Smlouva o zpracování osobních údajů

Tato Smlouva o zpracování osobních údajů ("**Smlouva**") se uzavírá mezi:

(1) **Oborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví**, se sídlem Praha 4, Roškotova 1225/1, PSČ 140 00, IČO: 47114321, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl A, vložka 7232 („**Správce**") na straně jedné;

a

(2) **Gappex s.r.o.**, se sídlem Na Cimbále 104/2, Modřany, 143 00 Praha 4, IČO: 06835732, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 289441 („**Zpracovatel**") na straně druhé;

(Správce a Zpracovatel dále společně jako „**Smluvní strany**” a každá jednotlivě jako „**Smluvní strana**”).

PREAMBULE

Vzhledem k tomu, že:

Správce a Zpracovatel uzavřeli Smlouvu o dílo a o poskytování služeb „Implementace Service Desk a ITIL procesů“ ev. č. 2023/SML/0202 (dále jen „**Smlouva o dílo a o poskytování služeb**") ohledně poskytování služeb v rozsahu v ní uvedených; a v souvislosti s poskytováním služeb dle Smlouvy o dílo a o poskytování služeb bude Zpracovatel zpracovávat osobní údaje pro Správce v rozsahu a za účelem uvedeným v této Smlouvě;

Smluvní strany ujednaly následující:

1. PŘEDMĚT SMLOUVY

Správce a Zpracovatel uzavřeli Smlouvu o dílo a o poskytování služeb týkající se služeb, které bude poskytovat Zpracovatel za úplatu pro Objednatele (dále jen „**Služby**"). Veškeré parametry těchto Služeb jsou definovány ve Smlouvě o dílo a o poskytování služeb a jejích přílohách.

Zpracovatel bude v souvislosti se Smlouvou o dílo a o poskytování služeb zpracovávat Osobní údaje pro Správce výhradně za účelem poskytování Služeb v rozsahu ujednaném podle Smlouvy o dílo a o poskytování služeb, konkrétně za účelem řádného a včasného poskytnutí SW řešení Implementace Service Desk a ITIL procesů a služeb s tím souvisejících (dále jen „**Účel**").

Smluvní strany se tímto dále dohodly, že Zpracovatel bude pro Správce zpracovávat Osobní údaje, jak jsou definovány v čl. 2 této Smlouvy, výhradně za Účelem, způsobem a na základě doložených pokynů a podmínek Správce a v souladu s nimi tak, jak vyplývají z této Smlouvy a Smlouvy o dílo a o poskytování služeb. V případě jakéhokoliv rozporu mezi ustanoveními této Smlouvy a ustanoveními Smlouvy o dílo a o poskytování služeb má přednost tato Smlouva.

2. ROZSAH ZPRACOVÁVANÝCH OSOBNÍCH ÚDAJŮ

Zpracovatel bude na základě Smlouvy o dílo a o poskytování služeb zpracovávat pro Správce osobní údaje týkající se zaměstnanců Správce, případně dalších fyzických osob - uživatelů využívajících Service Desk (dále jen jako „**Subjekty osobních údajů**").

Zpracovavatel bude na základě Smlouvy o dílo a o poskytování služeb u Subjektů osobních údajů zpracovávat pro Správce následující typy osobních údajů:

- jméno, příjmení, osobní číslo zaměstnance nebo jiný identifikátor fyzické osoby, e-mailová adresa, telefon. (dále společně jen jako „**Osobní údaje**").

Osobní údaje budou Zpracovatelem zpracovávány a ukládány na serverech umístěných.

Pokud Zpracovatel zpracovává na základě výslovného pokynu Správce osobní údaje, které tato Smlouva výslovně neuvádí, budou tyto nové osobní údaje zpracovávány za stejných podmínek.

3. DOBA ZPRACOVÁNÍ

Tato Smlouva je podepisovaná současně se Smlouvou o dílo a o poskytování služeb a je účinná až do splnění všech povinností v souvislosti s ukončením zpracování dle této Smlouvy. Údaje o osobách a jimi absolvovaných kurzech budou archivovány Zpracovatelem po celou dobu trvání Smlouvy o dílo a o poskytování služeb a dále do té doby, dokud tyto údaje kompletně nepředá po ukončení Smlouvy o dílo a o poskytování služeb dle pravidel tam uvedených, leda by Správce informoval Zpracovatele o nutnosti prodloužit tuto dobu např. s ohledem na pravidla pro skartaci těchto záznamů danou interními pravidly Správce.

4. ZABEZPEČENÍ ZPRACOVATELE

Zpracovatel se zavazuje přijmout všechna potřebná technická a organizační opatření k zajištění odpovídající bezpečnosti Osobních údajů, k zamezení nahodilého nebo neoprávněného přístupu k Osobním údajům, jejich pozměňování, zničení nebo ztrátě, neoprávněnému přenosu nebo jinému neoprávněnému zpřístupnění nebo zpracování předávaných Osobních údajů. Pro tyto účely Zpracovatel přijme technické a organizační opatření ujednané v Příloze č. 1 této Smlouvy.

Zpracovatel je povinen poskytnout svým zaměstnancům a ostatnímu personálu, který se podílí na zpracování Osobních údajů, přiměřené pokyny pro jejich zpracování, zejména ohledně povinnosti Zpracovatele dodržovat mlčenlivost ve vztahu ke všem Osobním údajům nebo důvěrným informacím, které zpracovává na základě této Smlouvy, a dále poskytnout svým zaměstnancům a ostatnímu personálu dostatečné pokyny k technickým a organizačním bezpečnostním opatřením přijatým pro ochranu a zabezpečení Osobních údajů Správce.

Zpracovatel je povinen zavázat dohodou o mlčenlivosti své zaměstnance, aby dodržovali povinnost mlčenlivosti ve vztahu ke všem Osobním údajům nebo důvěrným informacím, jako i k dodržování požadavků a norem Zpracovatele v souvislosti s poskytováním Služeb za účelem zpracování Osobních údajů pro Správce na základě této Smlouvy. Nedodržení těchto zásad, norem nebo požadavků opravňuje Správce k jednostranné výpovědi této Smlouvy ke dni zjištění porušení povinnosti Zpracovatele. Správce může požádat Zpracovatele o předložení důkazů k ověření výše uvedených skutečností. Tímto ujednáním není dotčena náhrada újmy nebo smluvní pokuta v souladu s příslušnými ustanoveními Dohody o mlčenlivosti.

5. POVINNOSTI ZPRACOVATELE

Zpracovatel se zavazuje zpracovávat Osobní údaje v souladu s platnými a účinnými právními předpisy.

Zpracovatel má povinnost poskytnout Správci požadovanou součinnost při plnění Účelu této Smlouvy, ochraně Osobních údajů před jakýmkoli zneužitím nebo neoprávněným přístupem a dodržováním příslušných právních předpisů při zpracování Osobních údajů.

Za účelem plnění této Smlouvy poskytne Zpracovatel Správci bez zbytečného odkladu veškerou požadovanou součinnost k usnadnění povinností Správce při zpracování Osobních údajů podle platných a účinných právních předpisů včetně, nikoliv však výlučně:

- při plnění Správcovy povinnosti reagovat na žádosti o výkon práv Subjektů osobních údajů podle nařízení Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), (dále jen „**Nařízení**“);
- při přijímání vhodných technických a organizačních opatření k zajištění úrovně bezpečnosti odpovídající možným rizikům při zpracování Osobních údajů podle této Smlouvy.

V případě, že Správce požaduje spolupráci nebo součinnost podle tohoto článku, je Správce povinen písemně oznámit Zpracovateli veškeré své požadavky k součinnosti nebo spolupráci a doložit je přesnými pokyny.

Zpracovatel je povinen zpracovávat Osobní údaje pouze v rozsahu, po dobu a k Účelu stanoveným touto Smlouvou, nebo pouze na základě písemných pokynů Správce.

Zpracovatel se zavazuje, že neposkytne Osobní údaje třetí straně, a to ani pro nekomerční účely vyjma případů, kdy takové poskytnutí vyžadují platné a účinné právní předpisy nebo Správce dal předem k poskytnutí výslovný písemný souhlas.

Zpracovatel se zavazuje, že nepředá Osobní údaje do země, která není členem EU, vyjma případů, kdy Správce předem poskytne písemný souhlas s předáním. V takovém případě je Zpracovatel dále povinen splnit veškeré požadavky na bezpečnostní opatření odpovídající platným předpisům o ochraně osobních údajů a/nebo pokynům Správce.

Zpracovatel je povinen umožnit Správci během běžné pracovní doby Zpracovatele provést v sídle Zpracovatele kontrolu dodržování povinností týkajících se zpracování Osobních údajů vyplývajících z této Smlouvy, a to i po ukončení stanovené doby zpracování, tj. po ukončení této Smlouvy, a to po dobu 6 měsíců. Správce písemně oznámí Zpracovateli provedení kontroly podle tohoto odstavce nejpozději 5 dnů před jejím provedením. Zpracovatel následně na vlastní náklady zpřístupní Správci veškeré informace nezbytné k prokázání plnění svých povinností podle této Smlouvy a poskytne Správci přiměřený přístup ke všem prostorům, zařízením a záznamům, které umožní Správci provedení ověřovací kontroly s přiměřeným dohledem předem určeného zástupce Zpracovatele, který bude zodpovědný, aby byla kontrola prováděna v rozsahu a v souladu s podmínkami této Smlouvy a Smlouvy o dílo a o poskytování služeb.

Zpracovatel se zavazuje, že bude řádně a bez prodlení odpovídat na veškeré dotazy ze strany Správce a Úřadu pro ochranu osobních údajů ohledně jakéhokoli Narušení bezpečnosti, jak je definováno v čl. 7 této Smlouvy, nebo jakéhokoli jiného aspektu zpracování nebo ochrany osobních údajů. Zpracovatel se také zavazuje řádně a bez prodlení odpovídat na veškeré dotazy související s chybami nebo problémy se změnami nebo aktualizacemi Osobních údajů, které vznese dotčený Subjekt osobních údajů, a které jsou nebo byly zpracovávány Zpracovatelem. Zpracovatel má povinnost notifikovat Správce do 24 hodin od obdržení jakéhokoli předvolání, soudního příkazu nebo správního příkazu vládním nebo správním orgánem, který požaduje přístup k Osobním údajům nebo jejich zveřejnění. V takových případech má Zpracovatel povinnost umožnit Správci, aby na vlastní náklady provedl ochranné opatření proti předvolání, soudnímu příkazu nebo správnímu příkazu, přičemž poskytne Správci veškerou potřebnou součinnost.

Zpracovatel neprodleně notifikuje Správce o jakýchkoli překážkách při plnění této Smlouvy a o veškerých okolnostech týkajících se závažného porušení povinností Zpracovatele ohledně zpracování a ochrany Osobních údajů stanovenými touto Smlouvou. Zpracovatel je dále povinný neprodleně poskytnout Správci veškerou součinnost k odstranění překážek a/nebo případnému zabránění nebo nápravě porušení povinností Zpracovatele.

Po ukončení zpracování Osobních údajů podle této Smlouvy je Zpracovatel povinen poskytnout Správci všechna zařízení obsahující Osobní údaje, pokud je to možné, a vymazat všechny zpracovávané Osobní údaje ze všech svých systémů nebo databází, včetně vymazání všech záložních kopií s výjimkou, kdy uchovávání vyžaduje právní předpis, nebo k tomu dal písemný souhlas Správce.

6. PODDODAVATELÉ PRO ZPRACOVÁNÍ

Zpracovatel ke zpracování Osobních údajů může zapojit poddodavatele pouze za následujících podmínek:

- na základě předchozího písemného souhlasu Správce za předpokladu, že zapojení poddodavatele je při poskytování Služeb souvisejících se zpracováním Osobních údajů nezbytně nutné a Zpracovatel zároveň předložil Správci veškeré informace o totožnosti poddodavatele, včetně míst zpracování;
- Zpracovatel uzavře s poddodavatelem smlouvu, zajišťující dodržování stejných podmínek a povinností ujednaných touto Smlouvou a Smlouvou o dílo a o poskytování služeb, zejména povinnost mlčenlivosti, zajištění bezpečnosti při zpracování Osobních údajů a poskytnutí dostatečných záruk pro zavedení stejných technických a organizačních opatření poddodavatelem;
- smlouva mezi Zpracovatelem a poddodavatelem uvedena v předchozím odstavci může být sjednaná výhradně na dobu určitou nepřesahující dobu účinnosti této Smlouvy.

Zpracovatel odpovídá za zpracování Osobních údajů poddodavatelem stejně, jako by Zpracovatel zpracoval Osobní údaje samostatně. Zpracovatel odpovídá Správci za to, že jeho poddodavatelé budou plnit povinnosti vyplývající z této Smlouvy a Nařízení a je ve všech případech plně odpovědný za následky jednání a opomenutí svých zaměstnanců, zástupců a poddodavatelů, které vedou k jakémukoli nesouladu nebo porušení ustanovení této Smlouvy.

7. NARUŠENÍ BEZPEČNOSTI OSOBNÍCH ÚDAJŮ

Narušení bezpečnosti osobních údajů znamená jakýkoli bezpečnostní incident zahrnující skutečné, předpokládané nebo potenciální ohrožení důvěrnosti, integrity nebo dostupnosti Osobních údajů nebo sítě, systémů nebo databází, na kterých jsou Osobní údaje uloženy, přenášeny nebo zpracovávány, včetně jakéhokoli nahodilého, neoprávněného, nepovoleného nebo protiprávního zničení, použití, získávání, ukládání, prohlížení, pořizování kopií, ztráty, krádeže, změně, zpřístupnění zveřejněním nebo přístupu k Osobním údajům (dále jen „**Narušení bezpečnosti**").

Při Narušení bezpečnosti Zpracovatel notifikuje bez zbytečného odkladu Správce a v každém jednotlivém případě nejpozději do 72 hodin po zjištění Narušení bezpečnosti způsobené Zpracovatelem, jeho zaměstnanci a/nebo poddodavateli a poskytne Správci podrobný popis Narušení bezpečnosti, kategorie a typ Osobních údajů, které byly předmětem Narušení bezpečnosti, identitu každého dotčeného Subjektu osobních údajů a veškeré další informace,

které může Správce nebo Úřad pro ochranu osobních údajů důvodně požadovat v souvislosti s dotčenými Subjekty osobních údajů a Narušením bezpečnosti.

Zpracovatel se zavazuje, že neprodleně a na vlastní náklady provede opatření potřebné k: (a) vlastnímu vyšetření Narušení bezpečnosti; (b) identifikaci, předcházení a zmírnění účinků jakéhokoli Narušení bezpečnosti; (c) poskytnutí přiměřené součinnosti Správci při oznamování Narušení bezpečnosti Úřadu pro ochranu osobních údajů a/nebo dotčeným Subjektům osobních údajů; a (d) k nápravě Narušení bezpečnosti. Před jakýmkoli zveřejněním nebo sdělením třetí osobě o výše uvedených oznámeních a/nebo podáních, sděleních, notifikacích nebo tiskových zprávách souvisejících s jakýmkoli Narušením bezpečnosti (dále jen „**Oznámení o narušení**"), je Zpracovatel povinen obdržet písemný souhlas Správce, a to v případě kdy (i) může být Správce konkrétně jmenován nebo odkazován v souvislosti s Oznámením o narušení; (ii) jsou zapojeny nebo ovlivněny Osobní údaje a/nebo systémy Správce; (iii) Oznámení o narušení je zaměřeno na Subjekty osobních údajů; nebo (iv) Správce má nebo může mít určité nezávislé právní, smluvní nebo jiné závazky v důsledku Narušení bezpečnosti.

Zpracovatel se dále zavazuje, že bude řádně a bez prodlení odpovídat na veškeré dotazy ze strany Správce, Úřadu pro ochranu osobních údajů, vládních orgánů nebo správních orgánů, a poskytovat nezbytnou součinnost, pokud jde o jakékoli Narušení bezpečnosti. Zpracovatel je povinen poskytnout Správci na jeho žádost a nejpozději do 24 hodin od doručení této žádosti informace o stavu Narušení bezpečnosti, a to i opakovaně až do doby odstranění stavu Narušení bezpečnosti nebo zjednání nápravy. Oznámení o narušení a každé jiné oznámení nebo notifikace s tím související bude Správci poskytnuto na jeho e-mailovou adresu ve lhůtě nejméně 2 dny při předpokládaném ohrožení nebo Narušení bezpečnosti, a nejvíce 24 hodin po dni, kdy k Narušení bezpečnosti skutečně došlo.

Správce je povinen Zpracovatele bezodkladně informovat, v případě, že zjistí nebo předpokládá Narušení bezpečnosti, které může ovlivnit poskytování Služeb Zpracovatele v jakémkoli rozsahu. Oznámení musí být Zpracovateli poskytnuto na jeho e-mailovou adresu ve lhůtě nejméně 2 dny při předpokládaném ohrožení nebo Narušení bezpečnosti, a nejvíce 24 hodin po dni, kdy k Narušení bezpečnosti skutečně došlo.

Zpracovatel uhradí Správci veškeré náklady, ztráty, způsobenou újmu a výdaje, které se vztahují nebo jsou výsledkem jakéhokoli Narušení bezpečnosti na straně Zpracovatele nebo jakéhokoli jiného porušení závazků Zpracovatele podle této Smlouvy. Výše uvedené zahrnuje mimo jiné také náklady na Oznámení o narušení, služby pro styk s veřejností a další krizová opatření a/nebo konzultační, účetní nebo auditorské náklady týkající se nebo vyplývající z vyšetřování a opatření Správce k Narušení bezpečnosti a/nebo pokuty uložené Správci Úřadem pro ochranu osobních údajů v souvislosti s jednáním nebo opomenutím povinností Zpracovatele podle této Smlouvy a/nebo platných a účinných právních předpisů vztahujících se k ochraně osobních údajů.

8. SMLUVNÍ POKUTA

Pokud Zpracovatel poruší jakoukoli povinnost podle této Smlouvy, je Zpracovatel povinen uhradit smluvní pokutu Správci ve výši 250 000,- Kč za každé jednotlivé porušení. Smluvní pokuta je splatná do 15 dnů ode dne doručení žádosti o platbu zaslané Správcem na základě tohoto ustanovení.

Zaplacením smluvní pokuty, jak je popsána v předchozím odstavci výše, není dotčeno právo Správce požadovat náhradu újmy způsobenou porušením ustanovení této Smlouvy.

9. ZÁVĚREČNÁ USTANOVENÍ

Tato Smlouva může být měněna pouze formou písemných dodatků. Práva a povinnosti ujednané touto Smlouvou nejsou převoditelná bez předchozího písemného svolení druhé Smluvní strany.

Tato Smlouva je vyhotovena ve 2 stejnopisech. Každá Smluvní strana obdrží po 1 stejnopise.

Tato Smlouva se řídí právem České republiky. K řešení sporů vyplývajících z této Smlouvy nebo v souvislosti s ní jsou příslušné obecné soudy České republiky.

V Praze dne dle elektronického podpisu

Za Oborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví

_____

V Praze dne dle elektronického podpisu

Za Gappex s.r.o.

_____

Příloha č. 1

TECHNICKÉ A ORGANIZAČNÍ OPATŘENÍ OCHRANY A BEZPEČNOSTI OSOBNÍCH ÚDAJŮ

1. POVINNOSTI ZPRACOVATELE

Zpracovatel je povinen:

(a) zabránit jakémukoli neoprávněnému přístupu k Osobním údajům a k způsobům jejich zpracování;

(b) zabránit neoprávněnému prohlížení, vytváření, pořizování kopií, přenášení, změnám nebo výmazům záznamů, které obsahují Osobní údaje;

(c) přijmout opatření umožňující s přesností určit a ověřit kdy, kým a z jakého důvodu byly Osobní údaje zpracovávány; a

(d) stanovit pravidla určující podmínky přístupu a dalšího zpracování Osobních údajů.

V případě automatizovaného zpracování Osobních údajů je Zpracovatel povinen:

(e) zajistit, že systémy pro automatizované zpracování Osobních údajů jsou používány jenom oprávněnými osobami;

(f) zajistit, aby fyzické osoby oprávněné k používání systémů automatizovaného zpracování Osobních údajů měly přístup jen k Osobním údajům odpovídajícím jejich oprávnění a jen na základě specifických uživatelských oprávnění konkrétního uživatele založeného výlučně pro tyto osoby;

(g) vytvářet elektronické záznamy umožňující určení a ověření toho, kdy, kým a z jakého důvodu byly Osobní údaje zaznamenány nebo zpracovávány; a

(h) předcházet jakémukoli neoprávněnému přístupu k datovým nosičům nebo serverům.

2. ZVLÁŠTNÍ OPATŘENÍ ZPRACOVATELE K ZAJIŠTĚNÍ OCHRANY OSOBNÍCH ÚDAJŮ

Fyzický přístup

Zpracovatel má zaveden bezpečnostní standard fyzické ostrahy, který má zabránit neoprávněnému fyzickému přístupu do prostor a k zařízením Zpracovatele. Toho je dosaženo následujícími způsoby, příkladně:

- fyzický přístup do prostor Zpracovatele je omezen na jeho zaměstnance, poddodavatele a ohlášené návštěvy;
- zaměstnancům, poddodavatelům a ohlášeným návštěvám se vydává identifikační průkaz, který je nutné mít v prostorách Zpracovatele fyzicky u sebe;
- monitorování přístupu do prostor Zpracovatele, včetně přístupu k zařízením s uloženými Osobními údaji a do míst zpracování na základě oprávnění;
- udržování kontrolního záznamu o přístupu do prostor Zpracovatele.

Řízení přístupů a jejich správa

Zpracovatel má zavedeny následující standardy pro řízení přístupu a správu IT prostředí s ohledem na zabezpečení zpracovávaných osobních údajů:

- účty s oprávněním Správce by měly být používány jenom pro potřeby administrátorské činnosti;
- každý účet s oprávněním Správce je vysledovatelný k jedinečně identifikovatelnému jednotlivci;
- veškerý přístup k počítačům a serverům musí být ověřen v rámci pracovního zařazení zaměstnance;
- počáteční hesla musí být uživatelem změněna při prvním použití;
- zobrazení hesel musí být maskované nebo jinak zakryté tak, aby neoprávněné strany nebyly schopny je pozorovat nebo je následně obnovit;
- hesla musí být při jejich přenosu nebo uložení v databázi šifrovaná;
- složitost hesla by nikdy neměla být menší než 3 ze 4 tříd znaků a musí mít volby třídy znaků, jako jsou velká písmena, malá písmena, číslice nebo speciální znaky;
- délka hesla musí být nakonfigurována tak, aby obsahovala nejméně 12 znaků;
- hesla musí vypršet každých 90 dnů;
- automatizovaný časový limit přístupu uživatele k počítačům a serverům, tj. v případě nečinnosti uživatele je požadováno heslo pro obnovení přístupu;
- účty musí být nastaveny na zablokování po třech chybných pokusech o přihlášení.

Zabezpečení proti virům

Počítače a servery mají přiměřeně aktuální verze softwaru zabezpečení, který může obsahovat firewall, antivirovou ochranu a aktualizované databáze a definice virů. Tento software je nakonfigurován tak, aby vyhledával a okamžitě odstranil nebo opravil zjištěné nálezy virů.

Zpracovatel uchovává v systému softwaru zabezpečení protokol detekce neoprávněného vniknutí, který monitoruje, zjišťuje a hlásí vzory zneužití, podezřelé činnosti, neoprávněně přihlášené uživatele a další bezpečnostní rizika.

Personál Zpracovatele

Zaměstnanci a případní poddodavatelé Zpracovatele jsou vyškoleni v zásadách ochrany a bezpečnosti osobních údajů a seznámili se s jejich odpovědností v oblasti ochrany soukromí a bezpečnosti.

Zaměstnanci a případní poddodavatelé Zpracovatele jsou smluvně zavázáni k zachování důvěrnosti Osobních údajů Správce nebo jiných důvěrných informací a dodržování příslušných zásad, norem nebo požadavků Zpracovatele v souvislosti se zpracováním Osobních údajů. Nedodržení těchto zásad, norem nebo požadavků bude předmětem šetření, které může vést k disciplinárním opatřením nebo ukončení pracovního poměru ze strany Zpracovatele.