

PŘÍLOHA Č. 3

SMLOUVA O PROVOZU A ROZVOJI

INFORMAČNÍHO SYSTÉMU ELEKTRONICKÉ DÁLNIČNÍ ZNÁMKY

OCHRANA OSOBNÍCH ÚDAJŮ



# ÚVODNÍ USTANOVENÍ

## Smluvní strany mají zájem na tom dostát všem povinnostem, které jim vyplývají z (i) GDPR a (ii) ZZOÚ.

## Pro účely této Přílohy č. 3 Smlouvy a Smlouvy vystupuje Objednatel, jakožto objednatel plnění ze Smlouvy, v roli správce Osobních údajů Subjektů údajů.

## Poskytovatel vystupuje z pohledu ochrany osobních údajů v roli zpracovatele zpracovávajícího Osobní údaje Subjektů údajů.

## Tato Příloha č. 3 Smlouvy upravuje veškeré vztahy, v rámci kterých Poskytovatel zpracovává Osobní údaje Subjektů údajů.

## Veškeré pojmy, které jsou v této Příloze č. 3 Smlouvy uvozeny velkým počátečním písmenem a zároveň nejsou v této Příloze č. 3 Smlouvy blíže specifikovány, mají význam jim přisuzovaný Smlouvou.

# předmět přílohy

## Předmětem této Přílohy č. 3 Smlouvy je vymezení vzájemných práv a povinností Smluvních stran při zpracování a ochraně 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 Poskytovatele 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 Poskytovatelem.

# Účel, rozsah a doba zpracování osobních údajů

## Objednatel pověřuje Poskytovatele zpracováním Osobních údajů, které Poskytovatel získává za účelem plnění předmětu Smlouvy.

## Za účelem plnění předmětu Smlouvy je Poskytovatel 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 při zachování zásady minimalizace zpracování Osobních údajů.

## Poskytovatel bude dle této Přílohy č. 3 Smlouvy zpracovávat Osobní údaje Subjektů údajů v rozsahu daném předmětem plnění Smlouvy dle čl. 3 Smlouvy. Jedná se zejména o následující kategorie Osobních údajů:

### státní poznávací značka;

### další údaje dle § 21a odst. 4 písm. b) až e) ZPK zapisované do IS EDAZ při činnosti Poskytovatele dle této Smlouvy v souvislosti se zpracováním kategorie Osobních údajů dle předchozího bodu;

### případně další kategorie Osobních údajů související se zpracováním Osobních údajů v rámci předmětu plnění Smlouvy.

## V případě, že Objednatel Poskytovateli poskytne nebo Poskytovateli budou jinak v souvislosti s plněním předmětu Smlouvy zpřístupněny i jiné Osobní údaje nebo osobní údaje jiných subjektů údajů, je Poskytovatel povinen zpracovávat a chránit i tyto osobní údaje, stejně jako Osobní údaje vyjmenované v bodě 3.3 této Přílohy č. 3 Smlouvy, v souladu s požadavky vyplývajícími (i) z GDPR, (ii) ze ZZOÚ a (iii) z této Přílohy č. 3 Smlouvy.

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

# Odměna za zpracování osobních údajů

## Smluvní strany se dohodly, že za zpracování Osobních údajů dle této Přílohy č. 3 Smlouvy nenáleží Poskytovateli zvláštní odměna, resp. že zpracování Osobních údajů dle této Přílohy č. 3 Smlouvy je již zohledněno v ceně plnění dle Smlouvy. Poskytovateli rovněž nevzniká nárok na náhradu jakýchkoliv nákladů, které mu v souvislosti se zpracováním Osobních údajů dle této Přílohy č. 3 Smlouvy vzniknou.

# Práva a povinnosti Poskytovatele

## Poskytovateli je při zpracování Osobních údajů povinen postupovat s náležitou odbornou péčí tak, aby nezpůsobil nic, co by mohlo představovat porušení GDPR a ZZOÚ.

## Pokud by Poskytovatel zjistil, že Objednatel porušuje povinnosti vyplývající pro něj z GDPR nebo ZZOÚ, je Poskytovatel ve smyslu článku 28 odst. 3 druhého pododst. GDPR povinen neprodleně Objednatele o této skutečnosti informovat.

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

## Poskytovatel je povinen dbát, aby žádný Subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a také dbá na ochranu před neoprávněným zasahováním do soukromého a osobního života Subjektů údajů.

## Jakmile pomine účel, pro který byly Osobní údaje zpracovány, zejména v případě zániku Smlouvy, nebo na základě oprávněné žádosti Subjektu údajů dle článku 17 GDPR, je Poskytovatel povinen na základě a v souladu s pokyny Objednatele provést likvidaci Osobních údajů nebo tyto Osobní údaje předat Objednateli.

## V případě, že se kterýkoli Subjekt údajů bude domnívat, že Objednatel nebo Poskytovatel provádí zpracování jeho Osobních údajů, které je v rozporu s ochranou soukromého a osobního života Subjektu údajů nebo v rozporu se zákonem, zejména budou-li Osobní údaje nepřesné s ohledem na účel jejich zpracování, a tento Subjekt údajů požádá Poskytovatele o vysvětlení nebo o odstranění vzniklého stavu, zavazuje se Poskytovatel o tom neprodleně informovat Objednatele.

## Poskytovatel je nápomocen Objednateli při plnění jeho povinnosti reagovat na žádosti o výkon práv Subjektů údajů, zejména na žádost na přístup k Osobním údajům, na opravu či výmaz Osobních údajů, na omezení zpracování či na přenositelnost Osobních údajů.

## Poskytovatel je od nabytí účinnosti Smlouvy povinen informovat Objednatele 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 Poskytovatel mohl o tomto Porušení zabezpečení osobních údajů či i o hrozbě vzniku Porušení zabezpečení osobních údajů vědět při vynaložení veškeré odborné péče. Nemohl-li Poskytovatel zjistit případ skutečného či hrozícího Porušení zabezpečení osobních údajů před uplynutím lhůty dle předchozí věty tohoto bodu 5.8 této Přílohy č. 3 Smlouvy, informuje Objednatele nejpozději do čtyřiadvaceti (24) hodin od okamžiku, kdy se o vzniku Porušení zabezpečení osobních údajů nebo jeho hrozbě Poskytovatel dozví. Poskytovatel je i po poskytnutí informace Objednateli 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.

## Informace dle předchozího bodu 5.8 této Přílohy č. 3 Smlouvy musí minimálně obsahovat:

### popis povahy daného případu Porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených Subjektů údajů 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.

## Poskytovatel se zavazuje být Objednateli 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 Poskytovatel k dispozici.

## Poskytovatel se zavazuje poskytnout Objednateli 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 Objednatelem nebo jiným auditorem, kterého Objednatel pověří, a k těmto auditům přispěje.

# Záruky technického a organizačního zabezpečení ochrany Osobních údajů

## Poskytovatel 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 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.

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

### víceúrovňový firewall;

### antivirovou ochranu a kontrolu neoprávněných přístupů;

### přístup k osobním údajům mají pouze pověřené osoby Poskytovatele; a

### aniž by byl dotčen bod 6.2.5 této Přílohy č. 3 Smlouvy, Poskytovatel v případě zpracování Osobních údajů prostřednictvím vlastních zaměstnanců pověří touto činností pouze své vybrané zaměstnance, které poučí o jejich povinnosti zachovávat mlčenlivost ohledně Osobních údajů, jakož i o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení Osobních údajů, a o dalších povinnostech, které jsou povinni dodržovat tak, aby nedošlo k porušení GDPR či této Přílohy č. 3 Smlouvy; ke zpracovávaným Osobním údajům budou mít přístup a zpracováním budou pověřeni pouze ti zaměstnanci Poskytovatele, do jejichž pracovní náplně spadají činnosti, jejichž předpokladem je zpracování Osobních údajů;

### nesvěří zpracování Osobních údajů jakékoliv třetí osobě bez předchozího konkrétního nebo obecného písemného povolení Objednatele. Objednatel tímto výslovně souhlasí s tím, aby Poskytovatel využil třetí osoby, a to Poddodavatele, jako další zpracovatele („**Další zpracovatel**“). Poskytovatel vždy předem informuje Objednatele o veškerých zvolených Dalších zpracovatelích, jakož i o všech zamýšlených změnách týkajících se přijetí Dalších zpracovatelů nebo jejich nahrazení, a poskytne tak Objednateli příležitost vyslovit vůči těmto změnám námitky;

### bude používat odpovídající technické zařízení a programové vybavení způsobem, který vyloučí neoprávněný či nahodilý přístup k Osobním údajům ze strany jiných osob než pověřených zaměstnanců Poskytovatele;

### 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 na základě přístupových kódů či hesel, a bude Osobní údaje pravidelně zálohovat;

### zajistí 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;

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

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

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

### zajistí bezpečnost zpracovávaných Osobních údajů při organizaci a řízení činností v oblasti informačních technologií, zejm. stanovením systému řízení, jednotlivých postupů, pravidelné údržby a kontrol, včetně plánů pro případ havárií;

### při ukončení zpracování Osobních údajů zajistí Poskytovatel dle dohody s Objednatelem bezpečnou fyzickou likvidaci Osobních údajů, nebo tyto Osobní údaje předá Objednateli;

### zálohy dat se provádějí do oddělené geografické lokality, data jsou šifrovaná během přenosu i po uložení a přístup k nim mají pouze pověřené osoby Poskytovatele.

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

## Pokud Poskytovatel zapojí ve smyslu bodu 6.2.5 této Přílohy č. 3 Smlouvy Dalšího zpracovatele, aby provedl určité činnosti zpracování, musí být tomuto Dalšímu zpracovateli uloženy na základě smlouvy stejné povinnosti na ochranu údajů, jaké jsou uvedeny v této Příloze č. 3 Smlouvy, a to zejména poskytnutí dostatečných záruk, pokud jde o zavedení vhodných technických a organizačních opatření tak, aby zpracování splňovalo požadavky GDPR a přinejmenším opatření uvedená v bodě 6.2 této Přílohy č. 3 Smlouvy (včetně zapojení Dalších zpracovatelů Dalšími zpracovateli). Neplní-li uvedený Další zpracovatel své povinnosti v oblasti ochrany údajů, odpovídá Objednateli za plnění povinností dotčeného Dalšího zpracovatele i nadále plně Poskytovatel.

## Poskytovatel poskytne Objednateli seznam Dalších zpracovatelů dle bodu 6.2.5 této Přílohy č. 3 Smlouvy (včetně případných Dalších zpracovatelů zapojených Dalšími zpracovateli) nejpozději do třiceti (30) dnů ode dne účinnosti Smlouvy a následně vždy bez zbytečného odkladu, nejpozději do třiceti (30) dnů od přijetí nového Dalšího zpracovatele.

## Identifikace subjektů bude prováděna pouze v části aplikace agendových funkcí IS EDAZ, která na základě ZPK bude v případě příjmu oznámení o osvobození provádět kontrolu, zdali provozovatel vozidla je oznamovatelem osvobození.

## Veškerá výměna dat a jejich přenosy budou probíhat šifrovanou formou. Přístupy Uživatelů a Interních uživatelů k datům budou zajištěny autorizací s příslušnou úrovní bezpečnosti. Přístupy a změny dat budou logovány a logy budou pravidelně kontrolovány v rámci bezpečnostního dohledu.

|  |  |
| --- | --- |
| Zabezpečení zpracování: | Data o identifikovaných vozidlech na zpoplatněné pozemní komunikaci budou šifrována a zároveň jejich integrita bude ochráněna prostředky asymetrické kryptografie, které zaručí nepopiratelnost a geografickou lokalizaci pořízených dat. |
| Doba uložení: | Evidence údajů na základě ZPK po dobu platnosti časového poplatku nebo po dobu trvání důvodů osvobození od zpoplatnění a následně ještě po dobu 2 let od doby, kdy pominula potřeba zpracování.  Evidence údajů na základě zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, po dobu minimálně 5 let.  Umožnění kontroly úhrady ze strany PČR nebo CSČR maximálně po dobu 72 hodin. |
| Právo na přístup: | Objednatel ve spolupráci s Provozovatelem na základě oprávněné elektronické nebo listinné žádosti poskytne subjektu informace o datech, která jsou zpracovávána v jeho kontextu. |
| Právo na opravu: | Objednatel ve spolupráci s Provozovatelem na základě oprávněné elektronické nebo listinné žádosti poskytne subjektu právo na opravu evidovaných informací, prokáže-li se jejich neshoda. Systém bude v pravidelných intervalech provádět synchronizaci dat z externích zdrojů (RSV, SEM) takovým způsobem, aby byla zachována co nejvyšší kvalita dat. |
| Právo na výmaz: | Uživatel/klient má právo na výmaz osobních údajů pouze za vymezených podmínek podle GDPR. |
| Právo na omezení zpracování: | Uživatel/klient má právo na omezení zpracovávání svých osobních údajů pouze za vymezených podmínek podle GDPR. |
| Právo na přenositelnost: | Nerelevantní – Subjekt údajů má právo na přenos údajů k jinému správci. Podle ZPK Výběr časového poplatku zajišťuje Státní fond dopravní infrastruktury. |
| Právo vznést námitku | Uživatel/klient má právo vznést kdykoliv námitku proti zpracování osobních údajů za vymezených podmínek podle GDPR. Zpracování těchto údajů není dále možné, pokud se neprokážou závažné oprávněné důvody pro zpracování. |
| Právo nebýt předmětem automatizovaného individuálního rozhodnutí, včetně profilování: | Subjekt údajů má právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro subjekt údajů právní účinky nebo se subjektu údajů obdobným způsobem významně dotýká. Při získávání informací z Registru silničních vozidel dochází k automatizovanému rozhodování a k profilování, avšak toto automatizované rozhodování a profilování je dovoleno ZPK. |

# Povinnosti po zániku Smlouvy

## Poskytovatel 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 Objednatele tyto Osobní údaje Poskytovatel předá Objednateli nebo provede jejich bezpečnou likvidaci.

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

# Závěrečná ustanovení

## V případě, pokud Objednatel 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 Smlouvy nestanovené, je Poskytovatel povinen taková opatření provést a obě Smluvní strany takovou změnu promítnou písemnou změnou této Přílohy č. 3 Smlouvy nejpozději do dvou (2) měsíců od provedení posouzení vlivu na ochranu osobních údajů, přičemž Poskytovatel se zavazuje na potřebu změny této Přílohy č. 3 Smlouvy Objednatele upozornit. Obdobně se Smluvní strany zavazují postupovat v případě rozhodnutí ÚOOÚ o přijetí vzorových smluvních klauzulí o ochraně osobních údajů nebo kodexu chování.

## Smluvní strany shodně konstatují, že v souvislosti s uzavřením Smlouvy a na jejím základě si Smluvní strany vzájemně předávají a i do budoucna budou předávat za účelem zajištění řádného plnění Smlouvy Osobní údaje kontaktních osob, které se podílejí nebo budou podílet na plnění Smlouvy, s uvedením jejich Osobních údajů: jméno, příjmení, titul, funkce, telefonický a e-mailový kontakt, u kterých právním důvodem pro jejich zpracování Smluvními stranami, jako správci těchto osobních údajů, je jejich oprávněný zájem na plnění Smlouvy, na kterém se v mezích své kompetence podílejí kontaktní osoby.

## V souvislosti s bodem 8.2 této Přílohy č. 3 se každá Smluvní strana zavazuje v rámci svých povinností, jako správce předaných Osobních údajů, zajistit, aby subjekty těchto údajů byly při poskytnutí Osobních údajů informovány dle článku 13 GDPR o zpracování poskytnutých Osobních údajů pro účel plnění Smlouvy, a že toto zpracování je v souladu s úpravou dle článku 6 odst. 1 písm. f) GDPR a dále aby Subjekty údajů byly informovány o svých právech v rozsahu, jak pro ně vyplývají z GDPR.