

Dohoda o zpracování dat (DoZD)
Ke smlouvě č. 184/2020 (číslo Dodavatele) ze dne 13.5.2020

mezi

Povodí Ohře, státní podnik

Sídlo: Bezručova 4219, 43003 Chomutov

IČO: 70889988

DIČ: CZ70889988

zastoupeným: Ing. Zbyňkem Folkem, generálním ředitelem

ve věcech smluvních: [REDACTED]

Zapsaným v OR vedeného u Krajského soudu v Ústí nad Labem pod spisovou značkou A 13052

- Dále uváděn jako **“Klient”** nebo **„Správce“** -

a

Mechanika Teplice, družstvo

Masarykova 31

415 22 Teplice

IČO 00556157

DIČ CZ00556157

zastoupena při podpisu smlouvy Josefem Hajným, předsedou představenstva

a Markétou Klímovou, členkou představenstva

Zapsané v OR Krajského soudu v Ústí nad Labem sp. zn. Dr 119

- Dále uváděn jako **“Dodavatel”** nebo **„Zpracovatel“** -

- souhrně jako **“Strany”** nebo **„smluvní strany“** -

Tato DoZD sjednává práva a povinnosti stran v souvislosti s ochranou dat zpracovávaných na základě Smlouvy o užívání aplikace TIS-Web ze dne 13.5.2020 (dále jako **“hlavní smlouva”**). DoZD se vztahuje na veškeré aktivity spojené s hlavní smlouvou, během kterých mají zaměstnanci dodavatele a/nebo třetích stran sjednaných dodavatelem přístup k datům poskytnutých klientem.

1. OBSAH A TRVÁNÍ SMLOUVY O ZPRACOVÁNÍ DAT

Dodavatel sbírá, zpracovává nebo užívá osobních informací výhradně v souladu s instrukcemi klienta. Dodavatel je zodpovědný za soulad opatření o ochraně dat s platnými právními předpisy EU, zejména Nařízením Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen GDPR) a platnými právními předpisy ČR, zejména zákonem č. 110/2019 Sb., o zpracování osobních údajů.

1.1 Podstata smlouvy o zpracování dat:



Podstata smlouvy o zpracování dat vychází z hlavní smlouvy uzavřené mezi smluvními stranami a jejím popisem služeb, pokud je dostupný. To zahrnuje plnění úkolů dodavatelem uvedených v hlavní smlouvě č. 184/2020, příloha 1.

1.2 Trvání:

Trvání smlouvy je určeno dle podmínek hlavní smlouvy.

Ukončení smlouvy bez předchozího oznámení:

Platnost této smlouvy končí zánikem resp. ukončením smlouvy hlavní. Způsoby zániku resp. ukončení smlouvy hlavní je upraveno ve smlouvě hlavní, která je přílohou k této smlouvě.

2. OBSAH SMLOUVY O ZPRACOVÁNÍ DAT

Dodavatel může sbírat, zpracovávat nebo užívat osobní údaje získané od klienta pouze v rozsahu daném smlouvou hlavní, k účelu stanovenému smlouvou hlavní a za podmínek uvedených v této smlouvě, a dle pokynů klienta (viz odstavec 8).

2.1 Rozsah, typ a účel smlouvy o zpracování dat:

Rozsah, typ a účel sběru, zpracování a/nebo užívání osobních údajů je odvozen z hlavní smlouvy. Ta obsahuje procedury zpracování dat uvedených v hlavní smlouvě č. 184/2020, příloha 1.

2.2 Typ dat:

Předmětem sběru, zpracování nebo užití jsou následující typy/kategorie osobních informací:

- Osobní data
- Kontaktní informace (jako telefon, e-mail)
- Data týkající se smlouvy (smluvní vztahy, produktové nebo smluvní zájmy)
- Historie zákazníka
- Fakturace a platební data o smlouvě
- Bankovní data (číslo účtu, IBAN)
- Plánovací a kontrolní data
- Data získaná od třetích stran, jako jsou veřejné registry atd.
- Speciální kategorie osobních dat

2.3 Datové subjekty:

Datové subjekty ovlivněné zacházením s osobními údaji obsahují následující kategorie osob:

- Zákazníci
- Zaměstnanci
- Dodavatelé
- Kontakty

2.4 Technická/organizační opatření:

Pokud není uvedeno v hlavní smlouvě, jsou technická a organizační opatření aplikovaná dodavatelem uvedena v příloze 1 této DoZD. Technická a organizační opatření jsou předmětem dalšího vývoje a úprav, a proto je dodavatel oprávněn implementovat adekvátní alternativní opatření. Případné změny bezpečnostních opatření budou uvedeny v dodatku této smlouvy.

3. PRÁVA DATOVÝCH SUBJEKTŮ – ÚPRAVY, ZAMEZENÍ ZPRACOVÁNÍ A SMAZÁNÍ DAT



- 3.1** Klient se podílí na zajištění ochrany práv datových subjektů a souladu příslušných právních závazků klienta, konkrétně v souvislosti s úpravami, smazáním a/nebo zamezení zpracování dat, upozorněním datových subjektů a poskytováním informací datovým subjektům.
- 3.2** Dodavatel může upravit, smazat nebo zamezit zpracování dat pouze v souladu s instrukcemi klienta. Pokud datový subjekt kontaktuje dodavatele, aby jeho data upravil, smazal nebo zamezil zpracování, zavazuje se dodavatel tuto žádost ihned klientovi předat a poskytnout mu součinnost v souvislosti s požadavkem datového subjektu.
- 3.3** Pokud je klient právně povinen podat informace ohledně sběru, zpracování nebo užití osobních údajů datovým subjektům nebo správním a jiným orgánům k jejich žádosti poskytne mu dodavatel součinnost, pokud:
- Klient požádá dodavatele, aby tak učinil v písemné formě a
 - Klient nese hotové finanční náklady vzniklé dodavateli v souvislosti s vykonáním této služby, tj. poplatky za poštovné, kolky apod.; dodavateli nevzniká nárok na úhradu takto dodavatelem poskytnuté služby

4. INSPEKCE A DALŠÍ ZÁVAZKY DODAVATELE:

Dodavatel rovněž odpovídá za splnění následujících závazků:

- 4.1** Ochrana utajení dat: Všechny osoby, které mají v rámci svých povinností přístup k osobním údajům klienta, musí být seznámeny s pravidly pro nakládání s osobními údaji dle Směrnice dodavatele vycházející z Nařízení GDPR.
- 4.2** Implementace a soulad se všemi nezbytnými technickými a organizačními opatřeními (viz také odstavec 2.4).
- 4.3** Schopnost ověřit přijatá technická a organizační opatření na základě klientova požadavku. Dodavatel může také odeslat současná prověření, hlášení nebo hlášení nezávislých subjektů (jako jsou auditoři, inspektoři, kontrolóři kvality, bezpečnostní experti), odpovídající certifikáty IT bezpečnosti nebo auditu ochrany dat.
- 4.4** Kontroly ve smyslu pravidelné inspekce prováděné dodavatelem, zahrnující provádění nebo plnění smluvního zpracování dat, konkrétně soulad s nezbytnými dodatky k nařízením a opatřením smluvního zpracování dat. Upozornění klienta na neshody a/nebo nedostatky zjištěné během kontrol.
- 4.5** Zajištění úplné písemné dokumentace týkající se sběru, zpracování nebo užití osobních údajů, na základě kterých může klient kdykoliv doložit právoplatnost zpracování dat.
- 4.6** Zajištění informací a dat nezbytných pro záznamy klienta ohledně zpracovávání dat; tyto informace musí být pouze na základě žádosti klienta a pouze v souvislosti se zpracováním dat prováděného dodavatelem v rámci této DoZD.
- 4.7** Zpracování a užití údajů bude probíhat výhradně v rámci České republiky, členského státu Evropské Unie nebo jiných zemí, které jsou součástí Evropského hospodářského prostoru. Jakýkoliv outsourcing do třetích zemí bude předmětem předchozího písemného schválení klientem. Pokud jsou zahrnuti subdodavatelé, aplikuje se tento požadavek k požadavkům v odstavci 5.



5. VZTAHY SUBDODAVATELŮ

5.1 Pokud zpracování nebo užití osobních údajů klienta zahrnuje subdodavatele, musí být splněny následující požadavky:

- Dodavatel musí subdodavatele pečlivě vybrat a zkontrolovat, zda je daný subdodavatel schopný plnit podmínky smlouvené mezi dodavatelem a klientem.
- Najmutí subdodavatele je povoleno pouze s předchozím písemným souhlasem klienta.
- Dodavatel musí smluvní podmínky mezi ním a subdodavatelem stanovit tak, aby byla zajištěna opatření ochrany dat aplikovaná ve smluvním vztahu mezi klientem a dodavatelem.

5.2 Služby získané dodavatelem jako pomocné služby podporující dodavatele v provádění smluvního zpracování údajů nejsou chápány jako subdodavatelský vztah ve smyslu tohoto článku smlouvy. Jde například o telekomunikační služby, údržba, úklidové služby, audity nebo likvidace datových médií. Dodavatel je nicméně povinen vypracovat vhodné a právně závazné dohody a přijmout kontrolní opatření k zajištění ochrany a bezpečnosti dat klienta, a to i s ohledem na pomocné služby prováděné třetími stranami.

6. KONTROLNÍ PRÁVA KLIENTA

6.1 Dodavatel je povinen na základě žádosti poskytnout klientovi veškeré potřebné informace nutné k ověření plnění povinností vztahujících se ke smluvnímu zpracování dat a s tím souvisejících osobních údajů a zpřístupnit mu relevantní certifikáty týkající se zabezpečení a zpracování dat a s tím souvisejících osobních údajů

7. UPOZORNĚNÍ NA NARUŠENÍ OSOBNÍCH ÚDAJŮ

7.1 Dodavatel nahlásí písemně každý případ narušení osobních údajů, za která jsou dodavatel, jeho zaměstnanci nebo subdodavatelé zodpovědní, klientovi na kontakt Mgr. Milan Kašpar, tel. 474636246, e-mail. kaspar@poh.cz.

7.2 Pokud je ztráta, nelegální převod nebo vyžazení osobních údajů možným rizikem pro práva a svobody fyzické osoby (datový subjekt), může vzniknout informační povinnost vůči dozorovému orgánu nebo přímo datovému subjektu. Klient tedy musí být informován o těchto případech bezodkladně bez ohledu na příčinu vzniku situace. To se také týká vážných narušení zpracovávacího procesu, podezření na porušení právních předpisů EU nebo ČR o ochranné osobních údajů, nebo dalších nepravdivostí při nakládání s osobními údaji klienta.

7.3 Ve spolupráci s klientem přijme dodavatel vhodná opatření k zajištění dat a k omezení potenciálně negativních důsledků pro datové subjekty. Pokud je klient povinen hlásit případy narušení bezpečností nakládání s osobními údaji dozorovému orgánu, je dodavatel povinen poskytnout klientovi nezbytnou součinnost.

8. KLIENTOVA PRAVOMOC K VYDÁVÁNÍ POKYNŮ

8.1 Osobní údaje jsou zprávně výhradně v rozsahu práv a povinností dodavatele dle hlavní smlouvy a v souladu s pokyny klienta. Klient si vyhrazuje právo vydávat pokyny ohledně typu, rozsahu a způsobu zpracování dat a případně poskytuje další podrobné instrukce dodavatelovi pro nakládání s osobními údaji klienta. Pokyny musí být činěny písemně. Pokud dodavatel odmítne řídit se pokyny klienta, musí tuto skutečnost obratem písemně sdělit klientovi, včetně



zdůvodnění, proč pokyn klienta odmítá vykonat. Trvá-li klient na svých pokynech i nadále, musí to dodavateli sdělit písemně; v takovém případě nese odpovědnost za případné škody takto vzniklé klient. Po dobu, než dodavatel obdrží potvrzení pokynů klientem, je oprávněn pozdržet vykonávání zpochybných pokynů.

- 8.2** Dodavatel může předat informace třetím stranám nebo datovým subjektům pouze s předchozím písemným souhlasem klienta.
- 8.3** Pokyny předané klientem ústně musí být jím bezodkladně potvrzeny písemnou formou (např. e-mailem). Dodavatel nesmí využít data pro žádný jiný účel, než který vyplývá z uzavřené hlavní smlouvy a pokynů klienta. Bez vědomí klienta nesmí vznikat žádné kopie nebo duplikáty. Toto se netýká záložních kopií, pokud jsou nezbytné pro zabezpečení řádného zpracování dat, a dat podléhajících archivační povinnosti.

9. ZVEŘEJNĚNÍ, SMAZÁNÍ DAT/NAVRÁCENÍ DATOVÝCH MÉDIÍ

- 9.1** Na žádost klienta, nebo po skončení smluvního vztahu dle hlavní smlouvy, je dodavatel povinen navrátit klientovi, nebo třetí straně označené písemně klientem, veškeré dokumenty které získal, datová média, veškeré zpracované výsledky a veškerá archivovaná data spojená se smluvním vztahem, nebo vzniklá jako smluvní zpracování dat. Tato povinnost také zahrnuje kopie a/nebo reprodukce datových médií a/nebo archivovaných dat. Dodavatel není oprávněn zadržovat tato data. Pokud by dodavatel z jakéhokoliv důvodu odmítl po ukončení smluvního vztahu data klientovi vydat, odpovídá za veškeré škody, které by klientovi v této souvislosti vznikly.
- 9.2** Po navrácení dat dle odstavce 8.1 nebo pokud si o jejich navrácení klient požádá, musí být veškerá zbývající data na straně dodavatele zničena nebo smazána dle nařízení o ochraně osobních údajů; před nezvratným zničením dat je nutné získat písemný souhlas klienta. Dodavatel musí poskytnout důkaz o provedení vymazání dat klientovi, pokud o to požádá, a to pomocí písemného prohlášení, ujištění nebo jiného dokumentu prokazujícího likvidaci dat. Klient nemusí požadovat zničení uložených dat, pokud je dodavatel legálně oprávněn taková data archivovat; tato data ale nemůže dodavatel nadále zpracovávat. Data namísto smazání nesmí být dále zpracována, pokud je to právně umožněno (například na základě specifické právní implementace zákona v dané zemi) a pokud není jejich vymazání možné z důvodu specifického typu archivování.
- 9.3** Dokumentace sloužící k prokázání řádného zpracování dat v souladu s touto DoZD a platnými právními předpisy musí být archivována dodavatelem i po skončení platnosti této DoZD a v souladu s archivačními podmínkami. Dodavatel se zproští veškeré odpovědnosti za řádné uchování a archivaci dat, pokud je po ukončení smluvního vztahu protokolárně předá klientovi.
- 9.4** Nařízení z odstavců 9.1 a 9.2 se vztahuje i na testovací a odpadní materiály.

10. POVINNOSTI KLIENTA

- 10.1** Klient je zodpovědný za dodržování opatření týkajících se ochrany osobních údajů, především za legálnost datových přenosů k Dodavateli.
- 10.2** Klient poskytne dodavateli včasné a plně informace, pokud zaznamená během kontroly výsledků zpracování dat jakékoliv problémy nebo nepravdivosti ve vztahu k opatřením o ochraně osobních údajů.
- 10.3** Klient vede záznamy o aktivitách v souvislosti se zpracováním dat.



11. ODPOVĚDNOST

11.1 Závazky o ochraně osobních údajů uvedených v této DoZD znamení významný závazek dodavatele uvedený v hlavní smlouvě vůči klientovi. S tímto ohledem je tato smlouva vnímána jako doplněk hlavní smlouvy.

12. VZTAH S HLAVNÍ SMLOUVOU, DALŠÍ ZÁVAZKY A OPATŘENÍ

12.1 Pokud by došlo ke ztrátě, zničení, zabavení dat klienta uložených u dodavatele, nebo data byla zabavena v rámci exekuce, insolvence či jiného jednání správního orgánu nebo došlo ke ztrátě, zničení, zabavení z důvodu jiných událostí nebo omezení třetími stranami, dodavatel okamžitě upozorní klienta (kontakt Mgr. Milan Kašpar, tel. 474636246, e-mail. kaspar@poh.cz). Dodavatel se zavazuje bezodkladně v případech uvedených v tomto odstavci vyznat zodpovědné strany, že má klient výhradní vlastnictví dat, datových médií, dokumentů atd.

12.2 Změny a/nebo dodatky k této DoZD jsou požadovány v písemné formě, aby byly platné. To také platí na případné zřeknutí se tohoto požadavku.

12.3 Opatření vyplývající z této smlouvy budou aplikována s ohledem na platné právní předpisy EU a ČR a místo působnosti.

12.4 Dodavatel bude zachovávat mlčenlivost o informacích a údajích, které budou předmětem zpracování.

13. ZÁVĚREČNÁ USTANOVENÍ

13.1 Tato smlouva se sjednává jako bezúplatná.

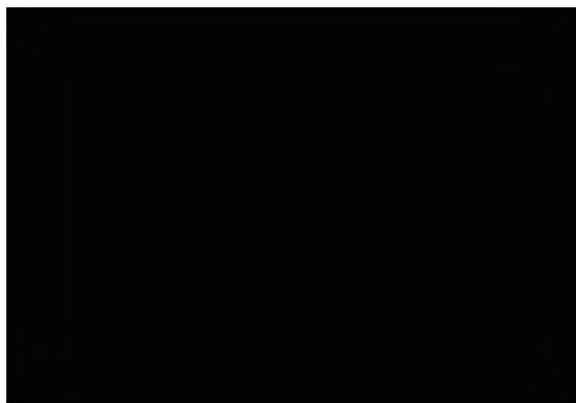
13.2 Tato smlouva je projevem svobodné vůle obou smluvních stran a tyto jí na důkaz souhlasu s jejím obsahem podepisují.

13.3 Tato smlouva je vyhotovena ve dvou stejnopisech, každá smluvní strana obdrží po jednom vyhotovení.

13.4 Tato smlouva nabývá platnosti a účinnosti dnem jejího podpisu poslední smluvní stranou.

V Děčíně dne 13.5.2020

V Chomutově dne 29.5.2020



PŘÍLOHA 1: Technická a organizační opatření pro zpracování dat

Bezpečnostní opatření uvedená v bodech 1 až 7 jsou pokryty bezpečnostním konceptem.

1. Kontrola fyzického přístupu

Bezpečnostní opatření pro přístup neautorizovaných osob do prostorů, ve kterých probíhá zpracování dat (například plot, vrátný, dveře se čtečkou karet, kamerový systém, kontrola přístupů)

Pro sběr, zpracování nebo použití osobních dat, jak je popsáno v této DoZD, přijal dodavatel následující technická a organizační opatření:

- Poplašný systém
- Čipové karty
- Videomonitoring přístupových dveří
- Bezpečnostní zámky

2. Kontrola přístupu k datům/Uživatelská kontrola

Zabránění třetí straně užívat automatické zpracovávací systémy vybavené k přenosu dat (autentifikace uživatele pomocí hesla).

Pro sběr, zpracování nebo použití osobních dat, jak je popsáno v této DoZD, přijal dodavatel následující technická a organizační opatření:

- Autentifikace uživatelským jménem a heslem (přiřazení hesla dle platných opatření)
- Užití antivirového softwaru
- Užití softwarového firewallu
- Tvorba uživatelských účtů
- Přiřazení uživatelských účtů k IT systému
- Užití technologie VPN

3. Kontrola užití dat/Kontrola datových médií/Kontrola paměti

Zabránění neautorizovanému čtení, kopírování, pozměňování nebo poškozování datových médií (kontrola datových médií), zabránění neautorizovanému přidání osobních informací a neautorizovaný přístup k nim, jejich měnění nebo mazání (kontrola paměti). Zajištění, že strany autorizované k užití automatických zpracovávacích systémů mají přístup pouze k informacím v rámci své autorizace (například pomocí hesel, předpisy pro přesun zaměstnanců na jiné pracoviště nebo opuštění společnosti) (kontrola užití dat).

Pro sběr, zpracování nebo použití osobních dat, jak je popsáno v této DoZD, přijal dodavatel následující technická a organizační opatření:

- Role a autorizace založené na zásadě „potřeby vědět“ (k informacím se dostane jen ten, kdo je potřebuje k práci)
- Množství administrátorů omezeno pouze na nezbytné množství
- Fyzické smazání datových médií před jejich znovupoužitím
- Použití scartovacích strojů
- Administrace oprávnění systémovým administrátorem
- Bezpečné skladování datových médií



4. Kontrola přenosu/přepravy

Zajištění, že důvěrnost a integrita dat bude ochráněna během přenosu dat nebo během přepravy datových médií (např. silným šifrováním datového přenosu, zapečetěním přepravovaných zásilek a šifrováním uložených dat na médiích).

Pro sběr, zpracování nebo použití osobních dat, jak je popsáno v této DoZD, přijal dodavatel následující technická a organizační opatření:

- Zřízení dedikovaných linek nebo VPN tunelu
- Šifrovaný přenos dat přes internet (jako je HTTPS, SFTP, atd.)

5. Kontrola přístupů/kontrola přenosu

Zajištění, že je možné zpět zjistit, které osobní informace byly vloženy nebo změněny, v jaký čas a kým, například skrze přihlášení uživatelů (kontrola přístupů).

V závislosti na systému zajištění možnosti určit kam byly osobní údaje přeneseny nebo poskytnuty nebo kam by mohli být přeneseny (kontrola přenosu).

Pro sběr, zpracování nebo použití osobních dat, jak je popsáno v této DoZD, přijal dodavatel následující technická a organizační opatření:

- Zaznamenávání přístupů, přidání a změn dat
- Dohledatelnost přístupů, změn a mazání dat pomocí unikátních uživatelských jmen
- Přiřazení práv k přístupu, měnění a mazání dat dle autorizačního konceptu
- Vytvoření přehledu jaká data mohou být aplikacemi vložena, měněna a mazána
- Uchování formátu, ve kterém jsou data získávána

6. Kontrola dostupnosti/Obnovitelnosti/Spolehlivosti/Integrity dat

Zajištění, že použité systémy mohou být obnoveny v případě poruchy (obnovitelnost). Zajištění, že všechny funkce systému jsou dostupné a veškeré poruchy jsou hlášeny (spolehlivost). Zajištění, že uložené osobní informace nemohou být poškozeny systémovou poruchou (integrita dat). Zajištění, že jsou osobní data chráněna proti náhodnému poškození nebo ztrátě dat (kontrola dostupnosti), např. implementací záložního řešení.

Pro sběr, zpracování nebo použití osobních dat, jak je popsáno v této DoZD, přijal dodavatel následující technická a organizační opatření:

- Nepřerušitelný zdroj napájení (UPS)
- Poplašná zařízení proti neautorizovanému přístupu do serverové místnosti
- Testování obnovitelnosti dat
- Skladování datových záloh na odděleném a zabezpečeném úložišti
- Vytvoření konceptu záloh a obnovitelnosti

7. Kontrola oddělení/Oddělitelnost

Zajištění, že data získána za různými účely mohou být zprávně odděleně (například logickým dělením zákaznickových dat, specializovaný přístupem (koncept autorizace), oddělování testovacích a produkčních dat).

Pro sběr, zpracování nebo použití osobních dat, jak je popsáno v této DoZD, přijal dodavatel následující technická a organizační opatření:

- Fyzicky oddělené skladování dat
- Nastavení databázových práv
- Logické oddělení klientů (softwarové)
- Oddělení produkčních a testovacích systémů