prijatiu alebo prenosu akéhokoľvek škodlivého kódu určeného na vyvolanie nežiadúcich účinkov alebo poškodenia **Počítačového systému**, alebo vedie k zlyhaniu predchádzania vyššie uvedeným zásahom. **Bezpečnostné zlyhanie** znamená ďalej takú neoprávnenú infiltráciu, ktorá je dôsledkom krádeže hesla alebo sieťového prístupového kódu z priestorov **Spoločnosti**, **Počítačového systému**, alebo štatutárnemu orgánu **Spoločnosti**, riadiacemu pracovníkovi, riaditeľovi alebo **Zamestnancovi Spoločnosti** inými ako elektronickými prostriedkami priamym porušením osobitných písomných bezpečnostných smerníc alebo postupov **Spoločnosti**.

Čakacia doba znamená dobu rovnajúcu sa počtu hodín uvedených v **Poistnej zmluve**, ktoré plynú po začatí **Prerušenia prevádzky siete** dovtedy, než začne vznikať **Strata spôsobená prerušením prevádzky siete**.

F.3 Výluky

Orgán štátnej a verejnej správy
Doplnkové poistenie podľa tohto ustanovenia sa nevzťahuje na **Straty spôsobené prerušením prevádzky siete** vyplývajúce z, založené na alebo pripísateľné akémukoľvek zmocneniu sa, zhabaniu, konfiškácii, znárodneniu alebo zničeniu **Počítačového systému** na základe rozhodnutia štátnej alebo inej verejnej inštitúcie.

Osobitné okolnosti prerušenia prevádzky siete
Doplnkové poistenie podľa tohto ustanovenia sa nevťahuje na **Stratu spôsobenú prerušením prevádzky siete** vyplývajúcu alebo inak súvisiacu s:

(a) Akoukoľvek škodou spôsobenou prerušením prevádzky externých sietí (ako napríklad elektrická energia a telekomunikácie vrátane internetu)
(b) **Prerušením prevádzky siete** alebo systému spôsobeným stratou spojenia s počítačovým systémom **Tretej osoby**, v dôsledku ktorého **Spoločnosť** nemôže nadviazať spojenie s týmito systémami;
(c) akýmikoľvek nákladmi na právne poradenstvo alebo zastúpenie;
(d) aktualizáciou, modernizáciou, vylepšením alebo výmenou akéhokoľvek **Počítačového systému** za systém vyššej úrovne, než na ktorej bol **Počítačový systém** predtým, než došlo ku **Strate spôsobenej prerušením prevádzky siete**;
(e) nevýhodnými obchodnými podmienkami; alebo
(f) odstránením softvérových programových chýb alebo nedostatkov.

COLONNADE
A FAIRFAX COMPANY

F.4 **Prehlásenie Poisteného**
Okrem ostatných povinností oznámenia skutočností podľa týchto **VPP**, je každý **Poistený** v súvislosti s uplatnením si nároku z Poistenia podľa tohto **Doplnkového poistenia** povinný:
(a) najneskôr do 90 dní po okamihu, kedy zistí **Stratu spôsobenú prerušením prevádzky siete** (pokiaľ nebude s **Poisťovňou** v písomnej forme dohodnuté inak), vyplniť, podpísať a odovzdať **Poisťovni** prehlásenie v písomnej forme obsahujúce detailný popis **Straty spôsobenej prerušením prevádzky siete** a okolností, ktoré k nej viedli. Toto prehlásenie musí ďalej obsahovať podrobný výpočet akýchkoľvek **Strát spôsobených prerušením prevádzky siete** ako aj všetky dokumenty a dôkazy, z ktorých výška **Strát spôsobených prerušením prevádzky siete** vyplýva;
(b) umožniť **Poisťovni** na jej žiadosť overiť si údaje, výpočty a dokumenty, ktoré sú rozhodujúce pre stanovenie výšky **Straty spôsobenej prerušením prevádzky siete** a poskytnúť jej ich; a
(c) vzdať sa prípadných profesijných výhod (vrátane povinnosti mlčanlivosti) a poskytnúť **Poisťovni** na jej žiadosť všetku potrebnú súčinnosť vrátane pomoci:
i. pri akomkoľvek vyšetrovaní / šetrení **Bezpečnostného zlyhania** alebo **Strát spôsobených prerušením prevádzky siete**;
ii. pri uplatnení si prípadných nárokov na náhradu škody v súvislosti s **Bezpečnostným zlyhaním**, ktoré má **Poistený alebo Spoločnosť** voči akejkoľvek Tretej osobe zodpovednej za zlyhanie;
iii. vyhotovením alebo poskytnutím všetkých dokumentov **Poisťovni**, ktoré si **Poisťovňa** vyžiada z dôvodu zaistenia si svojich práv vyplývajúcich z týchto **VPP**; a
iv. pri akýchkoľvek výpočtoch alebo oceňovaní uskutočňovaných **Poisťovňou** alebo pre **Poisťovňu** v súvislosti s ustanoveniami o **Prerušení prevádzky siete**.

Poisťovňa poskytne poistné plnenie z **Doplnkového poistenia** podľa tohto ustanovenia výlučne v prípade splnenia všetkých povinností v zmysle tohto článku **Poisteným**, a to až po tom, čo písomne potvrdí splnenie vyššie uvedených povinností **Poisteným**. Lehota na vyplatenie akéhokoľvek poistného plnenia v zmysle tohto ustanovenia je 15 dní.
Náklady a výdavky zistenia alebo preukázania škody **Poistených** v súvislosti s poistným krytím podľa tohto ustanovenia vrátane, nie však výlučne tých, ktoré súvisia s prípravou dokladov o výške **Straty spôsobenej prerušením prevádzky siete**, nie sú kryté **Poistnou zmluvou** a znáša ich **Poistený**.

Výpočet čistého zisku

F.5 **Určenie výšky čistého zisku**
Pri určení výšky **Straty spôsobenej prerušením prevádzky siete** za účelom stanovenia výšky poistného plnenia z poistného krytia **Straty spôsobenej prerušením prevádzky siete** sa osobitne prihliada na predošlé skúsenosti s obchodnou činnosťou **Spoločnosti** pred tým, ako **Bezpečnostné zlyhanie** nastalo a na pravdepodobný výsledok obchodnej činnosti **Spoločnosti** v prípade, **ak by k Bezpečnostnému zlyhaniu** nedošlo. Pri určení výšky **Straty spôsobenej prerušením prevádzky siete** sa neprihliada na (a **Poistná zmluva** nekryje) čistý výnos, ktorý by bol pravdepodobne dosiahnutý v dôsledku zvýšenia množstva obchodov zapríčineného priaznivými obchodnými podmienkami, ktoré spôsobili bezpečnostné zlyhania u iných podnikov. Určenie výšky **Straty spôsobenej prerušením prevádzky siete** bude založené na hodinovom základe a takom skutočnom znížení čistého zisku **Poisteného**, ktorý bol zapríčinený znížením výnosov alebo zvýšením poplatkov a výdavkov priamo pripísateľných **Prerušeniu prevádzky siete**.

F.6 **Stanovenie výšky Poistného plnenia**
V prípade, ak sa **Spoločnosť** a **Poisťovňa** nezhodnú na výške **Straty spôsobenej prerušením prevádzky siete**, každý z nich môže písomne požiadať o ohodnotenie výšky takejto straty. V prípade takejto požiadavky určí každá zo strán na tieto účely odborne spôsobilého a nezávislého odborníka. Každý z takto určených odborníkov potom samostatne určí výšku **Straty spôsobenej prerušením prevádzky siete**. Ak medzi nimi nedôjde k zhode, odborníci spoločne vyberú odborne spôsobilého a nezávislého experta so skúsenosťami v oblasti ohodnocovania strát s minimálne 10 ročnou praxou a predložia mu sporné otázky. Rozhodnutie / rozhodnutia odborníkmi zvoleného experta bude/ú konečné a záväzné. **Spoločnosť** a **Poisťovňa** sú samostatne povinní hradiť náklady svojich odborníkov a v rovnakej miere spoločne znášať náklady experta. Akékoľvek ohodnotenie **Straty spôsobenej prerušením prevádzky siete** musí byť realizované v súlade so všetkými podmienkami a výlukami **Poistnej zmluvy** vrátane týchto **VPP**.

3. Definície

3.1 **Pokuta uložená dozorným orgánom**
znamená akékoľvek poistiteľné pokuty, penále alebo iné finančné sankcie, ktoré je **Poistený** povinný zaplatiť štátu, príslušnému orgánu verejnej správy alebo inému **Dozornému orgánu** za porušenie **Príslušného právneho predpisu o ochrane osobných údajov. Pokuta uložená dozorným orgánom** nezahŕňa súkromno-právne pokuty, trovy správneho alebo súdneho konania, penále, sankcie alebo iné zmluvné dojednania obdobného charakteru a/alebo účinku a/alebo peňažné, nepeňažné, či iné tresty podľa predpisov trestného práva.

3.2 **Dáta** znamenajú:
(a) Dôverné informácie;

COLONNADE
A FAIRFAX COMPANY

(b) akékoľvek osobné údaje;
(c) akékoľvek iné informácie obchodnej, podnikateľskej alebo prevádzkovej povahy patriace **Spoločnosti** s výlukou kryptomien v akejkoľvek podobe (napr. Bitcoin, Litecoin, Namecoin, Peercoin a iné).

3.3 **Dcérska Spoločnosť** znamená akúkoľvek právnickú osobu, v ktorej **Poistník**, priamo alebo nepriamo, prostredníctvom jednej alebo viacerých **Spoločností** alebo osôb:
(a) ovláda zloženie štatutárneho orgánu;
(b) ovláda viac ako polovicu hlasovacích práv; alebo
(c) drží viac ako polovicu vydaných akcií alebo základného imania.
V prípade **Dcérskej Spoločnosti** alebo iného **Poisteného** sa **Poistenie** vzťahuje iba na porušenie **Príslušného právneho predpisu o ochrane osobných údajov** alebo skutok, pochybenie alebo opomenutie, ktoré viedlo k **Neoprávnenému prístupu do systému** a ku ktorému došlo v čase, keď takáto spoločnosť bola **Dcérskou spoločnosťou Poistníka**. **Poistná zmluva** sa vzťahuje iba na **Dcérsku spoločnosť** existujúcu v čase uzatvorenia **Poistnej zmluvy** a uvedenej v dotazníku vyplnenom **Poistníkom** a odovzdanom **Poisťovni** za účelom uzatvorenia **Poistnej zmluvy**. Iné dcérske spoločnosti ako dcérske spoločnosti podľa predchádzajúcej vety sú kryté týmto **Poistením** iba v prípade, ak s tým **Poisťovňa** vyslovila písomný súhlas.

3.4 **Dohoda o mimosúdnom vyrovnaní**
znamená akákoľvek dohoda o zmierlivom riešení sporu (vrátane súdneho zmieru) s konečnou platnosťou uzavretá medzi **Spoločnosťou** a **Treťou osobou** na základe predchádzajúceho písomného súhlasu **Poisťovne** za účelom dosiahnutia mimosúdneho riešenia akéhokoľvek prebiehajúceho alebo hroziaceho konania alebo sporu medzi **Poisteným** a **Treťou osobou**.

3.5 **Dotknutá osoba**
znamená akákoľvek fyzická osoba, ktorej **Osobné údaje** sú zhromažďované alebo spracúvané **Spoločnosťou** alebo pre **Spoločnosť**.

3.6 **Doplnkové poistenie**
znamená jednotlivé poistné krytia upravené v článku 2 týchto **VPP**, ktoré je možné, v prípade, ak to **Poistná zmluva** umožňuje, zahrnúť do poistného krytia v rámci **Poistenia**.

3.7 **Dozorný orgán**
znamená Úrad na ochranu osobných údajov Slovenskej republiky a akýkoľvek iný dozorný orgán, orgán verejnej správy ustanovený **Príslušným právnym predpisom o ochrane osobných údajov**, ktorý vykonáva dozor nad dodržiavaním povinností súvisiacich so spracúvaním a správou **Osobných údajov** (prípadne aj **Dôverných informácií**, pokiaľ je to relevantné), okrem iného aj Národná banka Slovenska.

3.8 **Dôverné informácie**
znamenajú akékoľvek;
(a) dôverné informácie, ktoré sú výlučným duševným vlastníctvom **Tretej osoby,** vrátane rozpočtov, zoznamov zákazníkov, marketingových plánov a iných informácií, ktorých sprístupnenie by prinieslo súťažnú výhodu inému súťažiteľovi, a ktoré inak nie sú iným súťažiteľom dostupné;
(b) dôverné informácie alebo informácie, na ktoré sa vzťahuje zákonná povinnosť mlčanlivosti (profesijné tajomstvo), ktoré patria **Tretej osobe** alebo ku ktorým má oprávnený prístup, vrátane akýchkoľvek dôverných informácií poskytovaných právnemu zástupcovi, účtovníkovi, daňovému alebo inému odbornému poradcovi v súvislosti s poskytovaním odborných služieb týmito osobami, pokiaľ takéto informácie nie sú verejne dostupné; alebo
(c) informácie, ktoré sú **Spoločnosti** oprávnene oznámené alebo inak sprístupnené, a ktoré **Spoločnosť** oprávnene získala a je o nich povinná zachovávať zákonnú alebo zmluvnú mlčanlivosť, prípadne ktoré jej boli poskytnuté alebo ich získala za okolností, z ktorých táto povinnosť mlčanlivosti priamo vyplýva; a ktoré boli oprávnene zhromaždené alebo sú spracúvané **Spoločnosťou** alebo pre **Spoločnosť**.

3.9 **IT / technické vybavenie**
znamená akákoľvek položka alebo prvok hardvéru, softvéru alebo vybavenia, ktorý je alebo môže byť použitý na účely vytvorenia, prístupu k, spracúvania, ochrany, monitorovania, uchovávania, obnovovania, zobrazovania alebo prenosu elektronických informácií akéhokoľvek druhu (vrátane hlasu).

3.10 **Konanie dozorného orgánu**
znamená akékoľvek formálne alebo oficiálne konanie, vyšetrovanie, šetrenie alebo audit zo strany **Dozorného orgánu** vedené voči **Poistenému** v oblasti ochrany **Osobných údajov** v súvislosti s použitím alebo údajným zneužitím **Osobných údajov** alebo kontrolou a spracúvaním **Osobných údajov** alebo postúpením spracúvania na **Subdodávateľa**, ktorý je regulovaný **Dozorným orgánom**. **Konanie dozorného orgánu** nezahŕňa akúkoľvek z vyššie uvedených alebo obdobných aktivít, ktorá sa týka všeobecne celého príslušného podnikateľského odvetvia.

3.11 **Kybernetický terorizmus**
znamená úmyselné použitie rušivých činností proti akémukoľvek počítačovému systému alebo sieti alebo výslovné ohrozenie používania takýchto aktivít so zámerom spôsobiť ujmu, ďalšie sociálne, ideologické, náboženské, politické alebo podobné ciele alebo zastrašiť akúkoľvek osobu za účelom dosiahnutia týchto cieľov.

3.12 **Limit poistného plnenia**
znamená čiastku hornej hranice **Poistného plnenia** za jednu a všetky **Poistné udalosti** počas **Poistného obdobia** uvedenú v **Poistnej zmluve** ako limit plnenia.

COLONNADE
A FAIRFAX COMPANY

3.13 **Mediálne významná udalosť**
znamená skutočné alebo hroziace verejné oznámenie alebo správa v akýchkoľvek médiách, ktorá priamo vyplýva zo skutočného, potenciálneho alebo údajného porušenia **Príslušného právneho predpisu o ochrane osobných údajov** alebo **Neoprávneného prístupu do systému,** a ktorá môže poškodiť povesť, goodwill a dobré meno **Spoločnosti** v okruhu osôb alebo podnikateľov, ktorí sú jej zákazníkmi alebo dodávateľmi, alebo s ktorými **Spoločnosť** pravidelne obchoduje v rámci výkonu svojej podnikateľskej činnosti.

3.14 **Náklady na odborné služby**
znamenajú primerané a nevyhnutné náklady, platby a výdavky na odmenu odborných poradcov, ktorí vykonávajú svoju činnosť pre **Poisteného** v súlade s týmito **VPP** a na základe predchádzajúceho písomného súhlasu **Poisťovne**.

3.15 **Náklady právneho zastúpenia**
znamenajú primerané a nevyhnutné náklady právneho zastúpenia, výdavky a ďalšie náklady, ktoré **Poistený** vynaložil v súlade s predchádzajúcim písomným súhlasom **Poisťovne** v súvislosti s obranou, šetrením akýmkoľvek opravným prostriedkom a / alebo vyrovnaním alebo iným zmierlivým riešením v súvislosti s akýmkoľvek **Nárokom** uplatneným voči **Poistenému**.
Náklady právneho zastúpenia nezahŕňajú fixné a personálne náklady, ani náhrady za stratu času **Poisteného**.

3.16 **Nárok**
znamená doručenie akéhokoľvek z nasledujúcich dokumentov **Poistenému:**
(a) doručenie **Oznámenia dozorného orgánu**;
(b) akúkoľvek písomnú požiadavku na náhradu ujmy alebo inú formu nápravy;
(c) akékoľvek občiansko-právne, správne alebo trestné konanie, v ktorom sa požaduje / ukladá náprava, uvedenie do súladu s právnym predpisom alebo iná sankcia; alebo
(d) písomná výzva **Dozorného orgánu** v súvislosti s **Konaním dozorného orgánu** (ale len vo vzťahu ku krytiu podľa časti B týchto **VPP**).
Nárok nezahŕňa akúkoľvek **Žiadosť dotknutej osoby** alebo nároky vznesené riaditeľom, členom predstavenstva, konateľom, **Zamestnancom zodpovedným za compliance (dodržiavanie právnych predpisov spoločnosti)**, alebo vedúcim právneho oddelenia **Spoločnosti**.
Nárok zo Spojených štátov amerických znamená akýkoľvek **Nárok** uskutočnený alebo trvajúci na území Spojených štátov amerických alebo akýchkoľvek ich štátov, správnych jednotiek, území a držav, a/alebo akýkoľvek **Nárok** založený na práve Spojených štátov amerických alebo akýchkoľvek ich štátov, správnych jednotiek, území a držav vznesený kdekoľvek na svete.

3.17 **Neoprávnené nakladanie s dôvernými informáciami**
znamená neoprávnené, náhodné alebo nedbalostné sprístupnenie alebo zverejnenie **Dôverných informácií Poisteným**, za ktoré zodpovedá **Spoločnosť**.

3.18 **Neoprávnené nakladanie s osobnými údajmi**
znamená neoprávnené sprístupnenie alebo zverejnenie **Osobných údajov Poisteným**, za ktoré zodpovedá **Spoločnosť** ako prevádzkovateľ alebo sprostredkovateľ v zmysle **Príslušného právneho predpisu o ochrane osobných údajov**.

3.19 **Neoprávnený prístup do systému**
znamená neoprávnený prístup **Tretej osoby** do **Počítačového systému Spoločnosti** alebo prístup a využitie **Počítačového systému Spoločnosti** nad rámec oprávnenia poskytnutého **Spoločnosťou**.

3.20 **Občiansky zákonník**
znamená zákon č. 40/1964 Zb. Občiansky zákonník, v znení neskorších predpisov.

3.21 **Osobné údaje**
znamenajú akékoľvek osobné informácie týkajúce sa **Dotknutej osoby**, ktoré je **Spoločnosť** oprávnená zhromažďovať alebo inak spracúvať alebo sú tieto údaje zhromažďované a spracúvané v mene **Spoločnosti** v rámci činnosti **Poisteného** v Európskej únii bez ohľadu, či sa spracúvanie vykonáva v Európskej únii a/alebo **Poistený** spracúva osobné údaje **Dotknutých osôb**, ktoré sa nachádzajú v Európskej únii.

3.22 **Počítačový systém**
znamená informačné technológie a komunikačné systémy, siete, služby a riešenia (vrátane IT / technického vybavenia), ktoré buď tvoria súčasť systémov a sietí **Spoločnosti**, alebo sa používajú pri poskytovaní služieb a riešení, ktoré sú prenajaté alebo inak sprístupnené **Spoločnosti** alebo sú vo výlučnom a bezpečnom užívaní **Spoločnosti** pre účely jej činnosti.

3.23 **Poistenie**
znamená poistenie rizík kybernetickej bezpečnosti, ktoré poskytuje **Poisťovňa** na základe **Poistnej zmluvy** uzavretej s **Poistníkom** a týchto **VPP**.

3.24 **Poisťovňa**
Colonnade Insurance S.A. so sídlom Rue Jean Piret 1, L-2350 Luxemburg, Luxembursko zapísaná v Obchodnom registri Luxemburg pod č. B 61605, konajúca v Slovenskej republike prostredníctvom Colonnade Insurance S.A., pobočka poisťovne z iného členského štátu, so sídlom Moldavská cesta 8 B, 042 80 Košice, Slovenská republika, IČO: 50 013 602, zapísaná v Obchodnom registri Okresného súdu Košice I, oddiel Po, vložka číslo 591/V

COLONNADE
A FAIRFAX COMPANY

3.25 **Poistná doba**
znamená doba, na ktorú bolo dojednané Poistenie, a ktorá je vymedzená v **Poistnej zmluve**. V prípade, že dôjde k zániku **Poistnej zmluvy** pred dátumom uvedeným ako koniec poistenia v **Poistnej zmluve**, pokladá sa za posledný deň **Poistenia** dátum zániku **Poistnej zmluvy**.

3.26 **Poistná udalosť**
znamená náhodnú skutočnosť, bližšie opísanú v **Poistnej zmluve** a/alebo týchto **VPP**, s ktorou je spojený vznik povinnosti **Poisťovne** poskytnúť **Poistné plnenie**.

3.27 **Poistná zmluva**
znamená poistná zmluva uzatvorená medzi **Poisťovňou** a **Poistníkom**, predmetom ktorej je **Poistenie**, a ktorej neoddeliteľnou súčasťou sú tieto **VPP**.

3.28 **Poistné**
znamená odplata za **Poistenie**, ktorú je **Poistník** povinný platiť **Poisťovni** vo výške a spôsobom dohodnutým v **Poistnej zmluve**. **Poistné** môže byť dohodnuté ako jednorazové poistné za celú **Poistnú dobu** alebo ako bežné poistné za jednotlivé poistné obdobia. Ak nie je v **Poistnej zmluve** stanovené inak, poistným obdobím je jeden kalendárny rok.

3.29 **Poistné plnenie**
znamená peňažné plnenie, ktoré **Poisťovňa** poskytne **Poistenému** v prípade vzniku **Poistnej udalosti**, a to spôsobom a za podmienok stanovených v **Poistnej zmluve** a týchto **VPP**.

3.30 **Poistník**
znamená právnickú alebo fyzickú osobu, ktorá uzatvorila **Poistnú zmluvu** s **Poisťovňou,** a ktorá je označená v **Poistnej zmluve** ako **Poistník**, na základe čoho je povinná **Poisťovni** platiť **Poistné**.

3.31 **Poistený**
znamená
(a) **Spoločnosť**;
(b) akákoľvek fyzická osoba, ktorá je štatutárnym orgánom **Spoločnosti** alebo jej členom, spoločníkom **Spoločnosti** alebo **Zamestnancom zodpovedným za compliance (dodržiavanie právnych predpisov)** alebo vedúcim právneho oddelenia **Spoločnosti** alebo iným členom vedenia **Spoločnosti** v rozsahu, v ktorom takáto osoba koná v rámci tejto funkcie;
(c) ktorýkoľvek zákonný alebo zmluvný zástupca **Poisteného** podľa písmena (a) a (b) vyššie v rozsahu, v ktorom je voči nemu uplatnený **Nárok** v súvislosti s konaním, chybou alebo opomenutím takéhoto **Poisteného**.

3.32 **Príslušný právny predpis o ochrane osobných údajov**
znamená nariadenie (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES, v znení neskorších zmien, zákon č. 18/2018 Z. z. o ochrane osobných údajov v znení neskorších predpisov a, ak je to aplikovateľné, jeho vykonávacie právne predpisy, vždy v platnom a účinnom znení, vrátane akýchkoľvek iných právnych predpisov ktoré ho / ich môžu počas **Poistnej doby** nahradiť, ako aj akékoľvek osobitné právne predpisy Európskej únie a Slovenskej republiky upravujúce práva a povinnosti pri spracúvaní a ochraňovaní **Osobných údajov** a súkromia pre konkrétnu hospodársku oblasť, v ktorej **Spoločnosť** vykonáva svoju podnikateľskú činnosť (napr. oblasť bankovníctva, poisťovníctva, energetiky, telekomunikácií, zdravotníctva a iné), vrátane súvisiacich podzákonných predpisov a vykonávacích ustanovení.

3.33 **Retroaktívny dátum**
znamená dátum uvedený v Poistnej zmluve ako retroaktívny dátum.

3.34 **Spoločnosť**
znamená **Poistníka** a ktorúkoľvek **Dcérsku Spoločnosť.**

3.35 **Spoluúčasť**
znamená čiastku uvedenú v Poistnej zmluve ako spoluúčasť, o ktorú je znížené Poistné plnenie.

3.36 **Strata**
znamená:
(a) **Škodu**, **Náklady právneho zastúpenia**, **Náklady na odborné služby**, **Pokuty uložené dozorným orgánom**; a
(b) **Stratu spôsobenú vydieraním** (pokiaľ je toto **Doplnkové Poistenie** dojednané v **Poistnej zmluve**) a **Stratu spôsobenú prerušením prevádzky siete** (pokiaľ je toto **Doplnkové Poistenie** dojednané v **Poistnej zmluve**).
Strata nie je plnenie, náklady na vedenie a interné (fixné alebo personálne) náklady **Poisteného** alebo náhrada za stratu času **Poisteného**.

3.37 **Subdodávateľ**
znamená fyzickú alebo právnickú osobu, ktorá pre **Spoločnosť** v súlade s **Príslušným právnym predpisom o ochrane osobných údajov** zhromažďuje alebo spracúva **Osobné údaje** alebo **Dôverné informácie** či už na základe zmluvy alebo právneho predpisu.

3.38 **Škoda**
znamená akúkoľvek čiastku, ktorú bude **Poistený** povinný zaplatiť **Tretej osobe** na základe:
(a) právoplatného rozsudku alebo rozhodnutia vynesené v neprospech **Poisteného**,

(b) **Dohodu o mimosúdnom vyrovnaní**, ktorá je uzatvorená **Spoločnosťou** na základe písomného súhlasu **Poisťovne** z dôvodu konania alebo opomenutia alebo porušenia povinností na strane **Poisteného**.
Pokiaľ nie je v týchto **VPP** uvedené alebo v **Poistnej zmluve** výslovne dohodnuté inak, **Škoda** nezahŕňa a toto **Poistenie** nekryje žiadne:

i. dane;
ii. čiastky nad rámec náhrady škody, vrátane, ale nie výlučne, peňažných trestov alebo zmluvných pokút;
iii. pokuty a penále, okrem pokút za porušenie ochrany osobných údajov;
iv. náklady a výdavky spojené so splnením akéhokoľvek príkazu, rozhodnutia alebo dohody o poskytnutí neodkladného opatrenia alebo inej nepeňažnej náhrady alebo nepeňažného plnenia;
v. odmenu, iné požitky, interné alebo režijné náklady, poplatky alebo výdavky **Poisteného** ani náklady za stratený čas **Poisteného**; a
vi. iné položky, ktoré môžu byť nepoistiteľné podľa právneho poriadku, ktorým sa spravuje **Poistná zmluva** alebo právneho poriadku štátu, v ktorom je vznesený nárok.

3.39 **Tretia osoba**
znamená akúkoľvek právnickú alebo fyzickú osoba, nezahŕňa však

i. **Poisteného (**s výnimkou zamestnancov **Spoločnosti** v prípade ak vystupujú v pozícii **Dotknutej osoby)**; alebo
ii. akúkoľvek inú právnickú alebo fyzickú osobu, ktorá má významný finančný alebo riadiaci podiel na činnosti **Spoločnosti**

3.40 **Výzva dozorného orgánu**
znamená výzvu **Dozorného orgánu,** v ktorej požaduje od **Spoločnosti**, aby v uvedenej lehote:
(a) preukázala súlad s príslušnými **Príslušným právnym predpisom o ochrane osobných údajov;**
(b) vykonala potrebné opatrenia pre zaistenie súladu s príslušnými **Príslušným právnym predpisom o ochrane osobných údajov**;
(c) sa zdržala akéhokoľvek spracúvania určitých **Osobných údajov** alebo **Dát tretích osôb**.

3.41 **Zamestnanec** znamená akúkoľvek fyzickú osobu, ktorá je zamestnaná na dobu neurčitú na základe pracovnej zmluvy so **Spoločnosťou.**
Zamestnancom nie je**:**

a. riaditeľ **Spoločnosti,** člen štatutárneho orgánu alebo spoločník; alebo
b. osoba, ktorá je zamestnaná na dobu určitú, samostatne zárobkovo činná osoba alebo **Subdodávateľ.**

3.42 **Zamestnanec zodpovedný za compliance (dodržiavanie právnych predpisov)**
znamená vedúceho zamestnanca **Spoločnosti**:
(a) povereného implementáciou predpisov týkajúcich sa ochrany **Osobných údajov** a iných dát vrátane kontroly takejto implementácie, zavádzania príslušných interných predpisov a postupov a plnenia oznamovacej povinnosti súvisiacej so spracúvaním **Osobných údajov** a iných dát;
(b) povereného riadením súladu konania **Spoločnosti** s verejnoprávnymi predpismi;
(c) vo funkcii vedúceho právneho oddelenia **Spoločnosti**.

3.43 **Žiadosť dotknutej osoby**
znamená požiadavku **Dotknutej osoby** v písomnej forme voči **Spoločnosti** týkajúcu sa povinného sprístupnenia:
(a) **Osobných údajov**, prípadne kategórií dotknutých **Osobných údajov**, týkajúcich sa **Dotknutej osoby**, pokiaľ z ich povahy vyplýva, že môžu byť priradené konkrétnym osobám;
(b) Dôvodu a účelu, prečo sú takéto **Osobné údaje** zhromažďované alebo spracúvané;
(c) príjemcov alebo kategórie príjemcov, ktorým v minulosti boli alebo v budúcnosti môžu byť také **Osobné údaje** sprístupnené;
(d) zdroj / zdroje takých **Osobných údajov**;
(e) predpokladaná doba uchovávania **Osobných údajov**, alebo ak to nie je možné, kritéria na jej určenie;
(f) existenciu automatizovaného rozhodovania vrátane profilovania.

4. Výluky z Poistenia

Poisťovňa neposkytne poistné plnenie za **Stratu** vyplývajúcu z alebo inak súvisiacu s/so:

4.1. **Konaním proti hospodárskej súťaži**
t.j. akýkoľvek skutočné alebo údajné konanie proti hospodárskej súťaži alebo právnym predpisom na ochranu proti nekalej súťaži. Táto výluka sa však nevzťahuje na poistné udalosti kryté podľa odseku D.1 (e) vyššie, za podmienky, že toto **Doplnkové poistenie** bolo dojednané;

4.2. **Škodou na zdraví alebo majetku**
t.j. akákoľvek:
(a) **Škoda na zdraví**, ktorá znamená telesnú ujmu, ochorenie, chorobu alebo smrť; a pokiaľ bolo spôsobené uvedeným aj nervový šok, emocionálne rozrušenie, duševné muky alebo mentálnu ujmu, okrem duševných múk a mentálnej ujmy z dôvodu porušenia **Príslušného právneho predpisu o ochrane osobných údajov Spoločnosťou**; alebo

(b) **Škoda na majetku**, ktorá znamená stratu alebo zničenie hmotného majetku, iného ako **Osobných údajov**, prípadne stratu práva ho užívať alebo s odcudzením alebo stratou **IT/technického vybavenia Spoločnosti**;

4.3. **Zmluvnou povinnosťou k náhrade ujmy / zmluvnými zárukami**
t.j. akákoľvek záruka alebo zodpovednosť prevzatá alebo prijatá **Poisteným** podľa akejkoľvek zmluvy alebo dohody, okrem prípadu, že by takáto zodpovednosť bola **Poistenému** pripísateľná v prípade absencie takejto zmluvy alebo dohody;

4.4. **Trestnými činmi**
t.j. akékoľvek:
(a) úmyselné nesplnenie akejkoľvek povinnosti stanovenej rozhodnutím súdu, poroty alebo iného oficiálneho tribunálu alebo senátu alebo iného orgánu vrátane **Dozorného orgánu** alebo iného regulátora;
(b) úmyselné spáchanie, účasť na alebo schvaľovanie;
(c) nečestný, zlomyseľné alebo podvodný čin; alebo
(d) trestný čin (zločin alebo prečin, aj nedbanlivostný);
ak sa vyššie uvedeného dopustili:
i. riaditeľ, štatutárny orgán **Spoločnosti** alebo jej člen, spoločník **Spoločnosti** alebo **Zamestnanec zodpovedný za compliance (dodržiavanie právnych predpisov)** alebo zástupca **Spoločnosti** na základe plnej moci; alebo
ii. **Zamestnanec** alebo **Subdodávateľ** konajúci v zhode s ktorýmkoľvek riaditeľom, **Zamestnancom** zodpovedným za dodržiavanie právnych predpisov, zodpovednou osobou alebo vedúcim právneho oddelenia **Spoločnosti**.
V takom prípade je **Poistník** povinný odškodniť **Poisťovňu** za celú **stratu** vyplatenú v súvislosti s takýmto **nárokom**.

4.5. **Rizikovými dátami**
t.j. akékoľvek dáta, ktoré sa v kvalite, citlivosti alebo hodnote podstatným spôsobom líšia od dát uvedených v dotazníku, alebo o ktorých zhromažďovaní alebo spracúvaní **Poistený Poisťovňu** informoval pred vznikom tohto **Poistenia**;

4.6. **Duševným vlastníctvom**
t.j. akékoľvek porušenie licenčných, patentových alebo iných práv duševného vlastníctva, porušenia obchodného tajomstva alebo zbavenia práv k prihláseniu alebo registrácii patentu alebo iného práva duševného vlastníctva v dôsledku neoprávneného zverejnenia.
Táto výluka sa ale nevzťahuje na Poistné udalosti podľa článku A.2 vyššie;

4.7. **Úmyselným konaním**
t.j. akékoľvek úmyselné alebo vedome nedbalé konanie fyzickej osoby, ktorá je alebo bola štatutárnym orgánom, členom štatutárneho orgánu alebo dozorného orgánu **Spoločnosti**, spoločníkom alebo prokuristom **Spoločnosti** alebo **Zamestnancom zodpovedným za compliance (dodržiavanie právnych predpisov),** vedúcim právneho oddelenia **Spoločnosti** alebo iným členom vedenia **Spoločnosti**, pokiaľ bolo možné rozumne predpokladať, že svojim konaním môže spôsobiť vznik **Nároku** voči **Poistenému**;

4.8. **Licenčnými poplatkami**
t.j. akékoľvek skutočné alebo údajné záväzky k uhradeniu licenčných poplatkov;

4.9. **Predchádzajúcimi nárokmi a známymi skutočnosťami / pochybeniami**
t.j. Nárokom alebo **Nárokmi** uskutočnenými alebo hroziacimi pred uzavretím **Poistnej zmluvy** alebo vyplývajúcich z, založených na alebo pripísateľných akejkoľvek skutočnosti, ktorá bola **Poistenému** známa pred uzavretím **Poistnej zmluvy** a **Poistený** mohol rozumne očakávať, že táto skutočnosť môže odôvodniť vznik **Nároku**;

4.10. **Nárokmi týkajúcimi sa cenných papierov**
t.j. Nárokom alebo **Nárokmi** vyplývajúcimi z, založené na alebo pripínateľné skutočnému alebo údajnému porušeniu akéhokoľvek právneho predpisu alebo pravidla vzťahujúcemu sa na vlastníctvo, nákup, predaj, ponuku alebo výzvu na ponuku nákupu alebo predaja cenných papierov;

4.11. **Štrajkom/Terorizmom/vojnou**
t.j. Nárokom alebo **Nárokmi** vyplývajúcimi z, založené na alebo pripísateľné akejkoľvek vojne (vyhlásenej alebo inej), terorizmu, vojnovej, vojenskej, teroristickej alebo partizánskej činnosti, sabotáži, použitiu vojenskej sily, nepriateľskému činu (vyhlásenému alebo nevyhlásenému), rebélii, revolúcii, občianskym nepokojom, vzbure, násilnému prevzatiu moci, konfiškácii, znárodneniu alebo zničeniu alebo poškodeniu majetku v dôsledku príkazu akéhokoľvek štátneho, verejného alebo miestneho orgánu alebo inej politickej alebo teroristickej organizácie; týmto nie je vylúčený **Nárok** pri skutočnom, údajnom alebo hroziacom **Kybernetickom terorizme.**

4.12. **Obchodnou stratou**
t.j. akákoľvek strata alebo záväzok súvisiaci s podnikaním na kapitálovom trhu; finančná hodnota elektronických prevodov finančných prostriedkov alebo transakcia uskutočnená **Poisteným**, v jeho mene alebo na jeho účet, pokiaľ príde ku strate, poškodeniu alebo zníženiu hodnoty počas prevodu z účtu, na účet alebo medzi účtami; alebo nominálnou hodnotou kupónov, zliav, cien, ocenenia alebo iného oceniteľného plnenia poskytnutého nad rámec celkovej zmluvnej alebo predpokladanej čiastky;

4.13. **Neoprávneným podnikaním na kapitálovom trhu**
t.j. akékoľvek skutočné alebo údajné podnikanie Poisteného na kapitálovom trhu, pokiaľ v dobe jeho výkonu ide nad rámec:
(a) povolených finančných limitov, alebo

(b) povolených produktov;

4.14. **Neoprávneným zhromažďovaním dát**
t.j. neoprávnené alebo protiprávne zhromažďovanie **Dát tretej osoby Spoločnosťou**;

4.15. **Obchodným oznámením**
t.j. akékoľvek zasielanie nevyžiadanej elektronickej pošty vrátane obchodných oznámení, pošty, faxov, telegramov, audio alebo video nahrávok a telemarketingom alebo iným direct marketingom;

4.16. **Nepoistiteľnou stratou**
t.j. akýkoľvek **Nárok,** ktorý je alebo mal byť poistený príslušným povinným alebo zákonným poistením, alebo ktorý je alebo mal byť kryté inou ochrannou schémou, ochranným alebo garančným fondom, alebo iným obdobným inštitútom na základe **Príslušného právneho predpisu o ochranne osobných údajov** resp. akýkoľvek **Nárok** alebo udalosť, ktorá je nepoistiteľná podľa práva Slovenskej republiky, alebo iného právneho predpisu, na základe ktorého je vznesený **Nárok** alebo ktorým sa riadi iná škodová udalosť podľa týchto **VPP**;

4.17. **Nárokmi zo Spojených štátov amerických, tzv. R.I.C.O.**
t.j. Nárokom vyplývajúcim z, založeným na alebo pripísateľným skutočnému alebo údajnému porušeniu zákona o kontrole organizovaného zločinu prijatého v Spojených štátoch amerických v roku 1970 – „United States Organized Crime Control Act of 1970", známeho aj ako „Racketeer Influenced And Corrupt Organizations Act" alebo „R.I.C.O." – v znení neskorších predpisov a akéhokoľvek obdobného právneho predpisu. Táto výluka sa aplikuje výlučne vo vzťahu k **Nároku zo Spojených štátov amerických**.

5. Oznámenie nárokov

5.1. **Oznámenie nárokov a skutočností**
Toto **Poistenie** sa vzťahuje len na **Straty** vzniknuté v dôsledku vznesenia **Nároku** za podmienky, že:
(a) k akémukoľvek konaniu alebo pochybeniu zo strany **Poisteného**, ktorého následkom vznikne **Poistná udalosť** krytá týmito **VPP**, dôjde po **Retroaktívnom dátume** a najneskôr v posledný deň **Poistnej doby**;
(b) **Nárok** bol po prvýkrát vznesený proti **Poistenému** počas **Poistnej doby** a/alebo počas **Rozšírenej doby na ohlasovanie nároku** v zmysle odseku 5.5 nižšie;
(c) k akýmkoľvek **Neoprávneným prístupom do systému**, porušeniam **Príslušného právneho predpisu o ochrane osobných údajov**, **Mediálne významným udalostiam**, **Vydieraniu** alebo **Prerušeniam prevádzky siete** dôjde počas **Poistnej doby**;
(d) akékoľvek **Konanie dozorného orgánu** / regulátora je zahájené počas **Poistnej doby** a **Sankcie uložené dozorným orgánom** sú uložené v **Konaní dozorného orgánu** počas **Poistnej doby**;
(e) všetky skutočnosti uvedené v bodoch (a) až (d) vyššie budú oznámené **Poisťovni** bez zbytočného odkladu po ich zistení, najneskôr však v posledný deň **Rozšírenej doby na ohlasovanie nároku**.
Ak počas **Poistnej doby** dôjde ku skutočnosti, konaniu alebo pochybeniu, pri ktorých možno rozumne očakávať, že budú príčinou **Poistnej udalosti** podľa týchto **VPP** (t.j. **Nároku**, **Konania dozorného orgánu** / regulátora, **Neoprávneného prístupu do systému,** porušeniu **Príslušného právneho predpisu o ochrane osobných údajov**, **Mediálne významnej udalosti**, **Vydierania** alebo **Prerušenia prevádzky siete**), je **Poistený** povinný takéto skutočnosti, konanie alebo pochybenie neodkladne v písomnej forme oznámiť **Poisťovni**.
Takéto oznámenie musí byť podrobné, chronologické a musí obsahovať aspoň tieto informácie:
(a) popis a povaha relevantných skutočností;
(b) identifikáciu skutočných, predpokladaných alebo údajných porušení povinnosti;
(c) deň, čas a miesto skutočných, predpokladaných alebo údajných relevantných skutočností;
(d) osoby, ktoré si v tejto súvislosti môžu potenciálne uplatniť **Nárok** a iné dotknuté osoby;
(e) odhad možnej **Straty**;
(f) potenciálne mediálne dopady a dopady v oblasti dozoru.

5.2. **Súvisiace nároky**
Pokiaľ **Poistený** podá riadne oznámenie podľa predchádzajúceho odseku 5.1., potom:
(a) akýkoľvek nadväzujúci **Nárok**, **Konanie dozorného orgánu, Neoprávnený prístup do systému,** porušenie **Príslušného právneho predpisu o ochrane osobných údajov**, **Mediálne významná udalosť**, **Vydieranie** alebo **Prerušenie prevádzky siete** vyplývajúce alebo inak súvisiace so skutočnosťou takto oznámenou **Poisťovni**; a
(b) akýkoľvek nadväzujúci **Nárok**, **Konanie dozorného orgánu, Neoprávnený prístup do systému,** porušenie **Príslušného predpisu o ochrane osobných údajov**, **Mediálne významná udalosť**, **Vydieranie** alebo **Prerušenie prevádzky siete** vyplývajúce alebo inak súvisiace s možnými **Stratami** takto oznámenými **Poisťovni**,
bude považovaný za prvýkrát uplatnený voči **Poistenému** a oznámený **Poisťovni** v momente, kedy **Poisťovňa** obdržala oznámenie podľa predchádzajúceho odseku 5.1.
Akýkoľvek **Nárok**, **Konanie dozorného orgánu, Neoprávnený prístup do systému,** porušenie **Príslušného právneho predpisu o ochrane osobných údajov**, **Mediálne významná udalosť**, **Vydieranie** alebo **Prerušenie prevádzky siete** vyplývajúce alebo inak súvisiace s:
(a) rovnakou príčinou;

(b) totožnou **Stratou**; alebo
(c) radom nepretržitých, opakujúcich sa alebo inak súvisiacich príčin, alebo strát;
bude pre účely tohto **Poistenia** považovaný za jeden **Nárok**, **Konanie dozorného orgánu, Neoprávnený prístup do systému,** porušenie **Príslušného právneho predpisu o ochrane osobných údajov**, **Mediálne významná udalosť**, alebo **Prerušenie prevádzky siete**.

5.3. **Adresa na oznamovanie Poisťovni:**
Akékoľvek oznámenie, ktoré musí byť podľa týchto **VPP** uskutočnené v písomnej forme, bude **Poisťovni** zasielané na: Colonnade Insurance S.A., pobočka Poisťovne z iného členského štátu so sídlom Moldavská cesta 8 B, 042 80 Košice, Slovenská republika.

5.4. **Podvodne uplatnené nároky a nesprávne informácie**
Pokiaľ **Poistník** alebo **Poistený** poskytnú **Poisťovni** pred uzatvorením **Poistnej zmluvy**, pri jej zmene alebo v súvislosti s uplatnením nároku na **Poistné plnenie** z tohto **Poistenia** nesprávne, neúplné alebo zavádzajúce informácie alebo podstatné informácie týkajúce sa **Poistenia** zamlčia, je **Poisťovňa**, za predpokladu, že by pri pravdivom a úplnom zodpovedaní otázok **Poistnú zmluvu neuzavrela**, oprávnená odstúpiť od **Poistnej zmluvy**. **Poisťovňa** je tiež oprávnená plnenie z **Poistnej zmluvy** primerane znížiť, ak na základe vedome nepravdivej alebo neúplnej odpovede **Poistníka** a/alebo **Poisteného** bolo určené nižšie **Poistné**, a to v takom rozsahu, aký vplyv malo predmetné poskytnutie nesprávnych, neúplných alebo zavádzajúcich informácií alebo zamlčanie podstatných informácií na rozsah povinnosti **Poisťovne** plniť. V takomto prípade môže **Poisťovňa** ďalej žiadať vrátenie akéhokoľvek plnenia, ktoré už z tohto **Poistenia Poistenému** poskytla, avšak nie je povinná vrátiť **Poistníkovi** akékoľvek ním uhradené **Poistné**.

5.5. **Rozšírená doba na ohlasovanie nároku**
V prípade, že dôjde k zániku **Poistnej zmluvy** z iného dôvodu ako pre nezaplatenie **Poistného**, **Poistník** má právo bez akéhokoľvek dodatočného **Poistného** v lehote tridsať (30) dní od zániku **Poistnej zmluvy** oznámiť akýkoľvek **Nárok** krytý týmto **Poistením**, ktorý bol prvýkrát vznesený voči **Poistenému** v takejto lehote. **Rozšírená doba na ohlasovanie nároku** nepredlžuje **Poistnú dobu**, nemení rozsah poistného krytia ani dohodnuté **Limity poistného plnenia**. Vzťahuje sa iba na **Straty**, ku ktorým došlo počas **Poistnej doby, ktoré však boli voči Poistenému prvýkrát uplatnené po skončení Poistnej doby**. Právo z **Rozšírenej doby na ohlasovanie nároku** zaniká, ak je **Poistná zmluva** alebo poistenie obnovené alebo nahradené.

6. Právna ochrana a likvidácia nároku

6.1. **Právna ochrana**
Poisťovňa nemá povinnosť zabezpečiť právne zastúpenie pri akomkoľvek **Nároku** a **Poistený** je povinný využiť všetky dostupné prostriedky právnej ochrany proti vznesenému **Nároku**. **Poisťovňa** môže podľa svojho uváženia, prevziať právne zastúpenie a mimosúdne vyrovnanie v súvislosti s **Nárokom**, čo písomne oznámi **Poistenému**. V prípade, že **Poisťovňa** nevyužije toto právo, je oprávnená, nie však povinná, participovať v plnom rozsahu na právnej ochrane a rokovaní o akomkoľvek mimosúdnom vyrovnaní, ktoré sa dotýka **Poisťovne**, alebo sa takým odôvodnene javí, pričom **Poistený** je povinný poskytovať **Poisťovni** všetky súvisiace informácie. **Poistený** je povinný počínať si tak, aby obmedzil, odvrátil alebo zabránil vzniku **Škody**. **Súhlas Poisťovne**
Poisťovňa poskytne **Poistné plnenie** výlučne za podmienky, že **Poistený** neurobí bez predchádzajúceho písomného súhlasu **Poisťovne** žiadny úkon, ktorým by uznal svoju povinnosť na náhradu **Škody** alebo urobil akékoľvek rozhodnutie alebo otázku nespornou. Rovnako **Poisťovňa** neposkytne **Poistné plnenie**, ak **Poistený** uzná alebo uzatvorí zmier o akomkoľvek **Nároku**, vrátane nároku na náhradu nákladov, alebo ak príjme/uzná náklady vrátane **Nákladov právneho zastúpenia** a **Nákladov na odborné služby** bez predchádzajúceho písomného súhlasu **Poisťovne**.
Iba **Poisťovňou** vopred písomne odsúhlasené vyrovnania, zmiery alebo iné zmierne riešenia sporu, rozhodnutia alebo náklady vrátane **Nákladov právneho zastúpenia** a **Nákladov na odborné služby**, budú uhradené ako **Poistné plnenie**. **Poisťovňa** nemôže tento svoj súhlas bezdôvodne odoprieť, pokiaľ **Poistený** umožnil **Poisťovni**, aby sa zúčastnila obrany proti **Nároku** a akéhokoľvek vyjednávania súvisiaceho s **Nárokom a Poistený** splní svoje povinnosti v zmysle **Poistnej zmluvy** a týchto **VPP**.
Ak predtým, ako je možné získať v primeranom čase predchádzajúci písomný súhlas **Poisťovne**, vzniknú **Náklady na odborné služby** (Náklady definované v časti C týchto všeobecných poistných podmienok), potom **Poisťovňa** poskytne dodatočné schválenie takýchto primeraných a nevyhnutných nákladov až do výšky 10% príslušných sublimitov definovaných poistnou zmluvou. Tieto **Náklady na odborné služby** budú uhradené najskôr odo dňa doručenia oznámenia **Poisťovni** v súlade s článkom 5.1.
Splnenie akejkoľvek oznamovacej povinnosti podľa **Príslušného právneho predpisu o ochrane osobných údajov**, pokiaľ ide o ich skutočné alebo údajné porušenie, sa však pre účely tohto článku nepovažuje za uznanie povinnosti k úhrade ujmy.

COLONNADE
A FAIRFAX COMPANY

6.2. **Zmierlivé riešenie sporu**
Poistený je povinný na základe písomnej inštrukcie od **Poisťovne** uzavrieť dohodu o vyrovnaní, zmier alebo inak zmierlivo vyriešiť spor ohľadne akéhokoľvek **Nároku**. Ak **Poistený** nebude súhlasiť s takýmto mimosúdnym vyrovnaním, zodpovednosť / plnenie **Poisťovne** bude obmedzená / obmedzené len do výšky plnenia, ktoré by **Poisťovňa** bola povinná zaplatiť pri navrhovanom vyrovnaní, vrátane **Nákladov právneho zastúpenia**, ktoré vznikli do momentu, kedy bol návrh takého vyrovnania písomne predložený **Poistenému** (pri zohľadnení príslušnej **Spoluúčasti**).

6.3. **Prechod práv a povinností**
V prípade, že **Poisťovňa** odškodní akýkoľvek **Nárok** krytý **Poistnou zmluvou** za alebo v mene **Poisteného**, prechádzajú na **Poisťovňu** všetky práva na náhradu **Škody** alebo iné obdobné práva, ktoré **Poistenému** v súvislosti s jeho zodpovednosťou za škodu vznikli voči inému. **Poistený** sa zaväzuje pravdivo a úplne informovať **Poisťovňu** o všetkých jeho právach v súvislosti so vzneseným **Nárokom**, predložiť všetky doklady a podklady, ktoré by umožnili **Poisťovni** viesť konanie o náhrade **Škody** vo svojom mene alebo v mene **Poistených** a poskytnúť **Poisťovni** všetku potrebnú súčinnosť a spoluprácu, vrátane podpísania všetkých potrebných dokumentov a listín. **Poistený** nemá právo vzdať sa akéhokoľvek **Nároku**, alebo obmedziť svoj **Nárok**, týkajúci sa ich práv na náhradu **Škody** alebo iných obdobných práv bez súhlasu **Poisťovne**. **Poistený** sa tiež zaväzuje nevykonať nič, čo by poškodilo alebo ohrozilo tieto práva alebo ich uplatnenie. Akékoľvek odškodnenie z prechodu práv na **Poisťovňu**, ktoré by presiahlo výšku **Poistného plnenia** na základe vzneseného **Nároku** krytého **Poistným plnením** vyplateným **Poisťovňou** bude prevedené na **Poisteného** znížené o náklady, ktoré vznikli **Poisťovni** v súvislosti so získaním takéhoto odškodnenia.

7. Limit poistného plnenia a spoluúčasť

7.1. **Limit poistného plnenia**
Súhrn všetkých vyplatených **Poistných plnení** vrátane všetkých limitov plnenia a dodatočných krytí nesmie presiahnuť celkový **Limit poistného plnenia** dojednaný v **Poistnej zmluve**.
Využitie **Rozšírenej doby na ohlasovanie nároku** nezvyšuje celkový **Limit poistného plnenia** dojednaný v **Poistnej zmluve**.
Akékoľvek čiastkové limity plnenia uvedené v **Poistnej zmluve** a týchto **VPP** sú maximálnymi čiastkami **Poistného plnenia** pre odškodnenie jednotlivých **Poistných udalostí** a v súhrne nesmú presiahnuť celkový **Limit poistného plnenia** dojednaný v **Poistnej zmluve**.
Všetky čiastkové limity **Poistného plnenia**, vrátane **Nákladov na odborné služby**, **Doplnkových poistení**, **Nákladov právneho zastúpenia** a plnenia za iné krytia podľa tejto **Poistnej zmluvy** sú súčasťou celkového **Limitu poistného plnenia** a žiadny z čiastkových limitov alebo iných takýchto plnení nemôže byť akýmkoľvek spôsobom pokladaný za dodatočnú čiastku **Poistného plnenia** k celkovému **Limitu poistného plnenia**. Skutočnosť, že **Poistnou zmluvou** je krytý viac ako jeden **Poistený** rovnako nezvyšuje celkový **Limit poistného plnenia Poisťovne** podľa **Poistnej zmluvy**.
Pokiaľ nie je právnymi predpismi ustanovené inak, poistné krytie podľa **Poistnej zmluvy** je poskytnuté iba ako krytie nad rámec akéhokoľvek príslušného poistenia zodpovednosti za škodu, samopoistenia alebo iného platného a vymáhateľného poistenia, pokiaľ nebolo takéto iné poistenie uzavreté iba ako špecifické **Doplnkové poistenie** nad **Limit poistného plnenia** podľa **Poistnej zmluvy** a týchto **VPP**. Pokiaľ takéto iné poistenie poskytuje **Poisťovňa** alebo iný člen skupiny, sesterská alebo materská spoločnosť spoločnosti Colonnade Insurance S.A. („Colonnade"), potom maximálna čiastka splatná zo strany Colonnade podľa všetkých takých poistných zmlúv nepresiahne **Limit poistného plnenia** tej poistnej zmluvy, ktorá má najvyšší príslušný **Limit poistného plnenia**. Nič uvedené v **Poistnej zmluve** sa nesmie vykladať tak, že zvyšuje **Limit poistného plnenia** podľa **Poistnej zmluvy**.
V prípade, ak akékoľvek iné poistenie stanoví povinnosť **Poisťovne** viesť obranu proti akémukoľvek **Nároku**, nebudú náklady na takúto obranu uhradené z tohto **Poistenia**.

7.2. **Spoluúčasť**
Poisťovňa uhradí iba čiastku **Straty**, ktorá presahuje výšku **Spoluúčasti** v súvislosti s každou **Poistnou udalosťou** z tohto **Poistenia** (resp. v súvislosti so **Súvisiacimi nárokmi** podľa odseku 5.2 vyššie). **Spoluúčasť** znáša **Poistený** a nie je predmetom **Poistenia**. **Poisťovňa** môže podľa vlastného a výlučného uváženia vopred uhradiť časť predpokladaného **Poistného plnenia** bez úplného alebo čiastočného odpočítania príslušnej **Spoluúčasti**, v takom prípade **Poistení** uhradia bezodkladne po vyčíslení skutočného **Poistného plnenia**, na ktoré budú **Poistení** oprávnení, príslušnú čiastku **Spoluúčasti Poisťovni**. Pokiaľ by sa na jednu **Poistnú udalosť** z tohto **Poistenia** vzťahovala viac ako jedna **Spoluúčasť**, bude v súvislosti s takouto **Poistnou udalosťou** uplatnená najvyššia z takýchto **Spoluúčastí**.

8. Všeobecné dojednania

8.1. **Spolupráca a povinnosť prevencie**
Poistený je povinný na vlastné náklady:

(a) poskytnúť **Poisťovni** všetku rozumne požadovanú súčinnosť a spolupracovať pri právnej ochrane voči akémukoľvek **Nároku**, **Konaniu dozorného orgánu** / regulátora, **Neoprávnenému prístupu do systému,** porušeniu **Príslušných predpisov o ochrane osobných údajov**, **Mediálne významnej udalosti**, **Vydieraniu** alebo **Prerušeniu prevádzky siete** a uplatnení **Nároku** na odškodnenie alebo náhradu **Škody**;
(b) postupovať s náležitou starostlivosťou a uskutočniť všetky rozumné uskutočniteľné kroky, resp. zosúladiť svoje konanie pri uskutočňovaní všetkých rozumne uskutočniteľných krokov na predchádzanie alebo zmiernenie akejkoľvek **Straty** podľa tejto **Poistnej zmluvy**;
(c) poskytnúť **Poisťovni** také informácie a súčinnosť, akú bude **Poisťovňa** rozumne požadovať za účelom prešetrenia akejkoľvek **Straty** alebo určenia rozsahu zodpovednosti **Poisťovne** podľa tejto **Poistnej zmluvy**.

8.2. **Zabezpečenie dát**
Poistený je povinný uskutočniť všetky primerané opatrenia tak, aby úroveň zabezpečenia dát a informácií bola minimálne na úrovni uvedenej v dotazníku odovzdanom / zaslanom **Poisťovni** (alebo o ktorej **Poistený Poisťovňu** inak informoval) pred uzatvorením **Poistnej zmluvy**.
Poistený je ďalej povinný zaistiť, aby všetky zálohovacie systémy a postupy boli minimálne na úrovni uvedenej v dotazníku odovzdanom / zaslanom **Poisťovni** (alebo o ktorej **Poistený Poisťovňu** inak informoval) pred uzatvorením **Poistnej zmluvy** a že schopnosť obnoviť dáta je pravidelne a dostatočne testovaná v pravidelných intervaloch minimálne raz za 6 mesiacov.

8.3. **Embargo / ekonomické sankcie**
Poisťovňa neposkytne poistnú ochranu (poistné krytie) alebo poistné alebo iné plnenie, pokiaľ by poskytnutím takejto ochrany alebo plnenia došlo k porušeniu akéhokoľvek zákona, nariadenia alebo predpisu o sankciách alebo embargách a ktoré by vystavilo **Poisťovňu**, jeho materské spoločnosti alebo konečného užívateľa výhod riziku akéhokoľvek postihu. Toto ustanovenie je nadradené všetkým ostatným ustanoveniam **Poistnej zmluvy**.

8.4. **Informácie poskytnuté Poisťovni**
Poistník a **Poistený** sa zaväzujú pravdivo a úplne informovať **Poisťovňu** o všetkých skutočnostiach, ktoré by mohli mať vplyv na uzatvorenie alebo neuzatvorenie **Poistnej zmluvy**. Neoddeliteľnou súčasťou **Poistnej zmluvy** je vyplnený a podpísaný dotazník spolu so všetkými jeho prílohami a požadovanými informáciami. Pri poskytnutí krytia **Poistenému** sa **Poisťovňa** spoliehala na vyhlásenia a informácie uvedené v dotazníku, spolu s jeho prílohami a ostatnými informáciami poskytnutými **Poistníkom** a **Poisteným**. Rozsah poistného krytia vychádza z týchto vyhlásení, príloh a informácií, ktoré sa považujú za neoddeliteľnú súčasť **Poistnej zmluvy**.

8.5. **Prevod a Prechod práv**
Poistná zmluva a s ňou spojené práva a povinnosti nemôžu byť prevedené **Poistníkom** alebo **Poisteným** na inú osobu bez predchádzajúceho písomného súhlasu **Poisťovne**.
Zánik Poistenia
Poistenie zaniká v súlade s ustanoveniami § 800 a nasl. **Občianskeho zákonníka**. **Poistenie**, pri ktorom je dojednané bežné poistné, zanikne výpoveďou ku koncu poistného obdobia, pričom výpoveď sa musí dať aspoň šesť týždňov pred jeho uplynutím. Poistenie môže vypovedať **Poisťovňa** ako aj **Poistník** do dvoch mesiacov po uzavretí **Poistnej zmluvy**. Výpovedná lehota je osemdenná a výpoveď musí byť urobená písomne doporučenou zásielkou alebo prvou triedou prípadne inou primeranou cestou na adresu druhej strany, tak ako je uvedená v **Poistnej zmluve**. V prípade zániku **Poistenia** má **Poisťovňa Nárok** na čiastku **Poistného** za dobu do zániku **Poistenia**. Pokiaľ zmluvu zruší **Poistník**, ponechá si **Poisťovňa** zvyčajnú alikvotnú časť **Poistného** (zaniknutú časť **Poistného** mínus manipulačný poplatok, s výhradou neexistencie **Nároku** alebo okolnosti v rámci daného roka **Poistenia**). Vrátenie **Poistného** zo strany **Poisťovne** nepredstavuje odkladaciu podmienku účinnosti zániku **Poistenia**, vrátenie **Poistného** však musí byť uskutočnené bez zbytočného odkladu.

8.6. **Platobná neschopnosť**
Ak nie je v týchto **VPP** uvedené inak, platobná neschopnosť, nútená správa, vyhlásenie konkurzu alebo reštrukturalizácie **Poisteného** nezbavujú **Poisťovňu** jej povinností vyplývajúcich z **Poistnej zmluvy**.

8.7. **Definície, množné číslo a nadpisy**
Nadpisy jednotlivých článkov a odsekov sú len informačné, ich účelom je lepšia zrozumiteľnosť týchto **VPP** a nemajú žiadny špecifický význam, ktorý by sa mal použiť pri výklade **Poistnej zmluvy**. Niektoré slová a pojmy používané v týchto **VPP** majú špecifický význam, ktorý je uvedený v definíciách a sú podľa toho v týchto **VPP** používané, ak z kontextu nevyplýva očividne niečo iné. Slová a výrazy v jednotnom čísle zahŕňajú množné číslo a naopak. Pojmy a slová písané tučne a s veľkým začiatočným písmenom majú zvláštny význam definovaný v článku 3 (Definície) vyššie alebo v inej časti týchto **VPP**. Pojmy a slová, ktoré nie sú v týchto **VPP** osobitne definované majú význam, ktorý sa im bežne pripisuje.

8.8. **Teritoriálny rozsah poistného krytia a rozhodné právo**
Pokiaľ je to právne prípustné a s výhradou výluky **„R.I.C.O."** v zmysle týchto **VPP** sa **Poistná zmluva** vzťahuje na **Nárok** vznesený voči ktorémukoľvek **Poistenému** kdekoľvek na svete. Akákoľvek interpretácia a výklad **Poistnej zmluvy**, vrátane otázok jej platnosti alebo účinnosti musí byť v súlade s právnym poriadkom Slovenskej republiky, pričom na rozhodovanie akýchkoľvek sporov z **Poistnej zmluvy** sú príslušné slovenské súdy.

8.9. **Uzatvorenie a platnosť Poistnej zmluvy**

COLONNADE
A FAIRFAX COMPANY

Poistná zmluva sa považuje za uzatvorenú okamihom písomného upovedomenia **Poisťovne** o prijatí návrhu **Poistnej zmluvy** zo strany **Poistníka**, a to v lehote uvedenej v návrhu **Poistnej zmluvy**. Návrh **Poistnej zmluvy** možno prijať tiež zaplatením **Poistného** vo výške, spôsobom a lehote uvedenej v návrhu **Poistnej zmluvy**. **Poistná zmluva** je v takom prípade uzavretá, len čo bolo **Poistné** zaplatené. **Poistná zmluva** nie je platná a účinná, pokiaľ nie je podpísaná štatutárnym orgánom **Poisťovne** alebo jej oprávneným zástupcom.

8.10. Odchýlky

V zmysle § 788 odseku 4 **Občianskeho zákonníka** sa v týchto **VPP** uvádza, že v **Poistnej zmluve** je možné dojednať odchýlku od znenia ktorejkoľvek časti týchto **VPP**.

8.11. Súčasti Poistnej zmluvy

Súčasťou **Poistnej zmluvy** sú okrem týchto **VPP** aj osobitné poistné podmienky / osobitné zmluvné dojednania, poistné doložky alebo iné dojednania dohodnuté medzi **Poisťovňou** a **Poistníkom**, ktoré podrobnejšie špecifikujú podmienky a rozsah poistenia podľa **Poistnej zmluvy** vo vzťahu k niektorým druhom poistného krytia. Ustanovenia osobitných poistných podmienok / osobitných zmluvných dojednaní, poistných doložiek alebo iných dojednaní majú prednosť pred ustanoveniami týchto **VPP**. Neoddeliteľnou súčasťou **Poistnej zmluvy** je tiež **Poistníkom** a/alebo **Poisteným** vyplnený a podpísaný dotazník spolu so všetkými jeho prílohami a požadovanými informáciami.

8.12. Zmena právnych predpisov

V prípade, že počas **Poistnej doby** dôjde k takej zmene alebo nahradeniu **Príslušného právneho predpisu,** ktorá má vplyv na rozsah a podmienky tohto **Poistenia** alebo predstavuje odlišnú úpravu ochrany **Osobných údajov** a **Dôverných informácií**, s akou počíta **Poistná zmluva** a tieto **VPP**, **Poisťovňa** a **Poistník** sa zaväzujú na návrh **Poisťovne** v dobrej viere rokovať o zmene **Poistnej zmluvy** a / alebo **VPP** tak, aby **Poistenie** pri zohľadnení príslušnej zmeny alebo nahradenia **Príslušného právneho predpisu** zabezpečovalo efektívne krytie pre **Poistených** a zároveň zohľadňovalo riziká a oprávnené záujmy **Poisťovne**. Pokiaľ sa **Poisťovňa** a **Poistník** nedohodnú na zmene **Poistnej zmluvy** a / alebo týchto **VPP**, bude pre poistné krytie a práva a povinnosti **Poisťovne**, **Poistníka** a **Poistených** rozhodujúce aktuálne znenie **Poistnej zmluvy** a **VPP**, pričom však:

(a) **Poisťovňa** nebude povinná plniť ani uhradiť nič viac, ako by bola povinná plniť alebo uhradiť za predpokladu, že by k zmene alebo nahradeniu **Príslušného právneho predpisu** nedošlo; a

(b) **Poistník** a **Poistení** nemajú viac práv, ako by mali za predpokladu, že by k zmene alebo nahradeniu **Príslušného právneho predpisu** nedošlo.

8.13. Spôsob vybavovania sťažností

Sťažnosť je možné podať v akejkoľvek prevádzke **Poisťovne** počas prevádzkovej doby osobne alebo písomne na adrese: Colonnade Insurance S.A., pobočka poisťovne z iného členského štátu, Moldavská cesta 8 B, 042 80 Košice. Sťažnosť je možné podať aj elektronicky na e-mailovú adresu: info@colonnade.sk. Podrobnejšie informácie o mieste, spôsobe podania a postupe pri vybavovaní sťažností sú uvedené v dokumente - Vybavovanie sťažností, ktorý sa nachádza na webovom sídle **Poisťovne**. Sťažnosť bude vybavená bez zbytočného odkladu, najneskôr v lehote 30 dní od jej doručenia. V prípade, ak to vzhľadom na okolnosti prípadu nebude možné, bude sťažovateľ informovaný o dôvodoch predĺženia lehoty na vybavenie sťažnosti s uvedením predpokladaného termínu vybavenia sťažnosti.

8.14. Rozhodné právo

Pokiaľ nebolo v **Poistnej zmluve** dohodnuté inak, na poistné zmluvy uzavreté v zmysle týchto **VPP** sa vzťahuje právo Slovenskej republiky. Pre riešenie sporov vzniknutých v súvislosti s poistením sú príslušné súdy Slovenskej republiky.

Tieto **VPP** nadobúdajú účinnosť 01.12.2022.

Munich RE

Cyber Risk Assessment Questionnaire

Endorsement ICS and OT

Version: ME ORACLE 2019 EN ICS OT EN V1 DOCX
Print: 03.07.2020

Introduction

This questionnaire is an endorsement to the Cyber Risk Assessment questionnaire. The answers to the questions are very important to us for assessing the risk in order to provide cyber insurance to you based on the information we receive. Therefore we rely on your statements made in the questionnaire which are the basis for the insurance contract.

The term Industrial control system (ICS) embraces several types of control systems and associated instrumentation is used for industrial process control. Operational Technology (OT) is defined as collection of personnel, hardware and software that can affect or influence the safe, secure and reliable operation of an industrial process. Industrial Security in this context is used to secure Operational Technology.

Please complete this endorsement only if you have ICS and OT.

Are any further information or details regarding your information security enclosed by attachment?

1 Company / applicant information

Name of applicant	Slovenská elektrizačná prenosová sústava, a.s.
Address	Mlynské nivy 59/A, Bratislava 824 84
Country	Slovenská republika
Email	info@sepsas.sk
Phone	02/50692191
Subsidiaries	-
All web domain names (covered by this insurance)	www.sepsas.sk

2 Information Security

The following questions help us to evaluate the maturity of your information security. Please answer all questions and provide evidence where available (e.g. reports, presentations, documents etc.).

1 Do you use a third party organization for production, operation or maintenance?

If yes, please indicate which parts of the production and relevant company name(s).

2 Does your CISO (Chief Information Security Officer) have a direct reporting from production IT?

If yes, please indicate frequency and describe content of such reporting.

3 Does your formal Information Security Policy cover your industrial environment and processes?

4 Do you have a removable media handling policy in place?

5 Do you have a policy for handling suppliers of third party systems (e.g. engineering systems) in place?

6 Do you have industrial out of date/end of life software and/or hardware which is officially not provided with security updates by manufacturer/provider (e.g. Windows XP)?

If yes, please indicate criticality for production and reason for not updating.

7 Do you use restrictive application whitelisting on industrial systems; e.g. on Supervisory Control and Data Acquisition (SCADA) or Human Machine Interface (HMI)?

If not, what do you use?

	Anti-Virus		Anti-Spyware		Equivalent malware protection

8 Do you timely patch your industrial systems and applications after publication of a release?

If yes, how often?

	Within a day		Within a week		Within a month		At a longer time period

9 Do you test updates and upgrades of firmware, software, web-applications and products of your industrial systems before deployment?

10 Do you perform regular, automatic backups of industrial systems' firmware, operating systems, applications, licenses and configuration data sets?

11 Are roll-backs of backups of industrial systems regularly tested to validate the accuracy and integrity of the data and to verify the ability to restore data as quickly as possible with the least impact?

12 Do you or any supplier of third-party systems (e.g. for remote maintenance access) have local internet breakouts in your OT environment (modem, wireless, mobile network access)?

13 Are the office-IT- and OT-networks separated?

If yes, please describe the technology and IT architecture and attach an overview.

14 Are communication paths and data flows for the OT-environment documented?

15 Do you use industrial wireless technologies (e.g. WirelessHART, Bluetooth) with enabled access control and encryption features in dedicated networks?

16 Do you provide remote access to your industrial systems/networks?

17 Do you have a four eyes principle for industrial systems' remote access?

If yes, please describe your process and attach a description of the setup.

18 Do you check the security status of remote login systems?

19 Do you have a passive approach for your industrial systems regarding vulnerability scans?

If yes, please describe your approach and attach a description.

20 Do you provide at least yearly awareness training which covers industrial IT security and which is designed for blue collar worker?

3 Additional Comments

Would you like to share further information or details regarding your ICS and OT security?

Munich RE

Cyber Risk Assessment Questionnaire

Version MR CRAQUE 2019 WLP LARGE EN V1 WLP-7 COVER.DOCX
Print 9 February 2023

Introduction

This questionnaire is designed to provide us with a comprehensive view of the effectiveness and maturity of information and data security within your company. The answers to the questions are very important to us for assessing the risk in order to provide cyber insurance to you based on the information we receive. Therefore we rely on your statements made in the questionnaire which are the basis for the insurance contract. Considering this, someone within the company responsible for information security should answer and sign the questionnaire or at least support the person who is answering it by countersigning. If you have no information security resource, then the questionnaire should be completed by a senior representative (owner or board member).

This questionnaire is neither an offering nor binding of an insurance contract (coverage). Furthermore the completion of this questionnaire does not obligate the insurer to offer coverage to you.

Are any further information or details regarding your information security enclosed by attachment?

Currency used for this questionnaire: ☐ USD ☒ EUR ☐ GBP ☐ Other: .....

1 Company / applicant information

Name of applicant	Slovenská elektrizačná prenosová sústava, a. s.
Address	Mlynské nivy 59/A, Bratislava 824 84
Country	Slovenská republika
Email	info@sepsas.sk
Phone	02/50692191
Subsidiaries	-
All web domain names that should be covered by this insurance	https://www.sepsas.sk

1.1 Industrial sector(s)

Please check the industrial sector(s). Details and assignment are available in the annex on page 10.

- ☐ Business & Professional Services
- ☐ Defense / Military Contractor
- ☐ Education
- ☐ Energy
- ☐ Entertainment & Media
- ☐ Financial Services – Banking
- ☐ Financial Services – Insurance
- ☐ Financial Services – Investment management
- ☐ Food & Agriculture
- ☐ Healthcare
- ☐ Information Technology – Hardware
- ☐ Information Technology – Services
- ☐ Information Technology – Software
- ☐ Manufacturing
- ☐ Mining & Primary Industries
- ☐ Pharmaceuticals
- ☐ Public Authority; NGOs; Non-Profit
- ☐ Real Estate, Property & Construction
- ☐ Retail
- ☐ Telecommunications
- ☐ Tourism & Hospitality
- ☐ Transportation/Aviation/Aerospace
- ☐ Utilities
- ☐ Other

For "Other" type of industry, please specify	
Please specify details of your activities	

1.2 Turnover/revenue and regional footprint

	Domestic	USA	European Union	Rest of world
Your turnover / revenue for the last fiscal year				
Your share of turnover/revenue **created online** for the last fiscal year				

	Last year	Year before last	Last but two years
Your gross profit (or equivalent)			

Please state the number of employees				
Please state the (estimated) number of individual IT devices deployed		Server		Desktops
		Laptops		Mobile devices

1.3 Type and quantity of data

Please estimate type and volume of the following categories of sensitive data your company is maintaining/processing to the best of your knowledge.

Type of data	Number of unique records	Number of unique records of US citizens	Number of unique records stored in US data centres
Personally Identifiable Information (PII)			
Payment Card Information (PCI)			
Protectable Health Information (PHI)			
Intellectual property (IP)			

1.4 Requested cyber insurance

Policy period	From		To	-
Aggregate limit requested				
Retroactive date				
Territorial scope of insurance cover				

Cover modules/elements

Please check all cover modules requested.

First party losses	Deductible/SIR for each and every insured event	Sub-limit for each and every insured event and in the aggregate
Incident response		
Restoration		
Business interruption	WP = [.....] hours	
Cyber extortion		
Cyber Crime		
PCI-DSS		

Third party claims	Deductible/SIR for each and every insured event	Sub-limit for each and every insured event and in the aggregate
Confidentiality and privacy liability		
Network security liability		
Media liability		

1.5 Prior cyber insurance

1 Do you currently hold or have ever held cyber insurance providing the same or similar coverage as the insurance sought?

2 Has any insurer ever cancelled or non-renewed a policy that provided the same or similar coverage as the insurance applying for?

1.6 Information Security Events and Loss History

Please answer the following questions by considering any time during the past three years.

1 Have you had any **incidents, claims or suits** involving unauthorized access or misuse of your network, including embezzlement, fraud, theft of proprietary information, breach of personal information, theft or loss of laptops, denial of service, electronic vandalism or sabotage, computer virus or other incident?

2 Have you experienced an **unplanned business interruption** of longer than four hours caused by a cyber incident?

3 Have you experienced an **extortion attempt or demand** with respect to your computer systems?

4 Have you received any **claims or complaints** with respect to allegations of defamation, invasion or injury of privacy, theft of information, breach of information security, transmission of malware, participation in a denial of service attack, request to notify individuals due to an actual or suspected disclosure of personal information?

5 Have you been subject to any **government action, investigation or subpoena** regarding any (alleged) violation of any (privacy) law or regulation?

6 Are you aware of any **release, loss or disclosure of personally identifiable information** in your care, custody or control, or in the control of anyone holding such information on behalf of you?

7 Are you aware of any **actual or alleged fact, circumstance, situation, error or omission, or potential issue** which might give rise to a loss or claim against you under the cyber insurance policy for which you are applying for or any similar insurance presently or previously in effect or currently proposed?

If one question or more of this section 1.6 is answered with "Yes", please attach a description including complete details (cause, costs, notification, time to discover, recovery time and steps taken to mitigate future exposure) of each event (incident, claim etc.).

1. Security incident - theft of a SEPS employee's NTB from the LIDL store parking lot on 13/09/2021. The incident was immediately reported to the police, who initiated criminal prosecution in the matter of the intentional offense Theft according to § 212 par. 1 letter a) of the Criminal Code. On 14.10.2022, the district director of the police force issued a resolution on the suspension of the criminal prosecution, since it was not possible to establish the facts justifying criminal prosecution against a certain person. The device had BITLOCKER installed, which ensured encrypted protection of SEPS information. After the theft, SEPS monitoring did not record any attempts to authenticate this NTB into the SEPS infrastructure.

2. Security incident of disclosure of personal data within SEPS: Incident reported to the helpdesk on 5/30/2022. The subject of the incident was the disclosure of personal data (employee address) in the internal SharePoint application for business travel records. The incident was resolved by the DPO on June 1. 2022 by blocking employee access to this data.

1.7 Frameworks and Standards

Please check all legal frameworks you have to adhere to.

	General Data Protection Regulation (GDPR) of the European Union (EU)		US Federal Privacy Act
	US Health Insurance Portability and Accountability Act (HIPAA) and US Health Information Technology for Economic and Clinical Health (HITECH) Act		

Please check all standards for which you have successfully been audited or hold a valid certificate.

	Payment Card Industry Data Security Standard (PCI DSS)						
	Merchant level 1		Merchant level 2		Merchant level 3		Merchant level 4

	Critical Security Controls		Other
	COBIT 5 (Control Objectives for Information and Related Technologies)		Information Security Forum (ISF) The Standard of Good Practice for Information Security 2018

If "Other" standard(s) apply, please specify	
Please describe the scope of the certificate	

2 Information Security

The following questions help us to evaluate the maturity of your information security. Please answer all questions and provide evidence where available (e.g. reports, presentations, documents etc.). The questions are structured according to the clauses of the ISO/IEC 27002 standard. Hence questions focussing on one security objective can appear in different sections of this questionnaire. In order to create a better understanding about why we ask the questions, each section starts with the objective(s) of the ISO security control categories.

2.1 Information security policies

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

1 Have you developed and implemented a formal information security policy which is corporate-wide and permanently available for all employees and relevant external parties?
2 Are your information security policies annually reviewed and approved by senior management?

2.2 Organization of information security

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

1 Have you assigned a responsible person for information security (e.g. Chief Information Security Officer "CISO")?
2 Does your IT security responsible person regularly report to senior management?
3 Do you have an up to date list of authorities and external contacts, which must be informed in case of an information security incident?

2.3 Human resource security

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. To ensure that employees and contractors are aware of and fulfil their information security responsibilities. To protect the organization's interests as part of the process of changing or terminating employment.

1 Do you provide at least annual education to increase your users (employees and contractors) security awareness and to prepare users to be more resilient and vigilant against phishing?
2 Do you monitor and report to management on security awareness trainings?
3 Have you identified roles (e.g. privileged users, admins, executives) which need tailored security awareness training?

2.4 Asset management

Objective: To identify organizational assets and define appropriate protection responsibilities. To ensure that information receives an appropriate level of protection in accordance with its importance to the organization. To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

1 Do you keep an up-to-date inventory of software (incl. operating systems) and hardware assets in your network?
2 Do you have a comprehensive Configuration Management Database (CMDB) including: all IT assets, public cloud assets, dependencies, criticality, ownership, software and patch versions?
3 Do you use a Mobile Device Management (MDM) solution for all laptops and smartphones?
4 Do you classify information with regards to confidentiality?
5 Do you classify information with regards to integrity and availability requirements?
6 Are Information labelling procedures implemented in accordance with the above classification scheme?

7 Have you technically enforced the information classification scheme?
8 Do you provide guidance how to handle classified information?
9 Is the handling of information reviewed on a regular basis in order to ensure consistency with its classification?
10 Do you either restrict access to or encrypt confidential information stored on removable media like external storage devices (e.g. USB sticks or hard disks)?
11 Is an authorization required for media removed from the organization and is a record of such removals kept in order to maintain an audit trail?
12 Are media ports (e.g. USB) managed centrally or generally deactivated?
13 Do you securely dispose media containing sensitive information if it is not used any longer?
14 Do you enforce guidelines that the content - if no longer required - of any re-usable media that can be removed from the organization are made unrecoverable?

2.5 Access control

Objective: To limit access to information and information processing facilities. To ensure authorized user access and to prevent unauthorized access to systems and services. To make users accountable for safeguarding their authentication information. To prevent unauthorized access to systems and applications.

1 Do you restrict employees' and external users' privileges on a business-need to know basis (particularly administrative permissions and access to sensitive data e.g. personal data)?
2 Have you enforced multi-factor authentication for remote access?
3 Do you have a formal access provisioning process in place for assigning and revoking access rights?
4 Do you have implemented a central Identity and Access Management ("IAM") system for assigning and revoking access rights?
5 Does the data owner at least annually review access rights?
6 Do you prohibit local admin rights on workstations for users?
7 Do you use Privileged Identity and Account Management ("PIM", "PAM")?
8 Do you review user access rights at least annually?
9 Do you review shared accounts (e.g. used for high-privileged systems/applications) at least annually?
10 Do you review authorizations for privileged access rights intervalic at least on a bi-annual basis?
11 Do you revoke all system access, accounts and associated rights after termination of users (incl. employees, temporary employees, contractors or vendors)?
12 Do you have a process to remove unneeded user rights after organizational role changes?
13 Have you implemented a password policy enforcing the use of long and complex passwords across your organisation? Long and complex passwords are defined as: eight characters or more; not consisting of words included in dictionaries; free of consecutive identical, all-numeric or all-alphabetic characters.
14 Have you changed all default passwords on all your connected devices (e.g. router, Internet of Things)?
15 Do you provide an approved password manager for all your users?

2.6 Cryptography

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

1 Is all confidential information stored on mobile devices (e.g. smart phones and laptops) encrypted?

2 Do you encrypt sensitive data and confidential information that is stored in databases and file servers?
3 Have you developed and implemented a policy on the use, protection and lifetime of cryptographic keys?
4 Is your policy on cryptographic keys regularly reviewed and updated through their whole lifecycle?

2.7 Physical and environmental security

Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities. To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

1 Do you maintain a list of personnel (employees, vendors and visitors) with authorized access to your premises and sensitive security areas?
2 Have you installed advanced entry controls (e.g. biometric access control, mantraps)?
3 Have you installed advanced entry monitoring controls (e.g. 24-7 closed-circuit television (CCTV), documentation of every access)?

2.8 Operations security

Objective: To ensure correct and secure operations of information processing facilities. To ensure that information and information processing facilities are protected against malware. To protect against loss of data. To record events and generate evidence. To ensure the integrity of operational systems. To prevent exploitation of technical vulnerabilities. To minimise the impact of audit activities on operational systems.

1 Have you implemented change management procedures for critical systems?
2 Do your change management processes include testing, failback scenarios and reporting?
3 Does your decision to change the IT environment always consider requirements of business processes?
4 Is the IT-environment for development and testing separated from production IT-environment?
5 Do your developers use different accounts for development, testing and day-to-day tasks?
6 Do you use malware protection for all web-proxies, email-gateways, workstations and laptops?
7 Are updates of anti-malware signature files downloaded and installed automatically?
8 Besides traditional signature-based detection, does your malware protection use advanced heuristic- and behavioural-based detection mechanisms to protect against new malware?
9 Do you perform at least weekly regular backups of business critical data?
10 Do you store backups physically separated from your network (e.g. outside the office premises)?
11 Do you regularly ensure that data backups are complete and can be restored as quickly as possible with minimal impact to business?
12 Do you produce and regularly review event logs recording user activities, exceptions, faults and information security events (at least from your firewalls and domain controller)?
13 Do you have a Security Information and Event Management (SIEM) system in place including rules for generating reports and alerts on system security?
14 Have you implemented a centralized software installation process?
15 Do you apply a strict configuration management approach and develop secure images that are used to build all newly deployed workstations and servers?
16 Do you timely – at least within one month of release – apply updates to critical IT-systems and applications ("security patching")?

17 Do you timely - at least within one week of release - install security patches on internet-facing IT-systems and applications?
18 Do you regularly perform vulnerability scans, identify the associated risk and take appropriate actions?
19 Do you technically or organisationally ensure that users must not install software on their workstations by themselves?

2.9 Communications security

Objective: To ensure the protection of information in networks and its supporting information processing facilities. To maintain the security of information transferred within an organization and with any external entity.

1 Are all internet access points secured by appropriately configured firewalls?
2 Are all internet access points secured by Next-Generation Firewalls?
3 Have you implemented a Network Access Control ("NAC") technology to access your corporate wireless networks?
4 Do you monitor your network and identify security events?
5 Are you using an Intrusion Detection System (IDS)?
6 Do you have a Security Operations Centre (SOC) monitoring all events on a 24-7 basis?
7 Are all internet-accessible systems (e.g. web-, email-servers) segregated from your trusted network (e.g. within a demilitarized zone (DMZ) or at a 3rd party provider)?
8 Are all high risk network segments (e.g. point of sales (PoS) systems, sensitive data processing, office and operational technology (OT) production networks etc.) segregated?
9 Do you encrypt confidential communication (e.g. secure emails with SMIME (Secure Multipurpose Internet Mail Extensions) or SMTP-over-TLS (Simple Mail Transfer Protocol Secure))?
10 Do you use data loss prevention (DLP) software?

2.10 System acquisition, development and maintenance

Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks. To ensure that information security is designed and implemented within the development lifecycle of information systems. To ensure the protection of data used for testing.

1 Does your web-server encrypt confidential data (e.g. HTTPS)?
2 Do you protect your web-servers against denial of service attacks (e.g. by utilising a content delivery network provider)?
3 Do you test security functionality during the development lifecycle of information systems incl. IT security updates?
4 Do you conduct automated security tests or code analysis during system development?
5 Do you consider confidentiality when using operational data for testing to ensure that all sensitive details are protected by removal or modification?

2.11 Supplier relationships

Objective: To ensure protection of the organization's assets that is accessible by suppliers. To maintain an agreed level of information security and service delivery in line with supplier agreements.

1 Have you identified and documented all your important suppliers (including third party service providers)?
2 Have you identified and mandated information security controls to specifically address supplier access to your information in a policy?
3 Do agreements with third party service providers require levels of security commensurate with your own information security standard?
4 Do you periodically review and update agreements with your important suppliers (including third party service providers)?

5 Do you stipulate the right for third party audits within your contractual agreements?
6 Do you monitor third party service provider activities for security events to maintain an agreed level of information security?
7 Do you conduct audits (information security assessments) of suppliers (including third party service providers) and follow-up on issues identified?
8 Do your written and signed contracts with suppliers (including third party service provider) include a hold harmless agreement or waiver of liability in your favour in case such suppliers fail to safeguard your sensitive data?

2.12 Information security incident management

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

1 Do you have an information security incident response plan in place?
2 Have you appointed a responsible person or team for incident response?
3 Do you annually test your security incident response plan?
4 Do all your employees and third party providers know the reporting line for information security events?
5 Are all employees and contractors aware of their responsibility to report information security events?
6 Do you document all information security events in a central Security Information and Event Management (SIEM) system?
7 Are employees and contractors required to report any identified information security weakness (not yet an incident or event) in systems or services?
8 Do you offer a bug bounty program for reporting bugs, exploits or vulnerabilities?
9 Have you established an escalation procedure for information security incidents?
10 Do you collect evidence for forensic analysis?
11 Do you regularly inform management about past incidents?
12 Do you use knowledge gained from analysing and resolving information security incidents to reduce the likelihood or impact of future incidents?
13 Do you quantify and monitor types, volumes and costs of information security incidents?

2.13 Information security aspects of business continuity management

Objective: Information security continuity should be embedded in the organization's business continuity management systems. To ensure availability of information processing facilities.

1 Have you conducted a Business Impact Analysis (BIA)?
2 Are Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for critical systems and processes defined and documented?
3 Do you have a Business Continuity Management (BCM) plan in place that specifically addresses cyber incidents?
4 Do you have an IT Disaster Recovery (DR) plan in place?
5 Do you have advanced implementation controls for disaster recovery capabilities in place (e.g. full redundancy or automatic failover mechanisms)?
6 Do you test your information security continuity plans (e.g. Business Continuity Management, Disaster Recovery) at least annually?
7 Do you review and update your information security continuity plans (e.g. Business Continuity Management, Disaster Recovery) plans at least annually?
8 Are the results of the continuity test activities reviewed, documented, reported to management and are the plans revised based on lessons learned?

9 Are your information processing facilities (i.e. any system, service or infrastructure, or physical location housing it) implemented with redundancy?

10 Do you regularly - at least annually - conduct redundancy testing to ensure the failover from one component to another component works as intended?

2.14 Compliance

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements. To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

1 Have you implemented a procedure to permanently comply with all privacy relevant legislative statutory, regulatory and contractual requirements?

2 Have you assigned a Compliance Officer?

3 Does your Compliance Officer regularly report to senior management?

4 Do you have guideline issued on the retention, storage, handling and disposal of records and information?

5 Do you have a documented retention schedule to identify records and the period of time for which they should be retained?

6 Have you assigned a responsible person for providing guidance and ensuring awareness of privacy principles (e.g. Data Privacy Officer DPO)?

7 Does your Privacy Officer regularly report to senior management?

8 Do you have a policy for the privacy and protection of personally identifiable information developed and implemented?

9 Do you regularly scan critical systems (incl. penetration tests or vulnerability assessments) - either by yourself or supported by third party - particularly each time new systems are introduced and following changes?

3 Additional Comments and Signature(s)

Would you like to share further information or details regarding your information security?

Herewith, by undersigning this document (must be signed by officer, owner or manager), I confirm that I am a duly authorized representative of the company with sufficient technical skills to provide – to my best knowledge – accurate and comprehensive answers regarding the questions within this questionnaire on behalf of the company. The completed questionnaire and optional attachments are basis for the coverage and will therefore become part of the insurance contract.

Date	Date
Signature	Signature
Name	Name
Position, task	Position, task
Email	Email

Annex 1: Overview – Industrial sectors

Source: Cyber Insurance exposure data schema v1.0 by Cambridge Centre for Risk Studies

Business & Professional Services	Occupations providing specialist business advice and services. Some professional services require holding professional licenses such as architects, auditors, engineers, doctors and lawyers.
Defense / Military Contractor	Defense industry comprises government and commercial industry involved in research, development, production, and service of military materiel, equipment and facilities
Education	Colleges and universities, independent and unified school districts, student loans and tuition companies
Energy	Companies involved in the exploration, extraction and development of oil or gas reserves, oil and gas drilling, or integrated power firms.
Entertainment & Media	Enterprises involved in providing news, information, and entertainment: radio, television, films, theatre
Financial Services – Banking	Companies engaged in commercial banking, savings institutions, credit unions, credit card issuing, sales financing, mortgage and loan companies and brokers, financial transaction processing, reserve and clearinghouse activities, and central banking.
Financial Services – Insurance	Direct insurance carriers, reinsurance carriers, and insurance agencies and brokerages.
Financial Services – Investment management	Companies engaged in investment banking, securities dealing and brokerage, commodity contracts dealing and brokerage, securities and commodity exchanges, investment clubs and venture capital, portfolio management, investment advice, and legal entity funds and trusts
Food & Agriculture	Those involved in the food industry, including production, processing, distribution, and wholesale supply
Healthcare	Companies providing goods and services to treat patients with curative, preventive, rehabilitative, and palliative care.
Information Technology – Hardware	Companies engaged in manufacturing and/or assembling computers (mainframes, personal computers, workstations, laptops, and computer servers) and peripheral equipment (e.g. storage devices, printers, monitors etc.)
Information Technology – Services	Companies providing hosting or data processing services (incl. cloud and streaming services); internet publishing and broadcasting content (incl. social media); internet search portals; services relating to computer systems design, computer facilities management, computer programming services, and computer hardware or software consulting.
Information Technology – Software	Companies involved in the design, development, documentation, and publishing of computer software
Manufacturing	Companies making or process goods, especially in large quantities and by means of industrial machines
Mining & Primary Industries	Companies involved in the mining, quarrying, and processing of extracting minerals, coal, ores, main commodities, and natural resources.
Pharmaceuticals	Pharmaceutical industry develops, produces, and markets drugs or pharmaceuticals for use as medications. Pharmaceutical companies may deal in generic or brand medications and medical devices.
Public Authority; NGOs; Non-Profit	National or local government agencies, non-governmental and non-profit organizations
Real Estate, Property & Construction	Companies managing, developing, and transacting property consisting of land and buildings, along with its natural resources such as crops, minerals, or water
Retail	Retailers to general public, sellers of goods and services both in retail stores and online, wholesalers and distributors.
Telecommunications	Companies facilitating exchange of information over significant distances by electronic means.
Tourism & Hospitality	Companies providing services for tourism, travel, accommodation, catering and hospitality
Transportation/ Aviation/ Aerospace	Companies facilitating the transportation of goods or customers. The transportation sector is made up of airlines, railroads and trucking companies.
Utilities	The utilities sector contains companies such as electric, gas and water firms and integrated providers

Výpis z Obchodného registra Okresného súdu Bratislava I

Oddiel: Sa

Vložka číslo: 2906/B

Obchodné meno:	Slovenská elektrizačná prenosová sústava, a.s.	(od: 21.01.2002)
Sídlo:	Mlynské nivy 59/A Bratislava 824 84	(od: 19.12.2007)
IČO:	35 829 141	(od: 21.01.2002)
Deň zápisu:	21.01.2002	(od: 21.01.2002)
Právna forma:	Akciová spoločnosť	(od: 21.01.2002)
Predmet činnosti:	prenos elektriny	(od: 06.04.2006)
	filtrácia izolačných olejov z výroby a ich úprava v transformátoroch	(od: 21.01.2002)
	poradenská a konzultačná činnosť v oblasti diagnostiky energetického zariadenia	(od: 21.01.2002)
	výkon investorských činností v príprave a realizácii investičnej výstavby	(od: 21.01.2002)
	projektovanie, montáž, vykonávanie revízií, oprava a údržba meracej a regulačnej techniky	(od: 23.02.2011)
	informatívne meranie fyzikálnych veličín	(od: 23.02.2011)
	informatívne chemické a mikrobiologické analýzy	(od: 23.02.2011)
	diagnostika a meranie na energetických zariadeniach okrem vyhradených zariadení	(od: 23.02.2011)
	vykonávanie kalibračnej služby s výnimkou overovania určených výrobkov	(od: 23.02.2011)
	podnikanie v oblasti nakladania s odpadmi inými ako nebezpečnými odpadmi	(od: 23.02.2011)
	kúpa tovaru na účely jeho predaja konečnému spotrebiteľovi (maloobchod) alebo iným prevádzkovateľom živnosti (veľkoobchod)	(od: 23.02.2011)
	sprostredkovateľská činnosť v oblasti služieb	(od: 23.02.2011)
	prenájom hnuteľných vecí	(od: 23.02.2011)
	administratívne služby	(od: 23.02.2011)
	služby súvisiace s počítačovým spracovaním údajov	(od: 23.02.2011)
	vykonávanie mimoškolskej vzdelávacej činnosti	(od: 23.02.2011)
	verejné obstarávanie	(od: 23.02.2011)
	technik požiarnej služby	(od: 23.02.2011)
	bezpečnostnotechnické služby	(od: 23.02.2011)

	správa registratúry	(od: 23.02.2011)
	Ubytovacie služby v ubytovacích zariadeniach v rozsahu voľnej živnosti	(od: 21.09.2019)
	Poradenská činnosť v oblasti energetiky v rozsahu voľnej živnosti	(od: 21.09.2019)
	Prevádzkovanie športových zariadení a zariadení slúžiacich na regeneráciu a rekondíciu	(od: 21.09.2019)
	Výskum a vývoj v oblasti prírodných, technických, spoločenských a humanitných vied	(od: 21.09.2019)
	Podnikanie v oblasti nakladania s nebezpečným odpadom	(od: 21.09.2019)
	Montáž, oprava a údržba elektrických zariadení	(od: 21.09.2019)
	Inžiniersko-investorská činnosť v investičnej výstavbe- obstarávateľská činnosť v stavebníctve a v energetike	(od: 21.09.2019)
	Prenájom nehnuteľností, bytov a nebytových priestorov spojený s doplnkovými službami - obstarávateľská činnosť	(od: 21.09.2019)
	Poskytovanie elektronickej komunikačnej siete a poskytovanie elektronických komunikačných služieb	(od: 21.09.2019)
Štatutárny orgán:	predstavenstvo	(od: 27.02.2004)
	Ing. Peter Dovhun - Predseda predstavenstva Stará cesta 432/29 Šamorín 931 01 Vznik funkcie: 13.02.2021	(od: 11.03.2021)
	Marián Širanec , MBA - Podpredseda predstavenstva Tomášikova 15950/10A Bratislava - mestská časť Ružinov 821 01 Vznik funkcie: 13.02.2021	(od: 11.03.2021)
	Ing. Jaroslav Vach , MBA - Člen predstavenstva Šumavská 530/33 Bratislava - mestská časť Ružinov 821 08 Vznik funkcie: 13.02.2021	(od: 11.03.2021)
	Mgr. Martin Riegel - Člen predstavenstva Suchá 3005/9 Bratislava - mestská časť Nové Mesto 831 01 Vznik funkcie: 13.02.2021	(od: 11.03.2021)
	Ing. Miroslav Janega - Člen predstavenstva 150	(od: 11.03.2021)

	Teriakovce 080 05 Vznik funkcie: 13.02.2021	
Konanie menom spoločnosti:	Vo všetkých veciach v mene spoločnosti sú oprávnení konať a podpisovať vždy dvaja členovia predstavenstva spoločne. Predstavenstvo môže formou podpisových oprávnení delegovať podpisovanie vybraných dokumentov na nižšie úrovne riadenia. Podpisové oprávnenia sú podrobne upravené vnútornými predpismi spoločnosti. Podpisovanie za spoločnosť sa vykoná tak, že k vytlačenému alebo napísanému názvu spoločnosti, menám a funkciám podpisujúci pripoja svoj podpis.	(od: 16.12.2021)
Základné imanie:	235 000 000 EUR Rozsah splatenia: 235 000 000 EUR	(od: 10.07.2021)
Akcie:	Počet: 235 Druh: kmeňové Podoba: zaknihované Forma: akcie na meno Menovitá hodnota: 1 000 000 EUR	(od: 10.07.2021)
Akcionár:	Slovenská republika zastúpená Ministerstvom financií Slovenskej republiky Štefanovičova 5 Bratislava 817 82	(od: 16.12.2021)
Dozorná rada:	JUDr. Eva Murínová - člen dozornej rady Námestie sv. Ignáca 15/30 Leopoldov 920 41 Vznik funkcie: 20.02.2020	(od: 28.04.2020)
	Róbert Király - člen dozornej rady Jilemnického 643/12 Liptovský Mikuláš 031 01 Vznik funkcie: 17.04.2020	(od: 03.06.2020)
	Ing. Marcel Klimek - podpredseda dozornej rady Magurská 3488/5A Bratislava - mestská časť Nové Mesto 831 01 Vznik funkcie: 15.05.2020	(od: 04.06.2020)
	Ing. Milan Jarás , PhD. - člen dozornej rady Andreja Mráza 3160/6 Bratislava - mestská časť Ružinov 821 03 Vznik funkcie: 27.11.2020	(od: 13.01.2021)

	Juraj Mach Súťažná 1122/14 Bratislava - mestská časť Ružinov 821 08 Vznik funkcie: 16.02.2021	(od: 16.12.2021)
	Ing. Peter Habšuda - predseda dozornej rady Hurbanova 3470/19 Pezinok 902 03 Vznik funkcie: 01.04.2021	(od: 27.04.2021)
	Ing. Peter Dragúň - člen dozornej rady Homolova 2166/19 Bratislava - mestská časť Dúbravka 841 02 Vznik funkcie: 01.04.2021	(od: 27.04.2021)
	Ing. Vladimír Beňo Tatranská 3108/3 Žilina 010 08 Vznik funkcie: 01.05.2021	(od: 16.12.2021)
	PhDr. Ivan Pešout , PhD. Nám Sv. Františka 3406/14 Bratislava - mestská časť Karlova Ves 841 04 Vznik funkcie: 21.04.2021	(od: 16.12.2021)
	Ing. Michal Janíček Ferka Urbánka 3860/8 Trnava 917 01 Vznik funkcie: 21.04.2021	(od: 16.12.2021)
	Ing. Marek Šimlaštík - podpredseda dozornej rady Kataríny Franklovej 5413/3 Pezinok 902 01 Vznik funkcie: 08.09.2022	(od: 27.10.2022)
	Ľuboš Obžut - člen dozornej rady Hubová 2151/23 Sučany 038 52 Vznik funkcie: 21.08.2022	(od: 27.10.2022)
Ďalšie právne skutočnosti:	Obchodná spoločnosť bola založená zakladateľskou zmluvou zo dňa 13.12.2001 v zmysle ust. §§ 154-220 Obchodného zákonníka v dôsledku rozdelenia Slovenské elektrárne, a.s. na Slovenské elektrárne, a.s. Slovenská elektrizačná prenosová sústava, a.s., Tepláreň	(od: 21.01.2002)

Košice, a.s. na základe Uznesenia vlády SR č. č. 758 z 27.9.2000, v zmysle ust. § 69 ods. 4 Obchodného zákonníka.	
Rozhodnutie jediného akcionára zo dňa 28.03.2003. Deň zániku funkcie členov dozornej rady - Branislav Ďurajka: 28.03.2003 Ing. Ivan Demovič: 28.03.2003 prof. Ing. František Janíček, PhDr.: 28.03.2003 Ing. Michal Merga: 28.03.2003 Ing. Dagmar Repčeková: 28.03.2003 Ing. Jozef Urmín: 28.03.2003 RNDr. Dušan Jurčák: 28.03.2003	(od: 22.10.2003)
Rozhodnutie jediného akcionára zo dňa 30.06.2003. Deň zániku funkcie členov predstavenstva - Ing. Karol Česnek: 30.06.2003 Ing. Alexander Kšiňan: 30.06.2003 Ing. Ivan Maník: 30.06.2003 Ing. Alena Šalamonová: 30.06.2003 Deň zániku funkcie člena dozornej rady - Ing. Roman Krasňanský : 30.06.2003.	(od: 23.10.2003)
Rozhodnutie jediného akcionára z 24.10.2003.	(od: 26.02.2004)
Zmeny stanov vykonané rozhodnutím jediného akcionára zo dňa 28.11.2003 osvedčené notárskou zápisnicou N 2720/2003, Nz 111682/2003 spísanou Mgr. Tomášom Leškovským, notárskym kandidátom notára JUDr. Ľubomíra Vlhu.	(od: 27.02.2004)
Rozhodnutie jediného akcionára zo dňa 21.6.2004. Funkcia člena predstavenstva Ing. Š. Bugára sa končí dňom 21.6.2004. Funkcia člena dozornej rady Ing. V. Černáka sa končí dňom 21.6.2004.	(od: 21.07.2004)
Rozhodnutie jediného akcionára zo dňa 12.11.2004 vo forme notárskej zápisnice N 865/2004, Nz 81890/2004 spísanej Mgr. Tomášom Leškovským, notárskym kandidátom.	(od: 25.11.2004)
Rozhodnutie jediného akcionára zo dňa 26.10.2006.	(od: 16.11.2006)
Rozhodnutie jediného akcionára zo dňa 30.11.2007 spísané vo forme notárskej zápisnice N 326/2007, Nz 50585/2007	(od: 19.12.2007)
Zápisnica o priebehu a výsledku volieb členov dozornej rady zamestnancami spoločnosti zo dňa 20.2.2008.	(od: 15.03.2008)
Notárska zápisnica č. N 14/2009, Nz 3848/2009, NCRls 3879/2009 zo dňa 10.02.2009.	(od: 24.02.2009)
Rozhodnutie jediného akcionára zo dňa 21.10.2009.	(od: 07.11.2009)

Rozhodnutie jediného akcionára zo dňa 03.09.2010.	(od: 23.09.2010)
Rozhodnutie jediného akcionára vo forme notárskej zápisnice N 19/2011, Nz 3941/2011 zo dňa 04.02.2011	(od: 23.02.2011)
Rozhodnutie jediného akcionára zo dňa 04.05.2011.	(od: 18.05.2011)
Rozhodnutie jediného akcionára zo dňa 26.04.2012.	(od: 18.05.2012)
Rozhodnutie jediného akcionára zo dňa 14.06.2012.	(od: 29.06.2012)
Oznámenie o odstúpení z funkcie zo dňa 30.07.2012.	(od: 09.08.2012)
Rozhodnutie jediného akcionára zo dňa 06.09.2012.	(od: 15.09.2012)
Rozhodnutie jediného akcionára zo dňa 02.05.2013.	(od: 18.05.2013)
Notárska zápisnica č. N 436/2015, Nz 26163/2015, NCRls 26747/2015 zo dňa 28.07.2015.	(od: 26.08.2015)
Rozhodnutie jediného akcionára zo dňa 21.03.2019.	(od: 17.04.2019)
Rozhodnutie jediného akcionára o schválení výšky základného imania zo dňa 17.12.2020 vo forme Notárskej zápisnice (N 459/2020, Nz 53067/2020, NCR1s 53629/2020)	

COLONNADE
A FAIRFAX COMPANY

Informácie o spracúvaní osobných údajov

podľa článkov 13 a 14 nariadenia Európskeho parlamentu a Rady 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej len „**GDPR**")

V súvislosti so spracúvaním osobných údajov dotknutých osôb prevádzkovateľ týmto poskytuje príslušné informácie podľa článkov 13 a 14 GDPR.

Prevádzkovateľ: **Colonnade Insurance S.A.**, so sídlom Rue Jean Piret 1, L-2350 Luxemburg, Luxemburské veľkovojvodstvo, zapísaná v obchodnom registri v Luxembursku pod číslom č. B 61605, konajúca prostredníctvom Colonnade Insurance S.A., pobočka poisťovne z iného členského štátu, so sídlom Moldavská cesta 8 B, 042 80 Košice - mestská časť Juh, IČO: 500 13 602, IČ DPH: SK 4120026471, zapísaná v Obchodnom registri Okresného súdu Košice I., oddiel: Po, vložka č.: 591/V

Kontaktné údaje prevádzkovateľa:
adresa na zasielanie písomností Colonnade Insurance S.A., Rue Jean Piret 1, L-2350 Luxemburg, Luxembursko
alebo
Colonnade Insurance S.A., pobočka poisťovne z iného členského štátu, Moldavská cesta 8 B, 042 80 Košice, Slovenská republika, telefonický kontakt: +421 55 6826 222, emailový kontakt: info@colonnade.sk

Kontaktné údaje zodpovednej osoby:
adresa na zasielanie písomností Colonnade Insurance S.A., pobočka poisťovne z iného členského štátu Moldavská cesta 8 B, 042 80 Košice, Slovenská republika
telefonický kontakt: +421 55 6826 222, emailový kontakt: dpo@colonnade.sk

Účely a právne základy spracúvania:

I. Prevádzkovateľ spracúva osobné údaje klientov, potenciálnych klientov, ich zástupcov, škodcov, poškodených, príjemcov poistného plnenia a svedkov škodovej udalosti na nasledovné účely:
   a) Identifikácia klientov, ich zástupcov a možnosti následnej kontroly tejto identifikácie; uzavieranie poistných zmlúv a správa poistenia; likvidácia poistných udalostí alebo škodových udalostí; ochrana a domáhanie sa práv prevádzkovateľa; zdokumentovanie činnosti prevádzkovateľa; výkon dohľadu nad prevádzkovateľom a nad jeho činnosťou; na plnenie povinností a úloh prevádzkovateľa podľa zákona č.39/2015 Z. z. o poisťovníctve v znení neskorších predpisov (ďalej len „Zákon o poisťovníctve") alebo osobitných predpisov; správa zaistných zmlúv medzi prevádzkovateľom a zaisťovňou, zaisťovňou z iného členského štátu alebo pobočkou zahraničnej zaisťovne; vybavovanie nárokov zo zaistných zmlúv a na účel kontroly poskytnutých plnení z poistných zmlúv, ku ktorým zaisťovňa, pobočka zaisťovne z iného členského štátu a pobočka zahraničnej zaisťovne poskytuje zaistenie – prevádzkovateľ spracúva osobné údaje na právnom základe článku 6 ods. 1 písm. c) GDPR – spracúvanie je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa podľa § 78 Zákona na právnom základe článku 6 ods. 1 písm. b) GDPR - spracúvanie je nevyhnutné na plnenie zmluvy.
   b) Plnenie povinností vyplývajúcich z uplatňovania medzinárodných sankcií – na právnom základe článku 6 ods. 1 písm. c) GDPR – spracúvanie je nevyhnutné na splnenie zákonnej povinnosti podľa zákona č. 289/2016 Z. z. o vykonávaní medzinárodných sankcií v znení neskorších predpisov.
   c) Poskytovanie údajov orgánom verejnej moci – na právnom základe článku 6 ods. 1 písm. c) GDPR – spracúvanie je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa .
   d) Priamy marketing – oslovovanie klienta s obchodnými informáciami a ponukami – na právnom základe článku 6 ods. 1 písm. f) GDPR (viď Recitál 47 GDPR) - spracúvanie je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ.
   Oprávneným záujmom prevádzkovateľa je realizácia práva na výkon podnikateľských činností a z toho vyplývajúci záujem o oslovovanie klienta s obchodnými informáciami a ponukami ďalších produktov s úmyslom následného uzavretia poistnej zmluvy.

e) Overenie identifikácie fyzickej osoby a jej výskytu na sankčných zoznamoch – na právnom základe článku 6 ods. 1 písm. f) GDPR – spracúvanie je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ.
Oprávneným záujmom prevádzkovateľa, resp. jeho vlastníkov, na účely overenia identifikácie fyzickej osoby a jej výskytu na sankčných zoznamoch je splnenie povinností vyplývajúcich z právnych predpisov, ktorými sa spravuje prevádzkovateľ, jeho vlastníci, prípadne ich štatutárne orgány.

f) Priamy marketing – oslovovanie dotknutej osoby s ponukami produktov a služieb, reklamnými materiálmi a ďalšími informáciami o inováciách a aktivitách prevádzkovateľa – na právnom základe článku 6 ods. 1 písm. a) GDPR – súhlas so spracúvaním osobných údajov.

II. Prevádzkovateľ spracúva prostredníctvom sprostredkovateľov aj osobitnú kategóriu osobných údajov klientov a ich zástupcov – biometrické údaje obsiahnuté v biometrickom podpise na účely uzavretia zmluvného vzťahu prostredníctvom biometrického podpisu a následnej správy (uchovania) k tomu zodpovedajúcej zmluvnej dokumentácie, obsahom ktorej je získaný biometrický podpis – na právnom základe článku 6 ods. 1 písm. a) GDPR – súhlas so spracúvaním osobných údajov.

Kategórie dotknutých osobných údajov:

1. bežné osobné údaje podľa článku 6 GDPR (body I. a), b), c) a e)), získavané aj prostredníctvom hlasových nahrávok telefonických hovorov s dotknutými osobami;
2. osobitná kategória osobných údajov – údaje týkajúce sa zdravotného stavu (bod I. a)) a biometrický podpis (bod II.);
3. súbory cookies[1] – všetky typy a druhy (najmä nevyhnutné, preferenčné, analytické, štatistické, trackingové, profilovacie, na cielenú reklamu – targeting, marketingové, geolokačné, plug-iny pre sociálne siete).

Kategórie príjemcov osobných údajov: finanční agenti, finanční poradcovia, finanční sprostredkovatelia z iného členského štátu v sektore poistenia alebo zaistenia, znalci, poskytovatelia asistenčných služieb, zdravotnícke zariadenia, lekári pripravujúci posudky a odborné stanoviská, zaisťovatelia, spoločnosti poskytujúce služby mimosúdneho vymáhania pohľadávok, spoločnosti poskytujúce poštové a súvisiace služby, spoločnosti poskytujúce služby správy a uloženia dokumentov a dát, ich skartovania a likvidácie, zálohovania a obnovy dát, poskytovatelia IT služieb, spoločnosti spracúvajúce súbory cookies, osoby poskytujúce služby v oblasti riešenia poistných udalostí, osoby prevádzkujúce registre informácií o poistných / škodových udalostiach alebo zoznamy sankcií alebo sankcionovaných entít, exekútori, orgány činné v trestnom konaní, súdne orgány, Národná Banka Slovenska, ďalšie orgány verejnej moci a orgány dohľadu a/alebo dozoru.

Prenos osobných údajov do tretích krajín: Prevádzkovateľ môže prenášať niektoré osobné údaje medzi krajinami Európskej únie („EÚ") a krajinami mimo EÚ, pričom takéto prenosy podliehajú pravidlám špecifikovaným v štandardných zmluvných doložkách EÚ (Standard Contractual Clauses, „SCC") alebo sú vykonávané na základe rozhodnutia Európskej komisie o primeranosti podľa článku 45 GDPR.

Doba uchovávania osobných údajov: osobné údaje sú spracúvané maximálne po dobu 10 rokov od skončenia účelu spracúvania; pre jednotlivé cookies sú tieto doby uvedené na webovej stránke prevádzkovateľa www.colonnade.sk v časti Nastavenia súborov cookies / Vyhlásenie o cookies.

Profilovanie: Prevádzkovateľ môže využívať automatizované rozhodovacie procesy založené na údajoch poskytnutých dotknutou osobou a / alebo jej zástupcom (napríklad poistený, osoba nárokujúca si poistné plnenie, právny zástupca, finančný sprostredkovateľ, ...) a profilovanie dotknutej osoby. Algoritmy prevádzkovateľa zohľadňujú rôzne faktory, ako je demografia dotknutej osoby (napr. vek), aktuálne rizikové trendy súvisiace s konkrétnymi poistnými krytiami, história škôd, súbory cookies a iné. Tieto automatizované procesy možno použiť v nasledujúcich situáciách:

1. posúdenie poistného rizika, ktoré môže ovplyvniť rozsah ponúkaného produktu, výšku poistného alebo odmietnutie uzavretia poistnej zmluvy;

[1] Cookie je v protokole HTTP malé množstvo stavových dát, ktoré WWW server pošle webovému prehliadaču súčasne s požadovanou webovou stránkou daného webového sídla, ak toto používa cookies. Ak sú cookies v prehliadači povolené, uložia sa na počítači používateľa, zvyčajne ako krátky textový súbor na určené miesto.

2. oslovenie dotknutej osoby prostredníctvom priameho marketingu alebo iného predajného kanála a ponúknutie jej poistného produktu alebo služby;
3. vyplatenie náhrady škody v určitých typoch nárokov, pokiaľ ide o ich schválenie a výšku vyplateného plnenia;
4. dodržiavanie medzinárodných sankcií, ktoré môžu mať vplyv na možnosť uzavretia poistnej zmluvy alebo výplaty škôd.

Dotknutá osoba a/alebo jej zástupca má okrem iného právo obrátiť sa na Prevádzkovateľa a požadovať zdôvodnenie automatizovaného rozhodnutia alebo takéto rozhodnutie napadnúť.

Práva dotknutej osoby:

1. právo na prístup k osobným údajom, ktoré sa jej týkajú,
2. právo na opravu nesprávnych osobných údajov, ktoré sa jej týkajú,
3. právo výmazu osobných údajov, ktoré sa jej týkajú,
4. právo na obmedzenie spracúvania osobných údajov,
5. právo namietať proti spracúvaniu osobných údajov, ktoré sa jej týkajú,
6. právo na prenosnosť osobných údajov,
7. právo kedykoľvek odvolať svoj udelený súhlas na spracúvanie osobných údajov,
8. právo podať sťažnosť dozornému orgánu.

Vyššie uvedené práva má dotknutá osoba v rozsahu podľa článkov 15 až 21 a článku 77 GDPR. Dotknutá osoba si môže uplatniť svoje práva ústne, písomne alebo elektronicky, cez vyššie uvedené kontaktné údaje. Ak dotknutá osoba požiada o ústne poskytnutie informácií, informácie sa poskytnú po preukázaní jej totožnosti.

Ak sa osobné údaje spracúvajú na účely priameho marketingu, dotknutá osoba má právo kedykoľvek namietať proti spracúvaniu osobných údajov, ktoré sa jej týkajú na účely takéhoto marketingu, vrátane profilovania v rozsahu, v akom súvisí s takýmto priamym marketingom.

Neposkytnutie potrebných osobných údajov zo strany dotknutej osoby môže mať za následok neuzatvorenie príslušnej poistnej zmluvy, nevyplatenie poistného plnenia.

Informácie o zdroji osobných údajov: osobné údaje týkajúce sa dotknutej osoby boli získané z nasledovného zdroja: klient, zástupca klienta, finančný agent, finančný poradca, finančný sprostredkovateľ z iného členského štátu v sektore poistenia alebo zaistenia, osoby zadávajúce osobné údaje do portálov prevádzkovateľa, osoby hlásiace poistné / škodové udalosti, zaistený, sprostredkovateľ podľa článku 28 GDPR, Obchodný register, zmluvní partneri prevádzkovateľa, oprávnení poskytovať osobné údaje klientov pre účely priameho marketingu, exekútori, orgány činné v trestnom konaní, súdne orgány, Národná Banka Slovenska, ďalšie orgány verejnej moci a orgány dohľadu a / alebo dozoru.

Doplňujúce otázky k činnosti poisteného

1. Je spoločnosť, ktorú zastupujete, priamo alebo nepriamo vlastnená alebo kontrolovaná ruskou/ bieloruskou osobou (právnickými osobami registrovanými v Rusku/Bielorusku alebo fyzickými osobami s ruským/ bieloruským občianstvom)?

   Ak je odpoveď „Áno", uveďte prosím konečného(-ých) príjemcu(-ov) alebo konečného(-ých) vlastníka(-ov) akcií alebo kontrolné subjekty a ich kontrolný podiel v spoločnosti:

2. Je spoločnosť, ktorú zastupujete, priamo alebo nepriamo vlastnená alebo kontrolovaná akoukoľvek ukrajinskou osobou (právnickými osobami registrovanými na Ukrajine alebo fyzickými osobami s ukrajinským občianstvom)?

   Ak je odpoveď „Áno", uveďte prosím konečného(-ých) príjemcu(-ov) alebo konečného(-ých) vlastníka(-ov) akcií alebo kontrolné subjekty a ich kontrolný podiel v spoločnosti:

3. Má spoločnosť, ktorú zastupujete, nejaké dcérske spoločnosti alebo iné záujmy, aktíva alebo stále prevádzky v Rusku alebo v Bielorusku?

   Ak je odpoveď „Áno", uveďte prosím podrobnosti:

4. Má spoločnosť, ktorú zastupujete nejaké dcérske spoločnosti alebo iné záujmy, aktíva alebo stále prevádzky na Ukrajine?

   Ak je odpoveď „Áno", uveďte prosím podrobnosti:

5. Predáva spoločnosť, ktorú zastupujete nejaké výrobky/služby priamo na ruskom/bieloruskom trhu? Nakupuje spoločnosť, ktorú zastupujete nejaké výrobky/služby priamo od ruských/bieloruských osôb?

   Ak je odpoveď „Áno", uveďte prosím podrobnosti:

6. Predáva spoločnosť, ktorú zastupujete nejaké výrobky/služby priamo na ukrajinskom trhu? Nakupuje spoločnosť, ktorú zastupujete nejaké výrobky/služby priamo od ukrajinských osôb?

   Ak je odpoveď „Áno", uveďte prosím podrobnosti: