

PŘÍLOHA Č. 3

SMLOUVY O NÁVRHU, VÝVOJI, IMPLEMENTACI A SPRÁVĚ INFORMAČNÍHO SYSTÉMU
 PORTÁLU SLUŽEB SFDI

OCHRANA OSOBNÍCH ÚDAJŮ



# ÚVODNÍ USTANOVENÍ

## V souvislosti s plněním Smlouvy může docházet ke zpracování Osobních údajů Poskytovatelem (dále jen „**Zpracovatel**“) ve smyslu článku 4 bod 2) GDPR pro Objednatele (dále jen „**Správce**“). Pro zamezení pochybnostem Správce a Zpracovatel dále společně jako Smluvní strany anebo každý samostatně jako Smluvní strana.

## Smluvní strany mají zájem na tom dostát všem povinnostem, které jim vyplývají z (i) GDPR a (ii) Zákona o zpracování ZZOÚ a (iii) z této Přílohy č. 3 [*Ochrana osobních údajů*].

## Na základě článku 28 GDPR je Správce povinen uzavřít se Zpracovatelem písemnou smlouvu o zpracování osobních údajů, ve které Zpracovatel mimo jiné poskytne dostatečné záruky o technickém a organizačním zabezpečení ochrany Osobních údajů. Příloha č. 3 [*Ochrana osobních údajů*] tvoří podmínky zpracovatelské smlouvy dle čl. 28 GDPR.

## Smluvní strany mají zájem na tom, aby tato Příloha č. 3 [*Ochrana osobních údajů*] ve spojení se Smlouvou pokrývaly veškeré činnosti zpracování osobních údajů, které Zpracovatel provádí pro Správce v souvislosti anebo na základě Smlouvy. Účelem této Přílohy č. 3 [*Ochrana osobních údajů*] je stanovení rozsahu povinností Zpracovatele souvisejících především se zajištěním ochrany Osobních údajů při jejich zpracování. V případě rozporu opatření dle této Přílohy č. 3 [*Ochrana osobních údajů*] ve vztahu k Osobním údajům s opatřeními pro bezpečnost informací dle Smlouvy, mají přednost opatření pro bezpečnost informací dle Smlouvy.

## Zpracovatel bude pro Správce zpracovávat Osobní údaje koncových uživatelů IS PORTÁL SLUŽEB SFDI či osob evidovaných v IS PORTÁL SLUŽEB SFDI, příp. další Osobní údaje, které Správce získal nebo získá jako zaměstnavatel, objednatel anebo nadřízený orgán v roli správce Osobních údajů svých zaměstnanců, dodavatelů, spolupracovníků podřízených organizací a jiných subjektů anebo které pro Správce za tímto účelem získá samotný Zpracovatel ve smyslu článku 4 bod 2) GDPR („**Subjekty údajů\_2**“).

# předmět přílohy

## Předmětem této Přílohy č. 3 [*Ochrana osobních údajů*] Smlouvy je vymezení vzájemných práv a povinností Smluvních stran při zpracování Osobních údajů.

## Tato Příloha č. 3 Smlouvy dále stanoví rozsah Osobních údajů, které mají být zpracovávány, účel jejich zpracování a podmínky a záruky na straně Zpracovatele ohledně zajištění technického a organizačního zabezpečení Osobních údajů.

## Smluvní strany se zavazují dále postupovat v souladu s touto Přílohou č. 3 Smlouvy za účelem splnění povinnosti dle GDPR a ZZOÚ a zabezpečení ochrany Osobních údajů zpracovávaných Smluvními stranami.

# Účel, rozsah a doba zpracování osobních údajů

## Za účelem plnění předmětu Smlouvy je Zpracovatel oprávněn Osobní údaje v nezbytném rozsahu získávat, shromažďovat, zaznamenávat, uspořádávat a prohlížet je, jakož s nimi vykonávat i další operace, které jsou nezbytné k plnění předmětu Smlouvy zejména operace spočívající v migraci dat, testování úspěšnosti provedené migrace, testování počítačového programu, odstraňování Incidentů apod.

## Zpracovatel bude dle této Přílohy č. 3 [*Ochrana osobních údajů*] zpracovávat kategorie Osobních údajů Subjektů údajů uvedené v příloze A této Přílohy č. 3 [*Ochrana osobních údajů*].

## V případě, že Správce Zpracovateli poskytne nebo Zpracovateli budou jinak v souvislosti s plněním předmětu Smlouvy zpřístupněny i jiné Osobní údaje Subjektů údajů\_2 nebo Osobní údaje jiných subjektů údajů, je Zpracovatel povinen zpracovávat a chránit i tyto Osobní údaje v souladu s požadavky vyplývajícími (i) z GDPR, (ii) ze ZZOÚ a (iii) z této Přílohy č. 3 [*Ochrana osobních údajů*] Smlouvy.

## Správce prohlašuje a uzavřením Smlouvy potvrzuje, že zpracovává Osobní údaje Subjektů údajů\_2 v souladu s platnými a účinnými právními předpisy upravujícími ochranu osobních údajů, anebo v souladu se souhlasem Subjektů údajů\_2.

## Osobní údaje Subjektů údajů bude Zpracovatel zpracovávat nejdéle po dobu trvání Smlouvy. Povinnosti Zpracovatele týkající se ochrany Osobních údajů se Zpracovatel zavazuje plnit po celou dobu účinnosti Smlouvy, pokud ze Smlouvy nevyplývá, že mají trvat i po zániku její účinnosti.

# Odměna za zpracování osobních údajů

## Za zpracování Osobních údajů dle této Přílohy č. 3 [*Ochrana osobních údajů*] Smlouvy nenáleží Zpracovateli zvláštní odměna, resp. odměna je zahrnuta v rámci úplaty za plnění dle Smlouvy, tj. v rámci ceny Služeb. Zpracovateli rovněž nevzniká nárok na náhradu jakýchkoliv nákladů, které mu v souvislosti se zpracováním Osobních údajů dle této Přílohy č. 3 [*Ochrana osobních údajů*] Smlouvy vzniknou.

# Práva a povinnosti Zpracovatele

## Zpracovatel je při zpracování Osobních údajů povinen postupovat s náležitou odbornou péčí tak, aby nezpůsobil nic, co by mohlo představovat porušení GDPR, zejména článků 24, 25 a 32 GDPR ve spojení s článkem 28 GDPR, nebo porušení ZZOÚ.

## Pokud by Zpracovatel zjistil, že Správce porušuje povinnosti vyplývající pro něj z GDPR, je Zpracovatel ve smyslu článku 28 odst. 3 druhého pododst. GDPR povinen neprodleně Správce o této skutečnosti některým ze způsobů uvedených ve Smlouvě informovat.

## Zpracovatel je povinen řídit se při zpracování Osobních údajů na základě této Přílohy č. 3 [*Ochrana osobních údajů*] Smlouvy doloženými pokyny Správce. Zpracovatel je povinen písemně upozornit Správce bez zbytečného odkladu na nevhodnou povahu pokynů, jestliže Zpracovatel mohl tuto nevhodnost zjistit při vynaložení veškeré odborné péče. Zpracovatel je v takovém případě povinen pokyny provést pouze na základě písemného požadavku Správce.

## Zpracovatel je v souladu s článkem 82 GDPR povinen dbát, aby žádný Subjekt údajů\_2 neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a také dbát na ochranu před neoprávněným zasahováním do soukromého a osobního života Subjektů údajů\_2.

## Jakmile pomine účel, pro který byly Osobní údaje zpracovány, zejména v případě zániku Smlouvy, v případě odvolání souhlasu Subjektu údajů\_2, nebo na základě oprávněné žádosti Subjektu údajů\_2 dle článku 17 GDPR, je Zpracovatel ve smyslu článku 28 odst. 3 písm. g) Nařízení povinen na základě a v souladu s pokyny Správce předat Správci takové Osobní údaje v souladu se Servisní smlouvou nebo provést výmaz takových Osobních údajů dle volby Správce.

## V případě, že se kterýkoli Subjekt údajů bude domnívat, že Správce nebo Zpracovatel provádí zpracování jeho Osobních údajů, které je v rozporu s ochranou soukromého a osobního života Subjektu údajů\_2 nebo v rozporu se zákonem či GDPR, zejména budou-li dle Subjektu údajů\_2 Osobní údaje nepřesné s ohledem na účel jejich zpracování, a tento Subjekt údajů\_2 ve smyslu článku 15 GDPR požádá Zpracovatele o vysvětlení, opravu nebo o odstranění vzniklého stavu dle článku 16 GDPR nebo výmaz Osobních údajů dle článku 17 GDPR, zavazuje se Zpracovatel o tom neprodleně informovat Správce způsobem dle Smlouvy.

## Zpracovatel je povinen Správci neprodleně oznámit provedení kontroly ze strany ÚOOÚ a poskytnout Správci na jeho žádost podrobné informace o průběhu kontroly a kopii kontrolního protokolu. V případě zahájení správního řízení o uložení opatření k nápravě anebo uložení pokuty („**Správní řízení**“) je Zpracovatel rovněž povinen tuto skutečnost neprodleně oznámit Správci a poskytnout Správci na jeho žádost podrobné informace o průběhu a výsledcích Správního řízení, popř. Správci poskytnout plnou moc k nahlížení do spisu týkajícího se Správního řízení. Zpracovatel je povinen plnit povinnosti přezkoumávaného při provádění přezkumu ve smyslu článku 58 GDPR či kontrolované osoby dle zákona č. 255/2012 Sb., o kontrole (kontrolní řád), ve znění pozdějších předpisů, a zavazuje se poskytnout Správci kopii zprávy o odstranění nebo prevenci nedostatků zjištěných kontrolou/přezkumem, pokud je tato zpráva vypracována nebo může být na vyžádání Zpracovatele či Správce vypracována.

## Zpracovatel je povinen informovat Správce o každém případu ztráty či úniku Osobních údajů, neoprávněné manipulace s Osobními údaji nebo jiného porušení zabezpečení Osobních údajů („**Porušení zabezpečení osobních údajů**“), a to bez zbytečného odkladu, nejpozději do čtyřiadvaceti (24) hodin od vzniku Porušení zabezpečení osobních údajů nebo i pouhé hrozby, jestliže Zpracovatel mohl o tomto Porušení zabezpečení osobních údajů či i o hrozbě vzniku Porušení zabezpečení osobních údajů vědět při vynaložení veškeré odborné péče. Nemohl-li Zpracovatel zjistit případ skutečného či hrozícího Porušení zabezpečení osobních údajů před uplynutím lhůty dle předchozí věty tohoto bodu, informuje Správce nejpozději do čtyřiadvaceti (24) hodin od okamžiku, kdy se o vzniku Porušení zabezpečení osobních údajů nebo jeho hrozbě Zpracovatel dozví. Zpracovatel je i po poskytnutí informace Správci povinen být maximálně nápomocen při řešení Porušení zabezpečení osobních údajů, resp. při přijímání opatření ke zmírnění možných nepříznivých dopadů a zabránění vzniku obdobných situací v budoucnu.

## Zpracovatel se zavazuje být Správci nápomocen při zajišťování povinností dle GDPR, především povinnosti zabezpečit zpracování Osobních údajů, ohlašovat případy Porušení zabezpečení osobních údajů, zajištění posouzení vlivu na ochranu Osobních údajů či předchozí konzultace s ÚOOÚ, a to při zohlednění povahy zpracování a informací, jež má Zpracovatel k dispozici.

## Zpracovatel se zavazuje být Správci nápomocen při plnění jeho povinnosti reagovat na žádosti o výkon práv Subjektů údajů\_2, zejména na žádost na přístup k Osobním údajům, na opravu či výmaz Osobních údajů, na omezení zpracování či na přenositelnost Osobních údajů.

## Zpracovatel se zavazuje poskytnout Správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti zpracování Osobních údajů včetně zpracování prostřednictvím Dalších zpracovatelů (jak je tento pojem definován níže), a umožnit audity, včetně inspekcí, prováděné Správcem nebo jiným auditorem, kterého Správce pověří, a k těmto auditům přispěje.

## Informace dle bodu 5.8 této Přílohy č. 3 [*Ochrana osobních údajů*] Smlouvy musí minimálně obsahovat:

### popis povahy daného případu Porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených Subjektů údajů\_2 a kategorií a přibližného množství dotčených záznamů Osobních údajů;

### popis pravděpodobných důsledků Porušení zabezpečení osobních údajů;

### popis opatření, která Zpracovatel přijal nebo navrhl k přijetí s cílem vyřešit dané Porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

# Záruky technického a organizačního zabezpečení ochrany Osobních údajů

## Zpracovatel se zavazuje, že ve smyslu článku 32 GDPR přijme s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob veškerá technická a organizační opatření k zabezpečení ochrany Osobních údajů způsobem uvedeným v GDPR a ZZOÚ či jiných závazných právních předpisech k vyloučení možnosti neoprávněného nebo nahodilého přístupu k Osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití Osobních údajů. Tato povinnost platí i po ukončení zpracování Osobních údajů.

## Zpracovatel se zavazuje, že přijme zejména, nikoliv však výlučně, následující organizační a technická opatření:

### aniž by byl dotčen bod 6.3 této Přílohy č. 3 [*Ochrana osobních údajů*], Zpracovatel v případě zpracování Osobních údajů prostřednictvím vlastních zaměstnanců pověří touto činností pouze své vybrané zaměstnance a členy realizačního týmu, které zaváže povinností mlčenlivosti ohledně Osobních údajů a zaváže dodržovat další povinnosti, které jsou povinni dodržovat tak, aby nedošlo k porušení GDPR či této Přílohy č. 3 [*Ochrana osobních údajů*], a to například v rámci interního předpisu Zpracovatele, dohodě o mlčenlivosti či v pracovní smlouvě zaměstnance;

### bude používat odpovídající technické zařízení a programové vybavení způsobem, který vyloučí neoprávněný či nahodilý přístup k Osobním údajům ze strany jiných osob než pověřených osob Zpracovatele ve smyslu bodu 6.2.1 této Přílohy č. 3 [*Ochrana osobních údajů*];

### bude Osobní údaje uchovávat v náležitě zabezpečených objektech a místnostech;

### Osobní údaje v elektronické podobě bude uchovávat na zabezpečených serverech nebo na nosičích dat, ke kterým budou mít přístup pouze pověřené osoby Zpracovatele ve smyslu bodu 6.2.1 této Přílohy č. 3 [Ochrana osobních údajů] na základě přístupových kódů či hesel, a bude Osobní údaje pravidelně zálohovat, pokud takové zálohy neprovádí Správce v souladu se Smlouvou nebo Interními předpisy;

### zabezpečí dálkový přenos Osobních údajů buď pouze prostřednictvím veřejně nepřístupné sítě, nebo prostřednictvím zabezpečeného přenosu po veřejných sítích;

### písemné dokumenty obsahující Osobní údaje bude uchovávat na zabezpečeném místě, přičemž bude vést řádnou evidenci o pohybu takových písemných dokumentů;

### bude v co největší míře zpracovávat pouze pseudonymizované a šifrované Osobní údaje, je-li takové opatření vhodné a nezbytné ke snížení rizik plynoucích ze zpracování Osobních údajů;

### zabezpečí neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;

### prostřednictvím vhodných technických prostředků zabezpečí schopnost obnovit dostupnost Osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;

### zabezpečí pravidelné testování posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování;

### při ukončení zpracování Osobních údajů zabezpečí Zpracovatel dle dohody se Správcem výmaz Osobních údajů, nebo tyto Osobní údaje předá Správci viz bod 5.5 této Přílohy č. 3 [Ochrana osobních údajů]; a

### bude dodržovat další technická a organizační opatření uvedená v Interních předpisech, technických normách a pravidlech, které Správce za tímto účelem předá Zpracovateli.

## Zpracovatel je oprávněn pověřit zpracováním Osobních údajů dalšího zpracovatele (dále jen „**Další zpracovatel**“), a to pouze s předchozím písemným souhlasem Správce. Zpracovatel tak informuje Správce o veškerých Dalších zpracovatelích, které zamýšlí pověřit zpracováním Osobních údajů, o veškerých zamýšlených změnách týkajících se přijetí Dalších zpracovatelů nebo jejich nahrazení a poskytne tak Správci příležitost vyslovit vůči přijetí těchto Dalších zpracovatelů námitky. Mimo Další zpracovatele, vůči kterým Správce nic nenamítal, Zpracovatel nesvěří zpracování osobních údajů žádné třetí osobě. Další zpracovatel musí být zároveň Poddodavatelema splňovat podmínky stanovené pro Poddodavatele dle Smlouvy.

## Pokud Zpracovatel zapojí ve smyslu bodu 6.3 Přílohy č. 3 [*Ochrana osobních údajů*] Dalšího zpracovatele, aby provedl určité činnosti zpracování, musí být tomuto Dalšímu zpracovateli uloženy na základě smlouvy alespoň stejné povinnosti na ochranu Osobních údajů, jaké jsou uvedeny v této Příloze č. 3 [*Ochrana osobních údajů*], a to zejména poskytnutí dostatečných záruk, pokud jde o zavedení vhodných technických a organizačních opatření tak, aby zpracování splňovalo požadavky GDPR a ZZOÚ. Neplní-li Další zpracovatel své povinnosti v oblasti ochrany údajů, odpovídá Správci za plnění povinností dotčeného Dalšího zpracovatele i nadále plně Zpracovatel.

## Zpracovatel je povinen zavést a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany Osobních údajů v souladu s GDPR, ZZOÚ a jinými právními předpisy.

# Povinnosti po zániku Smlouvy

## Zpracovatel je po zániku Smlouvy povinen dodržovat veškeré povinnosti dle GDPR a ZZOÚ, zejména předejít jakémukoliv neoprávněnému nakládání s Osobními údaji do doby, než dle pokynů Správce a v souladu se Smlouvou tyto Osobní údaje Zpracovatel předá Správci nebo provede jejich výmaz.

## Povinnost zachování důvěrné povahy Osobních údajů včetně mlčenlivosti o bezpečnostních opatřeních zabezpečujících ochranu Osobních údajů trvá i po ukončení Smlouvy.

# Posouzení vlivu na ochranu Osobních údajů

## Pokud Správce na základě provedení posouzení vlivu na ochranu osobních údajů podle článku 35 GDPR dojde k závěru, že je nezbytné provést další opatření v této Příloze č. 3 [*Ochrana osobních údajů*] anebo Smlouvě nestanovené, je Zpracovatel povinen taková opatření provést a obě Smluvní strany takovou změnu promítnou změnou této Přílohy č. 3 [*Ochrana osobních údajů*] anebo Smlouvy prostřednictvím dodatku k této Smlouvě. Zpracovatel se zavazuje poskytnout veškerou součinnost nezbytnou k formulaci obsahu takového dodatku a bez vlivu na cenu Služeb uzavřít takový dodatek do třiceti (30) dnů ode dne zaslání výzvy Správce k uzavření takového dodatku. Obdobně se Smluvní strany zavazují postupovat v případě rozhodnutí ÚOOÚ o přijetí vzorových smluvních klauzulí o ochraně osobních údajů nebo kodexu chování. Zpracovatel se zavazuje na potřebu změny Přílohy č. 3 [*Ochrana osobních údajů*] Správce upozornit.

# Závěrečná ustanovení

## Jakékoliv doplňky či změny této Přílohy č. 3 [*Ochrana osobních údajů*] s výjimkou změny Přílohy A musí být učiněny formou vzestupně číslovaných písemných dodatků podepsaných oprávněnými zástupci obou Smluvních stran. Rozsah zpracovávaných Osobních údajů včetně kategorie Subjektů údajů\_2 nebo místa zpracování uvedena v Příloze A může Správce rozšířit či jinak změnit při zachování písemné formy i bez nutnosti uzavírat dodatek této Přílohy č. 3 [*Ochrana osobních údajů*] (oznámení o změně Přílohy A doručené Zpracovateli prostřednictvím e-mailu bude dostačující).

## Příloha A tvoří nedílnou součást Přílohy č. 3 [*Ochrana osobních údajů*].

**Příloha A**

**Rozsah zpracovávaných Osobních údajů**

| **Kategorie Subjektů údajů** | **Kategorie Osobních údajů** |
| --- | --- |
| Klient SFDI | **jméno, příjmení, adresa bydliště, datum narození (výjimečně), telefonní a elektronický kontakt, AIFO číslo** |
| Třetí osoba (osoba uvedená na projektové dokumentaci, rozhodnutí či jiné doprovodné dokumentaci) | **Jméno, příjmení, pracovní pozice, telefonní a elektronický kontakt, sken podpisu** |
| Zaměstnanec SFDI | **jméno, příjmení, pracovní pozice, telefonní a elektronický kontakt, čísla certifikátů (JIP-KAAS)** |
| Zaměstnanec CENDIS | **jméno, příjmení, pracovní pozice, telefonní a elektronický kontakt, čísla certifikátů (JIP-KAAS)** |
|  |  |
|  |  |

**Místa zpracování**

|  |  |
| --- | --- |
|  | **Adresa místa** |
| **Místo uchování**  | Uchování dat je dle umístění datacentra poskytovatele Microsoft Azure – West Europe, skládá se ze 3 geograficky oddělených datacenter v rámci Nizozemska. |
| **Místa zpracování**  | Zpracování bude probíhat v cloudu MS Azure (komponenty Azure DevOps, KeyVaults, Storage accounty, SQL database, Azure Backup, Log Analytics)  |