

## Príloha č. 1 K Sprostredkovateľskej zmluve o spracovaní osobných údajov - Technické a organizačné opatrenia k zabezpečeniu ochrany osobných údajov

### Obsah

Preambula .....	1
1. Kontrola vstupu .....	1
2. Kontrola prístupu .....	3
3. Prístupového oprávnenia .....	6
4. Kontrola sprístupňovania údajov .....	8
5. Nakladanie s dokumentmi obsahujúcimi osobné údaje .....	11
6. Kontrola pracovných postupov .....	11
7. Kontrola .....	dostupnosti 122
8. Kontrola zamýšľaného použitia .....	123
9. Organizačná .....	kontrola 133

### Preambula

Spoločnosť sprostredkovateľa implementovala požiadavky na ochranu súkromia pri nakladaní s osobnými údajmi (ďalej iba „Pravidlá“). Prijatím týchto pravidiel vytvára spoločnosť sprostredkovateľa jednotnú úpravu údajov na vysokej úrovni, ktorá platí po celom svete pre nakladanie s údajmi ako v rámci jednotlivých spoločností, tak medzi jeho jednotlivými spoločnosťami navzájom aj mimo krajín EÚ. V rámci spoločnosti sprostredkovateľa musí byť zaistené, že príjemca osobných údajov bude tieto údaje spracúvať v súlade so zásadami upravenými v právnych predpisoch na ochranu údajov, ktoré sa vzťahujú na ich odosielateľa teda subjektu usídleného v krajine EÚ.

Na účely týchto pravidiel sa Zákazníkom myslí prevádzkovateľ v zmysle Aplikovateľného práva a Dodávateľom Sprostredkovateľ v zmysle Aplikovateľného práva alebo kde Prevádzkovateľ spracúva dáta Zákazníka v pozícii sprostredkovateľa a sprostredkovateľ je teda v pozícii ďalšieho sprostredkovateľa v zmysle Aplikovateľného práva.

Dodávateľ podpisom zmluvy o spracovaní deklaruje splnenie požiadaviek uvedených v tejto prílohe, pokiaľ sú touto prílohou vyžadované na účely plnenia zmluvy. Prípadné odchýlky a riadenie rizík s tým spojených, vrátane zodpovedajúcich opatrení, sú uvedené nižšie, pri jednotlivých požiadavkách, s tým, že Zákazník je oprávnený vykonávať kontrolu plnenia takto zjednaných výnimiek a na ne nadväzujúcich opatrení.

### Kontrola vstupu



Pravidlá ustanovia: "... zabrániť prístupu neoprávnených osôb k informačným systémom na spracúvanie osobných údajov, v rámci ktorých sú tieto spracúvané či

používané (regulácia fyzického prístupu).

Pod pojmom „vstup“ sa rozumie fyzický prístup osôb do budov a zariadení, v ktorých sú prevádzkované a používané IT systémy. Tieto môžu zahŕňať napríklad počítačové centrá, v ktorých sú umiestnené webové servery, aplikačné servery, databáze, hlavné servery a systémy na uchovávanie dát a kancelárske priestory, kde zamestnanci pracujú s počítačmi. Tieto zariadenia zahŕňajú takisto zariadenia, kde sú umiestnené sieťové komponenty a sieťové káble.

- **Definícia bezpečnostných priestorov**

*Bezpečnostné požiadavky vzťahujúce sa na budovy či priestory sú stanovované s ohľadom na systémy na spracúvanie údajov, v rámci ktorých sú alebo môžu byť osobné údaje Prevádzkovateľa spracúvané alebo sprístupnené. Rozhodujúcim faktorom na hodnotenie je požiadavka na ochranu údajov Zákazníka, ku ktorým má Dodávateľ prístup.*

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

- **Implementácia účinných postupov na povoľovanie vstupu**

*Musia byť prijaté vhodné technické opatrenia (napr. bezpečnostné zasklenie, elektronický zabezpečovací systém, turnikety na čipové karty, bezpečnostný vstupný systém umožňujúci vstup jednotlivcovi, uzamykacie systémy) a organizačné opatrenia (napr. bezpečnostná ochranka) za účelom zabezpečenia bezpečnostných priestorov a prístupu do nich pred vstupom neoprávnených osôb.*

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

- **Špecifikácia osôb s oprávnením vstupu**

*Musia byť definované podmienky pre osoby so všeobecným oprávnením vstupu, rovnako ako pre skupinu týchto osôb, pričom oprávnenia na vstup do bezpečnostných priestorov musia byť obmedzené iba na nevyhnutne potrebný počet osôb („princíp nevyhnutného počtu oprávnení“). Akejkolvek osobe bez oprávnenia nebude vstup povolený. Prostriedky umožňujúce vstup do budov alebo priestorov budú vydané iba konkrétnym osobám a nesmú byť predávané tretím osobám. Užívatelia musia byť o tomto opatrení informovaní.*

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

- **Správa a evidencia jednotlivých oprávnení k vstupu po celú dobu životného cyklu**

*Musí byť vytvorený proces na podávanie žiadostí, schvaľovanie, vydávanie, správu a vrácanie prostriedkov umožňujúcich vstup a na zrušenie prístupových práv (vrátane správy a evidencie kľúčov, vizuálnych identifikačných kariet, transpondérov, čipových kariet, apod.). Tento proces musí byť popísaný a implementovaný. Musia byť stanovené pravidlá a postupy na zablokovanie oprávnení k vstupu. Pokiaľ akákoľvek osoba ukončí svoj pracovný pomer so spoločnosťou alebo bude prevezená do iného oddelenia, musia byť neodkladne vrátené/zablokované všetky prostriedky umožňujúce vstup a všetky prístupové práva vo vzťahu k priestorom, do ktorých príslušná osoba už nepotrebuje mať v súvislosti s plnením svojich pracovných povinností prístup. Všetky osoby poverené plnením povinností súvisiacich s bezpečnosťou, najmä bezpečnostná*



služba pri vstupe, budú informované o zamestnancoch, ktorí ukončili svoj pracovný pomer u spoločnosti alebo u ktorých došlo k zmene pracovných povinností.

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

- **Návštevníci a externí pracovníci**

Musia byť vytvorené písomné pravidlá pre vstup externých osôb, ako sú napríklad návštevy alebo dodávateľa, do priestorov spoločnosti. Tieto pravidlá musia minimálne stanovovať, aby externé osoby prítomné v priestoroch spoločnosti boli povinné kedykoľvek preukázať, že sú oprávnené sa v budove pohybovať, napr. na základe návštevnjej karty alebo identifikačnej karty Dodávateľa. Meno a pôvod osoby (jej zamestnávateľ, obchodná adresa alebo bydlisko) musia byť evidované. Povinnou požiadavkou je vykonávanie náhodných kontrol oprávnení vydaných pre vstup do spoločnosti. V prípade potreby zvýšenej ochrany (kategória ochrany 3 a vyššia) musia byť všetky osoby, ktoré nie sú zamestnancami spoločnosti, sprevádzané a pri plnení svojej práce musia byť pod dozorom.

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

### Kontrola prístupu

Pravidlá ustanovia: "...zaistiť, aby neoprávnené osoby nemohli informačné systémy na spracúvanie údajov používať (regulácia používania dátových systémov). Vedľa kontroly prístupu je cieľom kontroly prístupu zabrániť neautorizovaným osobám používať systémy spracúvania dát, v ktorých sú osobné údaje uchovávané, spracúvané alebo používané.

- **Ochrana prístupu (autentizácia)**

Prístup k systémom na spracúvanie údajov, v ktorých sú spracúvané údaje, môže byť umožnený až potom, čo dôjde k úspešnému overeniu totožnosti a oprávnení danej oprávnenej osoby (napr. pomocou užívateľského mena a hesla alebo čipovej karty/PIN) za pomoci najmodernejších bezpečnostných opatrení. V prípade

nedostatočného oprávnenia musí byť prístup odoprený.

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

- **Špeciálna autentizácia na účely zaistenia maximálnej úrovne ochrany**

Pri prístupe do systému, v ktorom sú spracúvané údaje z vonkajšieho prostredia (vzdialený prístup, prístup z internetu apod.), je rozhodnuté o potrebe vynútenia špeciálnej autentizácie. Rozhodnutie je učené na základe analýzy rizík, technických možností a/alebo obvyklej bezpečnostnej praxe s prihliadnutím k aktuálnym hrozbám, potenciálnym dopadom, ostatným zavedeným bezpečnostným opatreniam a nákladom potrebným na implementáciu špeciálnej autentizácie.

Špeciálna autentizácia je vždy založená na niekoľkých (aspoň dvoch) faktoroch, ako napr. určitá vec vo vlastníctve či nejaká znalosť alebo na špecifickom faktore, ktorý je jedinečný pre daného užívateľa (obvykle procesy využívajúce biometrické prvky). Príkladom sú:

- **Čipová karta s certifikátom a PIN**

Jednorazové heslá (generátor jednorazových hesiel, sms správa s autorizačným kódom, autorizácie pomocou chip TAN) a užívateľské heslá



## *Používanie biometrických postupov a hesiel*

*Jednoduchá autentizácia kombinovaná s prístupom cez VPN.*

*Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒*

- **Jednoduchá autentizácia pomocou užívateľského mena/hesla pre vysokú úroveň ochrany**

*Heslá musia spĺňať príslušné minimálne požiadavky, napr. minimálny počet znakov a zložitosť. Heslá musia byť menené v pravidelných intervaloch. Počiatočné heslá musia byť zmenené ihneď. Implementácia požiadaviek na dĺžku, zložitosť a platnosť hesiel musí byť zaistená prostredníctvom technického nastavenia, ak je to možné.*

*Dĺžka hesla musí byť aspoň 8 znakov.*

*Heslo sa musí skladať z kombinácie rôznych znakov. Dostupné znaky sa delia do štyroch kategórií:*

*malé písmená, napr. abcdefgh...*

*veľké písmená, napr. ABCDEFGH...*

*čísllice, napr. 123456...*

*zvláštne znaky, napr. !\$%&...',*

*heslá musia obsahovať kombináciu aspoň troch vyššie uvedených kategórií znakov.*

*Veľmi jednoduché heslá a slová, ktoré je možné ľahko uhádnuť, nesmú byť používané ako heslá.*

*Heslo musí byť menené v pravidelných intervaloch, aspoň raz za 90 dní.*

*Pri zmene hesla nesmie byť nové heslo zhodné so žiadnym zo štyroch naposledy používaných hesiel.*

*Heslo nesmie byť pri jeho zadávaní na obrazovke viditeľné ako prostý text.*

*Počiatočné heslo musí byť užívateľovi poskytnuté prostredníctvom zabezpečených kanálov a/alebo musí byť užívateľ požiadaný, aby si toto heslo zmenil ihneď po prvom prihlásení.*

*Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒*

- **Evidencia prístupu**

*Všetky úspešné i nepovolené pokusy o prístup musia byť zaznamenávané (užívateľské ID, počítač, použitá IP adresa) a uchovávané po dobu troch mesiacov vo forme umožňujúcej ich kontrolu. Na základe náhodných kontrol budú vykonávané pravidelné vyhodnocovania za účelom zistenia nesprávnych postupov.*

*Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒*



- **Zabezpečený prenos prihlasovacích údajov v sieti**

*Prihlasovacie údaje (ako je užívateľské ID a heslo) nesmú byť nikdy v sieti prenášané nezabezpečené.*

*Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy.* ☒

*Zablokovanie hesla po neúspešnom pokuse/nečinnosti a proces na opätovné nastavenie zablokovaného prístupu*

*Po opakovanom nesprávnom pokuse o prihlásenie musí byť prístup zablokovaný. Musí byť vytvorený proces na opätovné nastavenie alebo odblokovanie zablokovaného prístupu. Tento proces musí byť popísaný a implementovaný. Užívateľské ID, ktoré nie sú po dlhú dobu (maximálne 180 dní) používané, musia byť automaticky zablokované alebo nastavené ako neaktívne.*

*Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy.* ☒

- **Identifikácia oprávnených osôb**

*Skupina osôb oprávnených k prístupu k IT systémom Zákazníka musí byť obmedzená na absolútne minimum potrebné na plnenie konkrétnych povinností alebo funkcií danej osoby v rámci organizácie prevádzkových činností.*

*Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy.* ☒

- **Správa a evidencia jednotlivých prístupových oprávnení a prostriedkov autentizácie**

*Musí byť vytvorený proces na podávanie žiadostí, schvaľovanie, vydávanie a vrátenie prostriedkov umožňujúcich autentizáciu a prístupových oprávnení. Tento proces musí byť popísaný a implementovaný a musí zahŕňať aspoň postupy pre žiadosti o prístupové oprávnenia a prostriedky autentizácie a ich schvaľovanie a ďalej postupy na vrátenie prostriedkov autentizácie a na zrušenie prístupových oprávnení.*

*Prístupové oprávnenia musia byť vždy pridelené iba pre také systémy na spracúvanie údajov/druhy, ku ktorým daná osoba potrebuje prístup na účely plnenia svojich povinností („princíp najnižšieho možného oprávnenia). Prostriedky autentizácie a prístupové identifikačné údaje na prístup do systémov na spracúvanie údajov budú v zásade pridelené na individuálnom základe a budú naviazané (užívateľské ID) na osobné údaje (ako napr. heslo, token alebo čipová karta). Prostriedky autentizácie a/alebo kombinácie užívateľského ID/hesla nesmú byť predávané tretím osobám. Užívatelia musia byť o tomto opatrení informovaní.*

*V súlade s pravidlami na ochranu osobných údajov musia byť stanovené pravidlá a postupy na zablokovanie prístupových údajov alebo ich vymazanie. Ak akákoľvek osoba ukončí svoj pracovný pomer so spoločnosťou alebo bude prevezená do iného oddelenia, musia byť bezodkladne vrátené/zablokované všetky prostriedky autentizácie a všetky prístupové oprávnenia pre systémy na spracúvanie údajov, do ktorých príslušná osoba už nepotrebuje mať v súvislosti s plnením svojich pracovných povinností prístup. Rovnako je potrebné zaistiť, aby o skutočnosti, že daná osoba ukončila svoj pracovný pomer so spoločnosťou alebo došlo ku zmene jej náplne práce, boli informované všetky príslušné osoby (najmä IT administrátori/administrátori oprávnení)*

*Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy.* ☒

- **Adresné pridelovanie prostriedkov autentizácie a prístupových identifikačných údajov**

*Prostriedky autentizácie a prístupové identifikačné údaje na prístup do zariadení a systémov musia byť vždy pridelované konkrétnej osobe a naviazané na osobné heslo (užívateľské ID). Prostriedky autentizácie a/alebo kombinácie užívateľského ID/hesla nesmú byť predávané tretím osobám.*

*Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy.* ☒

- **Správanie užívateľov**

*Zamestnanci alebo zástupcovia Dodávateľa sú povinní dodržiavať technické a organizačné opatrenia vo vzťahu ku kontrole prístupu a musia zaistiť, aby z dôvodu nedodržania príslušných opatrení z ich strany nebol umožnený prístup k IT systémom Zákazníka neoprávneným osobám.*

*Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy.* ☒

### **Prístupového oprávnenia**

*Pravidlá u stanovia: "...zaistiť, aby osoby oprávnené na používanie informačných systémov na spracúvanie údajov mali prístup výlučne k údajom, ku ktorým sú oprávnené pristupovať, a aby neoprávnené osoby nemohli osobné údaje počas spracúvania či používania či po ich zaznamenaní čítať, kopírovať, meniť ani mazať (regulácia prístupu k údajom).*

*Cieľom požiadaviek na kontrolu prístupu k údajom je, aby oprávnené osoby mali prístup iba k údajom, na ktoré sa ich prístupové oprávnenie vzťahuje, a aby neoprávnené osoby nemohli osobné údaje čítať, ani s nimi inak manipulovať.*

- **Vytvorenie autorizačného konceptu**

*Autorizačný koncept (užívateľská a administrátorské práva) zaisťuje, aby bol prístup k údajom v systéme umožnený iba v rozsahu nevyhnutnom preto, aby užívateľ mohol vykonať príslušnú úlohu, a to na základe distribúcie interných úloh užívateľa a oddelenia príslušných funkcií. V rámci tohto konceptu budú stanovené pravidlá a postupy na vytvorenie, zmenu a výmaz autorizačných profilov a užívateľských rolí v súlade s pravidlami na ochranu údajov. Autorizačný koncept popíše jednotlivé užívateľské oprávnenia pre rôzne administratívne činnosti (systém, užívateľ, operácie, prenos) a špecifikuje, čo môžu jednotlivé skupiny užívateľov v systéme vykonávať, pričom sú regulované jednotlivé zodpovednosti.*

*Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy.* ☒

- **Implementácia prístupových obmedzení**

*Každé prístupové oprávnenie musí byť naviazané na autorizáciu prístupu k údajom, napríklad prepojením s jednou či viacerými rolami, ktoré sú definované v autorizačnom koncepte. V rámci a prostredníctvom aplikácií je každej osobe s prístupovým oprávnením umožnený prístup iba k tým údajom, ktoré táto osoba potrebuje ku spracovaniu konkrétnej operácie podľa príslušného zadania a ktoré sú nakonfigurované v individuálnom autorizačnom profile takej osoby. Ak sú v rámci rovnakej databázy uchovávané alebo v rámci rovnakého systému spracúvané údaje väčšieho počtu klientov, je nutné stanoviť jednotlivé prístupové obmedzenia*





*tak, aby bolo zaistené, že budú spracúvané výhradne údaje daného klienta (multi-tenancy). Samotná funkcia spracúvania údajov bude obmedzená na nevyhnutne*

*potrebný počet funkcií potrebných na účely spracúvania osobných údajov. Systémy na spracúvanie údajov obsahujú špecifické prvky, ktoré umožňujú osobám prihlasujúcim sa do systému určiť autentickosť daného systému. Osoba s prístupovým oprávnením sa takisto musí v systéme na spracúvanie údajov identifikovať a preukázať sa na základe jedinečných, overiteľných prvkov, ako napr. pomocou čítačky ID na koncových zariadeniach.*

*Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy.* ☒

- **Pridelenie nevyhnutného počtu oprávnení**

*Rozsah oprávnení musí byť obmedzený na nevyhnutné minimum potrebné na splnenie povinností a funkcií danej oprávnenej osoby. Prístup k osobným údajom a jednotlivé oprávnenia budú podliehať časovým limitom, ktoré budú nastavené pri určitých funkciách tak, aby nedošlo k zníženiu kvality spracúvania údajov.*

*Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy.* ☒

- **Správa a evidencia jednotlivých oprávnení na prístup k údajom**

*Musí byť vytvorený proces na podávanie žiadostí, schvaľovanie, vydávanie, zrušenie a kontrolu oprávnení na prístup k údajom; tento proces musí byť popísaný a implementovaný. Musia byť stanovené pravidlá a postupy na udeľovanie/zrušenie oprávnení alebo na prideľovanie užívateľských rolí. Prístupové práva k údajom musia byť implementované prostredníctvom procesu správy prístupových práv v rámci daného IT systému.*

*Jednotlivé oprávnenia musia byť naviazané na osobné ID užívateľa a užívateľský účet. Týmto je vylúčené použitie skupinových ID/hesiel väčším počtom osôb.*

*Pri udeľovaní oprávnení alebo priradovaní užívateľských rolí musí byť udelený iba taký počet prístupových práv, ktorý je nevyhnutný pre plnenie príslušných povinností (zásada nevyhnutne potrebného rozsahu). Je treba zaistiť, aby oddelenie funkcií vymedzených v danom systéme nebolo zrušené na základe kumulatívnych operácií.*

*Ak akákoľvek osoba ukončí svoj pracovný pomer so spoločnosťou alebo bude prevedená do iného oddelenia, musia byť bezodkladne zrušené všetky prístupové práva pre všetky systémy na spracúvanie a uchovávanie údajov, do ktorých príslušná osoba už nepotrebuje mať v súvislosti s plnením svojich pracovných povinností prístup. Rovnako je potrebné zaistiť, aby o skutočnosti, že daná ukončila svoj pracovný pomer so spoločnosťou alebo, že došlo k zmene jej náplne práce, boli informované všetky príslušné osoby (najmä IT administrátori/administrátori oprávnení). Príslušné dokumenty musia byť uchovávané po dobu troch mesiacov.*

*Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy.* ☒

- **Interná údržba, prístup k zariadeniam**

*Ak bude dodávateľ zaisťovať činnosti spojené so servisnými činnosťami v priestoroch Zákazníka, alebo ak mu bude umožnený prístup k hardware Zákazníka, je Dodávateľ povinný zaistiť, aby on a jeho zamestnanci poverení výkonom príslušných prác dodržiavali interné pravidlá a smernice Zákazníka upravujúce ochranu informácií a bezpečnosť IT systémov.*

Splnenie požiadavky 309 je záväznou podmienkou podľa tejto zmluvy. ☒

#### Kontrola sprístupňovania údajov

Pravidlá ustanovia: "...zaistiť, aby v priebehu elektronického prenosu či odovzdávania/sprístupňovania či nahrávania údajov na dátový nosič nemohli neoprávnené osoby osobné údaje čítať, kopírovať, meniť ani zmazať a aby bolo možné overiť a identifikovať spracovávateľov, ktorým majú byť osobné údaje prenášané prostriedkami na prenos osobných údajov (regulácia prenosu dát);

- **Stanovenie subjektov/osôb oprávnených prijímať informácie/vykonávať prenos informácií**

Dodávateľ a zákazník si musia dojednať, ktoré subjekty/osoby sú oprávnené zasielať informácie, o ktoré informácie sa bude jednať a komu môžu byť také informácie zasielané, a takisto sa musia dohodnúť na prenosovej ceste, ktorá môže byť za týmto účelom použitá.

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

- **Legalita prenosu do zahraničia**

V zásade je možné zhromažďovať alebo spracúvať dáta v iných krajinách iba s predchádzajúcim písomným súhlasom Zákazníka.

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

- **Prenos do externých systémov**

V prípade prenosu osobných údajov do externých systémov je šifrovanie nevyhnutnou podmienkou.

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

- **Implementácia bezpečnostných brán v tranzitných bodoch**

IT/NT systémy, prostredníctvom ktorých sa spracúvajú osobné údaje, musia byť zabezpečené voči neoprávnenému prístupu alebo nežiadúcim tokom dát z rovnakých i iných sietí pomocou najmodernejších opatrení (obvykle firewallov). Bez ohľadu na to, či sú implementované firewally na ochranu celej siete v hardware alebo či sú takisto využívané tzv. host-based firewally, musia byť firewally trvalo aktívne. Musia byť učené všetky nevyhnutné kroky za účelom efektívneho zamedzenia akejkoľvek deaktivácie alebo obídienia týchto funkcií zo strany užívateľov. Musia byť vytvorené také pravidlá, aby boli automaticky zablokované všetky komunikačné spojenia, s výnimkou tých nevyhnutne potrebných.

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

- **Posilnenie backend systémov**

Backend systémy musia byť posilnené pomocou najmodernejších technológií, aby boli zabezpečené proti útokom a neoprávnenému prístupu k systémom a údajom z dôvodu ich zraniteľnosti.

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

- **Popis všetkých rozhraní a polí s prenášanými osobnými údajmi**





Všetky rozhrania s inými IT procesmi musia byť zaznamenané. Príslušná

dokumentácia musí obsahovať aspoň nižšie uvedené informácie:

Všetky polia s osobnými údajmi

Smerovanie prenosu (import/export)

Účel prenosu

IT procesy/rozhrania, do ktorých sú údaje exportované

Typ autentizácie používané rozhraním

Ochrana prenosu (napr. šifrovanie)

Najmä musia byť popísané importné a exportné rozhrania zo súborov a do nich, spolu so spôsobom, akým je zabezpečené ich užívanie pomocou technických a organizačných opatrení. Rovnakým spôsobom ako rozhranie musia byť popísané aj migrácie dát.

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

- **Zabezpečené uchovávanie údajov**

Za účelom zaistenia čo najväčšej úrovne ochrany pri uchovávaní osobných údajov musí byť vytvorený systém na uchovávanie dát v zašifrovanom formáte. To isté platí aj pre akékoľvek zálohy dát.

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

- **Zabezpečené uchovávanie na mobilných dátových nosičoch**

Uchovávanie údajov na mobilných dátových nosičoch nie je povolené z dôvodu vysokého rizika straty dát. Ak je to však nevyhnutné, musia byť údaje na mobilných dátových nosičoch uchovávané v zašifrovanom formáte. Akékoľvek údaje, ktoré nie je potrebné týmto spôsobom uchovávať, musia byť bezodkladne vymazané v súlade s pravidlami na ochranu osobných údajov. Používaný hardware musí byť zabezpečený proti strate/odcudzeniu (pomocou káblových zámkov, vhodných uzamykateľných prepravných kontajnerov apod.)

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

- **Proces zhromažďovania a odstraňovania údajov**

Musí byť vytvorený a popísaný proces na zhromažďovanie, odstraňovanie, zničenie alebo vymazávanie údajov na dátových nosičoch a iných médiách v neelektronickej forme. V interných organizačných predpisoch a pokynoch musia byť popísané pravidlá a postupy pre zabezpečené zhromažďovanie a interné predávanie,

uchovávanie i zničenie nosičov s ohľadom na typické vlastnosti daných nosičov. Zničenie alebo vymazanie dátových nosičov musí byť v súlade s pravidlami na ochranu údajov včas vykonané na príslušnej pracovnej stanici, aby sa v podstatnej miere zamedzilo ukladanie dát na dočasných úložiskách. Týmto spôsobom je takisto obmedzený počet osôb, ktoré s dátovými nosičmi pracujú, a tým je zvýšené zabezpečenie. Za účelom vylúčenia alternatívnych metód odstraňovania dátových nosičov je potrebné vykonať príslušné organizačné kroky. Zamestnanci budú



o týchto skutočnostiach pravidelne informovaní.

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

- **Zavedenie metód na vymazávanie a zničenie údajov v súlade s predpismi na ochranu údajov**

*Z bezpečnostných dôvodov musia byť nezašifrované dátové nosiče predtým, než sú znovu použité na interné účely (napr. pri zmene primárneho užívateľa) alebo predané externým stranám, vymazané v súlade s pravidlami na ochranu údajov. Formátovanie je nevhodným spôsobom pre bezpečné vymazanie dát. Musia byť vybrané iné bezpečné metódy na vymazanie/zničenie dát, ktoré rekonštrukciu dát v maximálnej miere sťažia.*

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

- **Vedenie evidencie o vymazaní údajov**

*V súlade s pravidlami na ochranu údajov musia byť vedené príslušné záznamy o akomkoľvek procese úplného a trvalého vymazania údajov a dátových nosičov s osobnými údajmi. Záznamy musia byť uchovávané po dobu najmenej 12 mesiacov vo forme umožňujúcej ich kontrolu.*

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

- **Odvzdávanie dátových médií**

*Z bezpečnostných dôvodov musia byť nezašifrované údaje pred ich predaním tretím osobám vždy vymazané v súlade s pravidlami na ochranu údajov.*

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

- **Zákaz reprodukcie údajov**

*Akákoľvek (elektronická a/alebo analógová) reprodukcia údajov, dátových nosičov alebo dokumentov Zákazníka nie je povolená, pokiaľ to nie je výslovnou súčasťou plnenia zadanej úlohy. V takom prípade môžu byť vytvorené kópie iba pre účely vymedzené Zákazníkom, a to iba v nevyhnutnom rozsahu. Elektronický prenos prostredníctvom napr. emailu sa taktiež považuje za druh reprodukcie.*

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

- **Externé nosiče**

*K systémom Zákazníka na spracúvanie údajov je zakázané pripájať externé (odpojiteľné) dátové nosiče (USB, pamäťové karty, CD/DVD atď.), ako aj kopírovať údaje Zákazníka na externé (odpojiteľné) dátové nosiče, pokiaľ to nie je výslovnou súčasťou plnenia zadanej úlohy a nebolo schválené k tomu oprávneným manažérom príslušného oddelenia Zákazníka.*

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

## **Nakladanie s dokumentami obsahujúcimi osobné údaje**

- **Externé nosiče – papierové dokumenty**

*Tlač a kopírovanie dokumentov obsahujúcich osobné údaje musí byť fyzicky riadený autorizovanými užívateľmi, aby bolo zaistené, že žiadne dokumenty*



obsahujúce osobné údaje nezostanú ponechané v zariadeniach pre tlač či kopírovanie. Dokumenty obsahujúce osobné údaje musia byť klasifikované ako

„Dôverné“ a prenášané môžu byť iba v uzavretom nosiči (napr. kontajner, obálka), ktorý obsahuje označenie autorizovanej osoby, ktorej má byť dokument doručený.

Autorizovaná osoba je povinná zaistiť (napr. aplikáciou politiky čistého stolu), aby nedošlo k zneužitiu dokumentu obsahujúceho osobné údaje na jej pracovnom mieste a zaistiť bezpečné uloženie dokumentu, aby nemohlo dôjsť k neoprávnenému prístupu k osobným údajom (napr. uloženie v uzamykateľnej skrini, trezore).

Po opadnutí účelu spracovania musia byť papierové dokumenty obsahujúce osobné údaje, a to podľa výberu zákazníka, predané Zákazníkovi alebo zničené, či znehodnotené takým spôsobom, aby nebolo možné osobné údaje z dokumentu obnoviť (napr. skartácia).

### Kontrola pracovných postupov

Pravidlá ustanovia: „...zaistiť, aby osobní údaje spracúvané prijímcami/sprostredkovateľmi boli spracúvané výlučne v súlade s pokynmi prevádzkovateľa (kontrola pracovných postupov).

#### • Pravidlá a obmedzenia týkajúce sa plnenia zákaziek

Budú vykonané iba pracovné činnosti uvedené v pripravenom popise služby. Všetky ďalšie činnosti, ktoré sú nad rámec takého rozsahu, musia byť predom prerokované so zodpovedným zástupcom Zákazníka a písomne schválené. Dodávateľ je povinný koordinovať so Zákazníkom v predstihu harmonogram prác vykonávaných menom Zákazníka.

Dodávateľ je povinný Zákazníka bez zbytočného odkladu informovať o akýchkoľvek prípadoch vážneho prerušenia prevádzky a o akomkoľvek podozrení o porušení predpisov upravujúcich ochranu údajov, pokiaľ v priebehu spracúvania údajov Zákazníka dôjde k akejkoľvek chybe či iným nezrovnalostiam. Dodávateľ je povinný akékoľvek také problémy bezodkladne napraviť.

Po ukončení zmluvného vzťahu musia byť všetky výsledky práce a údaje, dokumenty a prijaté zariadenia na údržbu predané späť dohodnutým spôsobom.

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

#### • Subdodávateľa

V prípade, že Zákazník schválil využitie subdodávateľov (externí dodávateľia/poskytovatelia služieb), musia byť subdodávateľa dôkladne vybraní, druh a rozsah nimi poskytovaných služieb musí byť zjednaný v rámci subdodávateľského zmluvného vzťahu, ktorý musí byť v súlade s právnymi predpismi upravujúcimi ochranu osobných údajov a vykonávanie činností a poskytovania služieb musí byť kontrolované tak, aby bolo v súlade so zmluvnými dohodami so Zákazníkom. Výsledky týchto kontrol musia byť písomne zdokumentované a na požiadanie predložené Zákazníkovi. Právo Zákazníka na priamu kontrolu tým nie je nijak dotknuté.

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

#### • Rozdelenie úloh



Rozdelenie úloh medzi Zákazníka a Dodávateľa na jednej strane a Dodávateľa a subdodávateľa na druhej strane musí byť písomne špecifikované ešte pred zahájením príslušnej činnosti, pokiaľ nevyplýva z už uzavretých zmlúv.

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

- **Odobranie/Vrátenie údajov pri skončení zmluvného vzťahu**

Pri skončení zmluvného vzťahu musia byť výsledky práce, dokumenty a prevzaté zariadenia predané späť zjednaným spôsobom.

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

- **Zmeny konfigurácie**

Vykonávanie zmien konfigurácie zariadení alebo systémov Zákazníka nie je povolené, pokiaľ k takým zmenám nebol v rámci zákazky daný výslovný písomný súhlas. Ak bol súhlas daný, musia byť také zmeny predom odsúhlasené s príslušným oddelením a ich vykonanie musí byť spätne overiteľné na základe náležitej dokumentácie.

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

### **Kontrola dostupnosti**

Pravidlá ustanovia: "...zaistiť ochranu osobných údajov proti náhodnému zničeniu či strate (zabezpečenie dostupnosti údajov)";

- **Koncepcia zálohovania**

Údaje musia byť pravidelne zálohované, aby bolo zaistené, že budú dostupné aj

v prípade mimoriadnych alebo krízových situácií. Za týmto účelom bude vytvorená koncepcia zálohovania dát, vďaka ktorej budú oprávnení zamestnanci môcť využívať v prípade mimoriadnych situácií všetky dostupné prostriedky na zaistenie obnovy dát v primeranom čase po vzniku mimoriadnej udalosti.

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

- **Krízový plán**

Zákazník musí byť bezodkladne informovaný v prípade akejkoľvek poruchy (ako sú napr. úmyselné interné či externé útoky) alebo prerušenia spracúvania údajov. V prípade zistenia akejkoľvek známky poruchy musia byť bezodkladne učinené všetky príslušné kroky vedúce k minimalizácii škody a k zamedzeniu vzniku akejkoľvek ďalšej škody. Na tieto účely musí byť vytvorený krízový plán s podrobným popisom príslušných krokov, ktoré je nevyhnutné vykonať, a s uvedením osôb, ktoré musia byť o incidente informované, a to najmä na strane Zákazníka.

Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy. ☒

### **Kontrola zamýšľaného použitia**

Pravidlá ustanovia: "...zaistiť, aby údaje zhromaždené pro rôzne účely boli spracúvané oddelene (pravidlo oddeleného spracúvania údajov).";

- **Minimalizácia objemu zhromaždených údajov**



*Je potrebné zaistiť, aby bol zhromažďovaný, uchovávaný a spracúvaný iba taký objem údajov, ktorý je nevyhnutný k dosiahnutiu daného účelu alebo vykonania danej pracovnej úlohy či procesu. Tento účel nesmie byť v priebehu spracúvania*

*v žiadnom následnom kroku menený, a to ani pri prenose.*

*Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy.* ☒

- **Oddelené spracúvanie**

*Za účelom zaistenia, aby údaje a/alebo dátové nosiče používané na rôzne zmluvné účely boli spracúvané (zaznamenávané, upravované, vymazávané a prenášané apod.) a/alebo uchovávané oddelene, je nevyhnutné zdokumentovať a aplikovať príslušné pravidlá a opatrenia.*

*Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy.* ☒

## **Organizačná kontrola**

- **Implementácia školiacich opatrení**

*Všetky osoby, ktoré prichádzajú do styku s osobnými údajmi alebo ktoré sa iným spôsobom podieľajú na spracúvaní údajov (ako napr. v prípade zmluvného využitia služieb spoločností zaisťujúcich údržbu alebo likvidáciu údajov), musia byť preukázateľne inštruované v nižšie uvedených oblastiach:*

- **Zásady ochrany údajov, vrátane technických a organizačných opatrení;**

*požiadavka zachovania mlčanlivosti, dôvernosti údajov a dôvernosti informácií týkajúcich sa danej spoločnosti a obchodných tajomstiev, vrátane transakcií Zákazníka;*

*riadne a bezpečné používanie údajov, dátových nosičov a iných dokumentov;*

- **Dôvernosť elektronických komunikácií**

*iné špecifické povinnosti týkajúce sa zachovania dôvernosti, ak sú nevyhnutné;*

*iné špecifické informácie, ktoré môžu vyplývať zo zmluvného vzťahu alebo z tohto zoznamu minimálnych požiadaviek, ak sú nevyhnutné.*

*Školenie musí byť vykonané prostredníctvom vhodných opatrení a pravidelne opakované aspoň raz za dva roky alebo, ak je to nevyhnutné, v kratších intervaloch (napr. pri zmene zákazky alebo právnych predpisov).*

*Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy.* ☒

- **Oddelenie a pridelovanie funkcií**

*Oddelenie funkcií musí byť definované, zdokumentované a vysvetlené, napr. aké funkcie sa nemôžu navzájom kombinovať, a teda nemôžu byť vykonávané rovnakou osobou v rovnaký okamih. Príslušné požiadavky môžu vyplývať zo samotnej úlohy, z požiadaviek stanovených zmluvou alebo z právnych predpisov. V zásade nie je možné kombinovať výkonné funkcie s kontrolnými funkciami. Potom, čo bude definované požadované oddelenie funkcií, budú funkcie pridelené príslušným osobám.*





*Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy.* ☒

- **Interné kontroly**

*Musia byť zaznamenávané všetky transakcie čítania, zadávania, zmien a výmazu/anonymizácie (ID užívateľa, podrobnosti transakcie).*

*Interné kontroly v priestoroch dodávateľa zaistia, aby záznamy o prístupoch k osobným údajom boli pravidelne (minimálne však raz za dva mesiace) analyzované. Všetky nezrovnalosti musia byť zdokumentované. Zákazník o nich musí byť bezodkladne písomne vyrozumieť a záznamy o nich musia byť uchovávané po dobu troch mesiacov od dokončenia príslušnej zákazky alebo činnosti.*

*Splnenie požiadavky je záväznou podmienkou podľa tejto zmluvy.* ☒