PŘÍLOHA Č. 4 KE SMLOUVĚ O PORADENSKÝCH SLUŽBÁCH

(„Smlouva")

SMLOUVA O ZPRACOVÁNÍ ÚDAJŮ

TATO SMLOUVA O ZPRACOVÁNÍ ÚDAJŮ (dále jen „**DPA**") byla uzavřena dne Click to enter a date mezi:

1. **Správce: Plzeňský Prazdroj, a. s.**, sídlo: U Prazdroje 64/7, Východní Předměstí, 301 00 Plzeň, IČ: 45357366, společnost zapsaná v obchodním rejstříku vedeném Krajským soudem v Plzni pod sp. zn. B 227 zastoupený p. Rudolfem Šlehoferem, ředitelem odd. Craft a Heritage
(dále jen „**Správce**")

a

2. **Zpracovatel: Výzkumný ústav vodohospodářský T. G. Masaryka, veřejná výzkumná instituce**, sídlo: Podbabská 2582/30, 160 00 Praha 6, IČ: 00020711, DIČ: CZ00020711, společnost zapsaná v Rejstříku veřejných výzkumných institucí vedeném MŠMT ČR, zastoupená: Ing. Tomášem Fojtíkem, ve věcech technických**:** Ing. Dagmar Vološinová
(dále jen „**Zpracovatel**")

(každý jako „**Strana**" a společně „**Strany**")

Které se dohodly takto:

1. DEFINICE

1.1. Následující výrazy mají v této DPA následující významy:

Smlouva	znamená Smlouva o poradenských službách č. SMLP-2023-024-000001
Příslušné zákony na ochranu údajů	znamenají GDPR, z. č. 110/2019 Sb. ve znění pozdějších předpisů a vnitrostátní zákon(y), které upravují implementace a odchylky, pokud to GDPR povoluje, spolu s veškerými normativními rozhodnutími vydanými příslušným dozorovým úřadem a Evropským sborem pro ochranu osobních údajů.
DPA	znamená tuto Smlouvu o zpracování údajů.
GDPR	znamená NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 679/2016 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); včetně britského GDPR zachovaného v právu Spojeného království Velké Británie a Severního Irska jako součást zákona o ochraně údajů 2018.

Služby	znamenají služby poskytované Zpracovatelem, jak jsou popsány ve Smlouvě.
Standardní smluvní doložky	znamenají smluvní ustanovení uvedená v prováděcím rozhodnutí Komise (EÚ) 2021/914 ze dne 4. června 2021 o standardních smluvních doložkách pro předávání osobních údajů do třetích zemí podle nařízení Evropského parlamentu a Rady (EU) 2016/679, které může měnit nebo nahradit Komise.
Vedlejší zpracovatel	znamená subjekt najatý Zpracovatelem (nebo některým z jeho Subdodavatelů), který Zpracovává Údaje Správce jménem Zpracovatele (nebo příslušného (Vedlejšího) zpracovatele).
Opatření technické a organizační bezpečnosti	znamenají opatření zaměřená na ochranu Osobních údajů před porušením osobních údajů, (zejména pokud zpracování zahrnuje přenos údajů přes síť) a zajištění splnění ostatních požadavků GDPR.

1.2. Pokud DPA používá výrazy definované v GDPR, tyto výrazy mají stejný význam jako v GDPR.

2. ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

2.1. Během poskytování Služeb Správci Zpracovatel zpracovává nebo může zpracovávat osobní údaje jménem Správce. V takovém případě platí tato DPA.

2.2. V případě rozporu mezi ustanoveními této DPA a Smlouvy nebo ustanoveními jiných souvisejících dohod mezi Stranami existujícími v době, kdy je DPA dohodnuta nebo později uzavřena, mají přednost ustanovení DPA.

3. OSOBNÍ ÚDAJE SPRÁVCE

3.1. Podrobnosti operací souvisejících se zpracováním kategorií osobních údajů, na které se vztahuje tato DPA, jsou uvedeny v Příloze 1, která je nedílnou součástí této DPA. Aniž je tím dotčen tento seznam, budou veškeré další osobní údaje zpracovávané Zpracovatelem jménem Správce v průběhu poskytování Služeb předmětem této DPA.

3.2. Každá Strana zaručuje druhé straně, že bude zpracovávat osobní údaje v souladu s touto DPA a bude plnit své závazky podle této DPA takovým způsobem, aby nezpůsobila, že druhá Strana poruší jakékoliv povinnosti podle této DPA.

3.3. Osobní údaje Správce bude Zpracovatel používat pouze na poskytování Služeb, včetně účelů slučitelných s poskytováním těchto Služeb. Zpracovatel nepoužije osobní údaje ani nevyužije informace z nich odvozené pro jakýkoli reklamní nebo jiný účel, který není stanoven touto DPA. Správce si vyhrazuje zachování všech práv, právních základů a zájmů týkajících se osobních údajů. Zpracovatel vůči osobním údajům nenabude žádná práva, s výjimkou práv, které Správce uděluje Zpracovateli pro potřeby poskytování Služeb. Tento odstavec se netýká práv Zpracovatele ohledně softwaru a licencí softwaru nebo užívání jiných práv poskytovaných Správci.

4. SPRÁVCE A ZPRACOVATEL

4.1. Zpracovatel jmenoval Ing. Dagmar Vološinovou jako svého pověřence pro ochranu údajů. Změna pověřence pro ochranu údajů musí být bezodkladně oznámena Správci. Správce jmenoval dle článku 37 pověřence pro ochranu osobních údajů, kontakt: [redacted].

4.2. Správce zaručuje a odpovídá za zákonnost a přesnost údajů Správce, které shromažďuje a nezaručuje zákonnost údajů, pokud tyto údaje nejsou shromažďovány přímo Správcem.

4.3. Zpracovatel ručí a odpovídá za zákonnost a přesnost údajů, které shromažďuje, a to buď přímo, nebo prostřednictvím svých povolených Vedlejších zpracovatelů z titulu funkce Zpracovatele.

5. POKYNY SPRÁVCE

5.1. Zpracovatel bude zpracovávat pouze osobní údaje Správce (i) v rozsahu nezbytném pro poskytování Služeb Správci a pouze pro účely, jak uvádí pokyny Správce a (ii) způsobem, který je v souladu s touto DPA. Smlouva a tato DPA spolu s následnými pokyny předanými Zpracovateli Správcem (včetně e-mailu) jsou pokyny Správce Zpracovateli pro zpracování osobních údajů.

5.2. Pokud to Zpracovatel nemůže z jakýchkoli důvodů dodržet, musí neprodleně informovat Správce o jeho neschopnosti dodržet (pokyny) a v takovém případě je Správce oprávněn pozastavit nebo ukončit Smlouvu bez jakékoli pokuty.

5.3. Zpracovatel bezodkladně a řádně vyřídí všechny dotazy Správce týkající se zpracovávání údajů Správce.

5.4. Osoby oprávněné vydávat pokyny jménem Správce jsou: […]

5.5. Osoby oprávněné přijímat pokyny jménem Zpracovatele jsou: Ing. Dagmar Vološinová; [redacted].

5.6. Pokud je(jsou) kontaktní osoba (osoby) nahrazena nebo dlouhodobě nedostupná(é), musí být druhá Strana písemně informována (včetně e-mailu) o náhradním kontaktu nebo zástupci.

5.7. Pokyny mohou být zaslány emailem výše uvedeným osobám a budou uchovávány po celou dobu jejich platnosti a dále po dobu tří let od 1. ledna následujícího kalendářního roku.

5.8. Zpracovatel bude neprodleně informovat Správce, pokud podle jeho názoru pokyn Správce porušuje Příslušné zákony na ochranu údajů. Zpracovatel může po provedení ověření pozastavit provádění tohoto pokynu až do jeho potvrzení nebo změny odpovědnou osobou Správce.

6. UMÍSTĚNÍ ÚDAJŮ

6.1. Po dobu trvání Smlouvy Zpracovatel uchovává osobní údaje Správce v rámci EHP, změna je možná jen s předchozím písemným souhlasem Správce. Osobní údaje Správce nesmí být zpřístupněny nebo přeneseny mimo EHP bez předchozího písemného souhlasu Správce.

7. ZABEZPEČENÍ

7.1. Po celou dobu trvání Smlouvy Zpracovatel přijme a implementuje odpovídající Opatření technické a organizační bezpečnostní (včetně, ovšem bez omezení těch, která jsou uvedena v Příloze 2) k odpovídajícímu zabezpečení údajů Správce proti porušování osobních údajů.

7.2. Pro vyloučení pochybností nezbavuje implementace bezpečnostních požadavků uvedených v Příloze 2 Zpracovatele, aby provedl vlastní hodnocení a rozhodl, která dodatečná opatření jsou adekvátní, aby se zajistila úroveň bezpečnosti odpovídající zjištěným rizikům.

7.3. Zpracovatel musí bezodkladně a v každém případě nejpozději do 24 hodin po zjištění informovat Správce o jakémkoli porušení Osobních údajů, o kterém se dozví, že trvá, a poskytne Správci veškeré dostupné informace týkající se porušení těchto osobních údajů, včetně nápravy a dalších nápravných opatření přijatých nebo plánovaných, které má Zpracovatel uskutečnit. Zpracovatel poté podnikne veškerá nezbytná opatření k co nejrychlejšímu omezení a nápravě incidentu, řádně informuje Správce o vývoji a poskytne veškerou spolupráci, kterou Správce požaduje.

7.4. V případě jakéhokoli vyšetřování nebo zabavení osobních údajů vládním orgánem, orgánem dohledu nad ochranou údajů nebo orgánem pro vymáhání práva to Zpracovatel neprodleně oznámí Správci, pokud to není zakázáno příslušným právem nebo na žádost orgánů výkonu práva, pokud by takové oznámení bránilo probíhajícímu vyšetřování. V druhém případě Zpracovatel oznámí Správci, jakmile důvody, proč nebylo oznámení učiněno, přestaly platit. Zpracovatel zdokumentuje celou situaci a poskytne takovou dokumentaci Správci. Po celou dobu, kdy Správci nebyly poskytnuty informace a nebyl angažován, má Zpracovatel veškerou odpovědnost v souvislosti se zpřístupněním osobních údajů Správce orgánu státní správy, orgánu dohledu nad ochranou údajů nebo jakémukoli dotčenému orgánu pro vymáhání práva.

8. PRÁVA SUBJEKTU ÚDAJŮ

8.1. Zpracovatel bezodkladně oznámí Správci jakékoli požadavky subjektu údajů. Zpracovatel nebude na tyto požadavky odpovědět samostatně, pokud nebyl k tomu Správcem pověřen.

8.2. Po celou dobu trvání Smlouvy bude Zpracovatel podle výběru a požadavku Správce buď (1) poskytovat Správci možnost opravovat, mazat nebo anonymizovat osobní údaje; nebo (2) neprodleně učiní takové opravy, výmazy nebo anonymizaci jménem Správce.

8.3. Tam, kde Správce oznámí Zpracovateli, že subjekt údajů uplatnil právo na opravu, vymazání, omezení zpracování nebo námitku ohledně zpracování, zajistí Zpracovatel, že to bude okamžitě implementováno podle pokynů Správce a v každém případě do 15 dnů od pokynu Správce. Zpracovatel dále zajistí, aby tato skutečnost byla sdělena každému příjemci, kterému byly příslušné osobní údaje zpřístupněny (např. jeho Vedlejší zpracovatelé).

9. PERSONÁL ZPRACOVATELE

9.1. Zpracovatel je povinen zavést opatření k omezení přístupu k údajům Správce pouze na ty zaměstnance Zpracovatele, kteří potřebují přístup k těmto údajům, aby mohli plnit své pracovní povinnosti ve prospěch Správce na základě zásady „potřebuji vědět“ a „nejméně privilegovaný přístup“.

9.2. Bez omezení rozsahu článku 7.1 Zpracovatel učiní přiměřené kroky k zajištění spolehlivosti všech svých zaměstnanců, kteří mohou mít přístup k údajům Správce. Zpracovatel zajistí, aby jeho pracovníci byli řádně vyškoleni ohledně zpracování osobních údajů a zavázali se k zachování důvěrnosti nebo podléhají zákonné povinnosti mlčenlivosti. Na žádost Správce a na jeho náklady zajistí Zpracovatel, aby se jeho příslušný personál účastnil školení pořádaných Správcem.

10. VEDLEJŠÍ ZPRACOVATEL

10.1. Zpracovatel může využívat Vedlejšího zpracovatele k poskytování omezených služeb jeho jménem podle podmínek Smlouvy a této DPA. Jakýkoli takový Vedlejší zpracovatel bude mít právo zpracovávat údaje Správce pouze pro poskytování Služeb, které Zpracovatel tímto zajišťuje a Zpracovatel zajistí, že Vedlejší zpracovatel nebude zpracovávat údaje Správce za jakýmkoli jiným účelem.

10.2. Zpracovatel může nadále využívat Vedlejší zpracovatele, které již byli Zpracovatelem angažováni k datu této DPA, a to za předpokladu, že v každém případě, jakmile je to proveditelné, Zpracovatel splní povinnosti uvedené v článku 10.4 a poskytne o tom důkaz Správci.

10.3. Zpracovatel nesmí zapojit Vedlejší zpracovatele bez souhlasu Správce. Nejméně jeden měsíce před zapojením takového Vedlejšího zpracovatele poskytne Zpracovatel Správci předem upozornění identifikující Vedlejšího zpracovatele a uvede detaily hodnocení rizik provedené při výběru takového Vedlejšího zpracovatele a zejména technická a organizační opatření přijatá k zajištění ochrany práv subjektu údajů. Správce může předložit námitku ve lhůtě měsíce s uvedením důvodů, proč proti tomuto Vedlejšímu zpracovateli vznáší námitky. V případě takové výhrady, i když Zpracovatel nesouhlasí s postavením Správce, nebude Vedlejší zpracovatel ve vztahu k údajům Správce angažován a Strany budou pracovat v dobré víře, aby se pokusily o vzájemné vyřešení této záležitosti. Pokud po uplynutí maximální dodatečné lhůty jednoho měsíce Správce stále neschválí nového Vedlejšího zpracovatele, pak Správce může ukončit Smlouvu (nebo případně dotčenou Službu) bez sankce, a to písemnou výpovědí, která obsahuje vysvětlení důvodů pro neschválení.

10.4. S ohledem na každého Vedlejšího zpracovatele musí Zpracovatel:

(a) předtím, než Vedlejší zpracovatel nejprve zpracuje údaje Správce, zajistit, že je Vedlejší zpracovatel schopen poskytnout úroveň ochrany údajů Správce požadovaných touto DPA;

(b) zajistit, aby se ujednání mezi Zpracovatelem a Vedlejším zpracovatelem řídila písemnou smlouvou včetně podmínek, které nabízejí alespoň stejnou úroveň ochrany údajů Správce jako ty stanovené v této DPA a splňují požadavky čl. 28 odst. 3 GDPR bez práva dále činit svá práva a povinnosti předmětem subdodávky, pokud nebudou dodrženy předchozí práva na informace a ukončení Správcem uvedené výše;

(c) pokud toto ujednání zahrnuje předávání osobních údajů Správce od Zpracovatele k Vedlejšímu zpracovateli nebo další předávání údajů Správce od Vedlejšího zpracovatele k dalšímu Vedlejšímu zpracovateli nebo mezi dvěma provozovnami Zpracovatele nebo Vedlejšího zprostředkovatele, zajistit, aby Standardní smluvní doložky schválené Evropskou komisí nebo označené Správcem byly ve všech příslušných případech zahrnuty do dohody mezi Zpracovatelem a Vedlejším zpracovatelem nebo před tím, než Vedlejší zpracovatel nejprve zpracuje osobní údaje Správce, zajistit, že uzavře dohodu zahrnující Standardní smluvní doložky se Správcem; a

(d) identifikovat jakéhokoli Vedlejšího zpracovatele, který zpracovává údaje Správce, a zpřístupní podmínky zpracování Správci (s vyloučením jakýchkoli pochybností, jakékoliv relevantní obchodní podmínky).

10.5. Zpracovatel odpovídá za jednání a opomenutí jakéhokoli takového Vedlejšího zpracovatele ve stejném rozsahu, jako kdyby jednání nebo opomenutí byla učiněna Zpracovatelem.

11. VYMAZÁNÍ OSOBNÍCH ÚDAJŮ A OMEZENÍ POUŽITÍ

11.1. S výjimkou dalších pokynů Správce Zpracovatel vrátí údaje Správci nejpozději do 30 dnů od ukončení Smlouvy (nebo případně poté, co byl dokončen projekt v rámci Smlouvy) a vymaže všechny záznamy takových údajů v systémech (včetně zálohování).

11.2. Přenos dat na Správce, a to jak během plnění Smlouvy, tak při plnění výše uvedené povinnosti, se neposkytuje prostřednictvím e-mailu, ale v souladu s požadavky uvedenými v Příloze 2 (Bezpečnostní opatření).

11.3. Zpracovatel poskytne Správci písemné potvrzení, že plně dodržuje této článek 11 do 45 dnů od ukončení Smlouvy z jakéhokoli důvodu, stejně jako kdykoli o to Správce požádá.

11.4. Zpracovatel pokračuje v zajišťování souladu s DPA až do vymazání nebo vrácení osobních údajů.

12. AUDITY A KONTROLY

12.1. Strany se budou řídit Příslušnými zákony na ochranu údajů a navzájem si pomáhat při zajišťování souladu se všemi Příslušnými zákony na ochranu údajů, i když DPA na nich neodkazuje nebo neobsahuje povinnosti a závazky z nich přímo vyplývající.

12.2. Zpracovatel zpřístupní Správci na vyžádání veškeré informace nezbytné k prokázání dodržování této DPA a souladu s GDPR a Příslušnými zákony na ochranu údajů, povolí a přispěje k auditu zpracovatelských činností dle této DPA.

12.3. Jednou za rok má Správce právo na vlastní náklady na základě přiměřeného předběžného oznámení Zpracovateli provést audit osobně nebo určeným nezávislým auditorem. Zpracovatel bezodkladně vyřeší problémy uvedené v každé auditní zprávě k přiměřenému uspokojení Správce a Správce bude mít právo provést následný audit ve stejných aspektech, kdy byly poprvé zjištěny neshody, za stejných podmínek stanovených ve vztahu k primárnímu auditu. Správce zajistí, aby provedení auditů bylo sdělováno co nejvíce předem.

12.4. Zpracovatel bezplatně poskytne Správci přiměřenou součinnost s posouzením vlivu na ochranu osobních údajů a předchozími konzultacemi s dozorovými orgány, které Správce přiměřeně považuje za nutné nebo užitečné podle Příslušných zákonů na ochranu údajů, v každém případě výlučně ve vztahu ke zpracovávání osobních údajů Správce v rámci Služby, a s přihlédnutím k povaze zpracování a informace, které má Zpracovatel a/nebo jeho Vedlejší zpracovatelé k dispozici.

13. ODPOVĚDNOST

13.1. Zpracovatel odpovídá za jakékoli škody způsobené zpracováním provedeným Zpracovatelem.

13.2. Tam, kde Správce zaplatil náhradu škody, kterou utrpěl subjekt údajů a tato odpovědnost je zcela nebo zčásti přičitatelná Zpracovateli, je Správce oprávněn požadovat od Zpracovatele zaplatit tu část náhrady, která odpovídá jeho části odpovědnosti za škodu.

13.3. Aniž je dotčeno právo Stran rozporovat záležitost, pokud je Správci uložena správní pokuta podle Příslušných zákonů na ochranu údajů, pokud jde o záležitosti přičitatelné nebo způsobené Zpracovatelem, pak Zpracovatel odškodní Správce a pokryje celou výši takové pokuty. Je-li odpovědnost Zpracovatele částečná, pak náhrada Správce bude proporcionální.

13.4. Pro vyloučení pochybností se na odpovědnost za zpracování osobních údajů Zpracovatelem jménem Správce nebudou vztahovat žádná omezení.

14. TRVÁNÍ A UKONČENÍ

14.1. Tato DPA se uzavírá na dobu určitou, a to po dobu trvání Smlouvy a související zpracování osobních údajů pro účely nebo v souvislosti s plněním Smlouvy a poskytováním Služeb. Ukončením DPA nejsou dotčena ustanovení této DPA a Smlouvy nebo právní závazky, jejichž účelem je vyvolat účinky po ukončení.

15. ZÁVĚREČNÁ USTANOVENÍ

15.1. Zpracovatel je povinen vést záznamy o všech kategoriích zpracovatelských činností, které provedl jménem Správce, v souladu s čl. 30 odst. 2 GDPR.

15.2. Ustanovení Smlouvy týkající se mlčenlivosti, písemné formy prostřednictvím systému DocuSign, řešení sporů, pokud nejsou v rozporu s DPA, použijí se obdobně na tuto DPA.

15.3. Ustanovení týkající se technických a organizačních bezpečnostních opatření, jakož i auditorských práv Správce zůstávají platnými a vymahatelnými po dobu trvání této DPA, nebo dokud Zpracovatel nevymaže osobní údaje Správce podle čl. 11 DPA..

15.4. Pokud jde o předmět této DPA (zpracovávání osobních údajů), budou zde mít tato ustanovení přednost před Smlouvou.

15.5. Toto DPA se řídí českým právem. Veškeré spory mezi Stranami, které vzniknou z DPA nebo s ní souvisejí, budou řešit soudy České republiky.

15.6. Na tuto DPA se vztahují ustanovení Smlouvy o mlčenlivosti. Strana však může tuto DPA sdílet s orgánem dohledu nad ochranou údajů a v nezbytně nutném minimálním rozsahu se subjekty údajů bez souhlasu druhé Strany.

15.7. V případě, že bude jedno nebo více ustanovení obsažených v této DPA z jakéhokoli důvodu považováno za neplatné, neúčinné, nezákonné a/nebo nevymahatelné, platnost, zákonnost a vymahatelnost zbývajících ustanovení této DPA nebude nijak dotčena, a pokud je to nezbytné pro tento účel, považuje(í) se to(a)to ustanovení za vynechané z této DPA.

15.8. Strany se dohodly, že DPA podepíšou elektronicky s využitím zajištěného systému DocuSign. Správce umístí DPA nebo její dodatek, nebo přílohu v elektronické podobě do systému DocuSign a vyzve Zpracovatele k podpisu elektronického dokumentu. Zpracovatel poskytne potřebnou součinnost (zejména pak správnou elektronickou adresu osoby, která je oprávněná podepisovat jménem Zpracovatele). Každá ze Stran

elektronicky obdrží plně podepsaný dokument ve formátu.pdf opatřený DocuSign certifikátem (Certificate of Completion), takový dokument se považuje za písemné vyhotovení. NEBO: DPA se pořizuje ve 2 (dvou) stejnopisech v českém jazyce. Po podpisu DPA obdrží každá ze smluvních stran po 1 (jednom) její stejnopisu.

15.9. Změna této DPA může být realizována na základě vzájemné dohody a dohodnutým způsobem písemně - prostřednictvím systému DocuSign, jednáním oprávněné osoby za každou Stranu.

Strany prohlašují, že si DPA přečetly, obsahu, který považují za určitý a srozumitelný, porozuměli a tento vyjadřuje jejich svobodnou a vážnou vůli zbavenou jakýchkoli omylů, na důkaz čehož připojují své podpisy.

V Praze

Za Zpracovatele:

Ing. Tomáš Fojtík

Za a jménem Správce

PŘÍLOHA 1. POPIS ZPRACOVATELSKÝCH ČINNOSTÍ S OSOBNÍMI ÚDAJI

Kategorie subjektu údajů, jejichž osobní údaje jsou zpracovávány

Zaměstnanci správce a jiné osoby, které jsou ve smluvním vztahu ke správci

Kategorie osobních údajů

Adresní, identifikační a kontaktní údaje subjektů (jméno, příjmení, pracovní zařazení, telefon, emailová adresa), případně další údaje nezbytné pro plnění smlouvy

Popis zpracovatelských činností, včetně účelu zpracování

[…]

PŘÍLOHA 2. MINIMÁLNÍ STANDARDNÍ BEZPEČNOSTNÍ OPATŘENÍ

1. **Řízení a dodržování (pravidel)**
   a. Zpracovatel implementuje pravidla a standardy organizační bezpečnostní přizpůsobené standardům bezpečnostního průmyslu a zajistí jejich dodržování.
   b. Zpracovatel zajistí, aby jmenoval vhodného jednotlivce (nebo více jednotlivců), který(ří) bude(ou) odpovědný(i) za zajištění technického a organizačního souladu s bezpečnostními kontrolami a kontrolami ochrany definovanými v tomto dokumentu a vlastních pravidlech Zpracovatele.

2. **Řízení informačních rizik**
   a. Zpracovatel vytvoří rámec řízení s podporou pravidel řízení rizik, který umožní a podpoří řízení rizik.

3. **Kontinuita v podnikání**
   a. Zpracovatel musí mít vhodné plány kontinuity v podnikání, včetně plánu (plánů) obnovy IT po havárii, aby zabránil a/nebo zajistil včasné obnovení svých IT systémů, které uchovávají nebo zpracovávají data Správce nebo IT systémů, které jinak podporují služby poskytované Správci, a to v případě havárie.
   b. Zpracovatel zajistí, aby byly plány na obnovu po havárii pravidelně testovány a aktualizovány tak, aby bylo zajištěno, že jsou aktuální a účinné.
   c. Zpracovatel musí udržovat integritu a dostupnost a ochranu osobních informací před zničením nebo náhodnou ztrátou informací a zařízení pro zpracování informací prostřednictvím záložních kopií informací a softwaru, které budou pravidelně přijímány a testovány v souladu s dohodnutými pravidly pro zálohování.

4. **Školení o bezpečnosti a povědomí**
   a. Zpracovatel zajistí, aby si všichni zaměstnanci, dodavatelé a uživatelé třetích stran byli vědomi hrozeb a obav týkajících se bezpečnosti informací, svých povinností a odpovědnosti a byli v průběhu své práce vybaveni pro podporu pravidel organizační bezpečnosti.
   b. Zpracovatel zajistí, aby si jeho zaměstnanci, dodavatelé a uživatelé třetích stran, kteří zpracovávají osobní informace, byli vědomi definice osobních údajů a citlivých skupin osob.
   c. Zpracovatel zajistí, aby se v případě potřeby dostalo všem zaměstnancům, dodavatelům a uživatelům třetích stran odpovídajícího školení o povědomí, které by nemělo být provedeno po dobu delší než 12 měsíců.

5. **Nakládání s médii a výměna informací**
   a. Postupy pro nakládání s a uchovávání informací stanoví Zpracovatel k ochraně informací před neoprávněným zveřejněním nebo zneužitím.
   b. Zpracovatel zajistí, aby s médii bylo nakládáno spolehlivě a bezpečně, pokud již nejsou vyžadována, a to s využitím formálních postupů.
   c. Zpracovatel zajistí, aby byla dokumentace systému chráněna před neoprávněným přístupem.
   d. Zpracovatel bude udržovat bezpečnost informací a softwaru vyměňovaných v rámci své organizace a v rámci jakéhokoli externího subjektu. To zahrnuje dohody o výměně, fyzická tranzitní média, elektronické zasílání zpráv a ochranu informací spojených s propojením obchodních informačních systémů.

6. **Kontrola přístupu**
   a. Zpracovatel zavede a implementuje pravidla kontroly přístupu, která zajistí oprávněný přístup k uživatelům a zabrání neoprávněnému přístupu, a to zejména k osobním údajům.
   b. Zpracovatel bude pravidelně kontrolovat přístupová práva uživatelů, aby zajistil, že přidělení a užívání oprávnění bude v případě potřeby kontrolováno a omezeno.
   c. Pravidla Zpracovatele ohledně kontroly přístupu by měla vycházet z následujících zásad:
      1) Přístup neoprávněných osob do zařízení, které se používá k zpracování nebo ukládání údajů Správce, není povolen.
      2) Neoprávněné osoby nesmějí používat systémy zpracování osobních údajů.
      3) Budou přijata opatření, která zajistí, aby osoby, které jsou oprávněny používat systém zpracování údajů, měly přístup pouze k údajům na základě potřeby je znát a že osobní údaje nemohou být čteny, kopírovány, upravovány nebo odstraňovány bez ověření v průběhu zpracování nebo využití a uchování.
      4) Zpracovatel musí mít zaveden formální a zdokumentovaný proces, na základě kterého budou udělena/pozměněna/odvolána práva na přístup ke všem systémům a procesům v závislosti na tom, které informace Správce jsou zpracovávány, uchovávány nebo předávány.
      5) Přístupová práva uživatelů Zpracovatele jsou přísně omezena podle zásad „potřeba je znát“ a „nejméně privilegovaný přístup“, které by měly umožňovat přístup pouze k systémům a procesům, které jsou nezbytné pro plnění příslušných povinností.
      6) Všichni uživatelé Zpracovatele, kteří mají přístup k informacím Správce, k nim musí mít přidělen jedinečný identifikátor přístupu, který nesmí být sdílen s žádnou jinou osobou.
      7) Přístupová práva k systémům, které uchovávají, zpracovávají nebo předávají informace Správce, budou okamžitě zrušena, pokud uživatel opustí Zpracovatele nebo pokud jejich nové úkoly již nezahrnují přístup k těmto informacím.
      8) Všechna přístupová práva musí Zpracovatel nejméně každý rok přezkoumat.
      9) Přístup k operačním systémům, které uchovávají, zpracovávají nebo sdělují informace o Správci operace s nimi, musí být zaznamenávány a uchovávány pro účely auditu po dobu nejméně 90 dnů (viz kapitola auditu).
      10) Pokud Zpracovatel spravuje databázi (e) patřící Správci, pak Zpracovatel implementuje také bezpečnou metodu vzdáleného přístupu pro přiřazené uživatele Správce; toto bude zahrnovat jako bezpečnostní

požadavky s minimálním přístupem zabezpečené řešení VPN typu IPSec nebo SSL/TLS s mechanismem ověřování dvojího faktoru.

11) Pro služby spravované Zpracovatelem jménem Správce (např. účty sociálních médií) bude vytvořen také přístupový kód s právy pro uživatele Správce.
12) Za žádných okolností nebudou služby jménem Správce dodány bez administrativního přístupu přiděleného určeným uživatelům Správce.

7. **Ověření**

Zpracovatel by se měl řídit následujícími zásadami týkajícími se ověřovacích mechanismů:

a. Pro systémy, které zpracovávají, ukládají, nebo předávají informace Správce, jsou preferované ověřovací mechanismy ty, které jsou integrovány do systémů Správce (SSO, ADFS) nebo ty, které používají dva ověřovací faktory.
b. Pro řešení, která používají ověřování s jedním faktorem, musí hesla, která dodavatelé implementují a spravují v systémech, které uchovávají, zpracovávají nebo předávají informace Správce, splňovat alespoň minimální podmínky uvedené níže:
    - všechna přístupová hesla musí mít délku alespoň 8 znaků;
    - hesla musí obsahovat alespoň jeden alfanumerický znak a alespoň jeden zvláštní znak (*např.* -,)(*&^%$#@!)
    - hesla by neměla obsahovat samostatná slova ze slovníků; ověřovací fráze tvořené několika pracemi jsou akceptovány, pokud vyhovují všem ostatním podmínkám;
    - hesla nemusí být shodná s předchozími 6 (šest) hesly nastavenými dříve;
    - ukládání viditelných hesel nebo použití pouze reverzibilních šifrovacích metod je zakázáno; pro ukládání hesel musí být používány hashové funkce jednosměrného řazení;
c. Je-li použita metoda dvou faktorového ověřování, mělo by být použito principu ověřování mimo pásmo (sekundární ověřovací metoda prostřednictvím samostatného komunikačního kanálu).

8. **Kryptografická kontrola**

a. V situacích s vyšším rizikem doplní Zpracovatel stávající kontroly přístupu se šifrovacími řešeními jak pro data v klidovém stavu, tak i pro tranzit. Vyšší riziko se může týkat:
    - Typu dat (například citlivé osobní informace nebo informace, které mohou významně ovlivnit Správce, vyžadují lepší ochranu než údaje, které nejsou osobními údaji nebo jinak důvěrné).
    - Související zranitelnost (například data uložená v systému orientovaném na internet jsou zranitelnější než data uložená uvnitř soukromé sítě).
    - Související hrozby (např. data v tranzitu přes otevřenou síť jsou citlivější na hrozbu).
b. Zpracovatel musí mít pravidla týkající se používání kryptografických kontrol pro ochranu informací, která jsou implementována a dodržována.

9. **Důvěrná povaha a integrita přenosu dat**

a. Zpracovatel zajistí, aby sítě byly řádně spravovány a kontrolovány tak, aby byly chráněny před hrozbami a aby byla zachována bezpečnost systémů a aplikací využívajících síť, včetně informací v tranzitu.
b. Data budou převedena z firmy a do firmy Zpracovatele/Vedlejšího zpracovatele za použití výlučně služeb schválených Správcem; přenášená data zahrnují bez toho, aniž by byla omezen na: archivy, soubory, přílohy.

10. **Ochrana dat**

a. Zpracovatel zajistí, aby jejich bezpečnostní politika zahrnovala pravidla pro uchování a odstraňování dat a bezpečnostní standardy.
b. Zpracovatel zajistí, aby byly provedeny příslušné kontroly, aby se zabránilo záznamům ze ztrát, zničení nebo manipulace během doby jejich uchovávání.
c. Zpracovatel souhlasí s tím, že na žádost Správce nebo po ukončení Smlouvy zlikviduje (např. vymazáním, zničením nebo znehodnocením) všechny údaje Správce, které Zpracovatel, jeho přidružené subjekty, Vedlejší zpracovatelé nebo subdodavatelé drží (s výjimkou jakýkoliv a všech kopií dat Správce, které se nacházejí na standardním záložním médiu Zpracovatele za předpokladu, že takové záložní médium je zabezpečeno v souladu s uznávanými a v té době aktuálními osvědčenými postupy o ochraně osobních údajů a bezpečnosti dat). Zpracovatel poskytne Správci písemnou zprávu s odpovídající mírou podrobnosti o datech uložených na záložních médiích, a to na žádost Správce a bez dalších nákladů Správce.
d. Pokud o to Správce požádá, Zpracovatel písemně potvrdí, že došlo k dokončení likvidace.
e. Následující výjimky se považují za výjimky z tohoto požadavku na zneškodnění:
    - Zpracovatel musí uchovávat údaje Správce ve spisu pro právní nebo regulatorní účely; tyto údaje Správce budou poté odstraněny, jakmile uplynou zákonné lhůty pro uchování.
    - Údaje Správce, ohledně kterých Správce požádal, aby je Zpracovatel uchovával archivovány pro účely zachování informací z důvodu soudního řízení.

11. **Bezpečnost systému a řízení technické zranitelnosti**

a. Zpracovatel zavede a bude udržovat pravidla, která prokazují adekvátní použití aktualizací a systémů oprav.
b. Zpracovatel vytvoří a bude udržovat inventáře hardwaru a softwaru a provádět pravidelné kontroly zranitelnosti.
c. Zpracovatel poskytne pravidelné zprávy z prověřování zranitelnosti a přijatých nápravných opatření.
d. Zpracovatel podnikne kroky ke snížení rizik vyplývajících z využívání zveřejněných technických zranitelností. Proces řízení zranitelnosti by měl být zaveden.
e. Na základě výsledků skenování zranitelnosti Zpracovatel odstraní zranitelnosti nejpozději do 30 dnů od data, kdy byly hlášeny;
f. Není-li stanoveno jinak, musí Zpracovatel implementovat zdokumentovaný systém správy aktualizací systému (správa opravy), který by měl zajišťovat implementaci všech potřebných aktualizačních balíků v systémech, které uchovávají, zpracovávají nebo předávají informace Správce.

g. Plánování aktualizací musí oznámit Zpracovatel a musí být odsouhlaseno Správcem v souladu s jejími vlastními pravidly řízení změn.
h. Kdykoli může aplikace aktualizací ovlivnit funkčnost služby poskytované Správci, Zpracovatel iniciuje výjimku ze standardu.

12. **Management incidentů informační bezpečnosti**
a. Zpracovatel zajistí, aby byly zavedeny odpovědnosti a postupy řízení, aby byla zajištěna rychlá, účinná a řádná reakce na bezpečnostní incidenty a aby byly hlášeny a řízeny případy a nedostatky v oblasti bezpečnosti informací.
b. Zpracovatel by měl Správci hlásit jakékoli zjištění porušení osobních údajů do 24 hodin od zjištění.

13. **Monitoring & audit**
a. Zpracovatel použije vhodné systémy a kontroly k odhalování neoprávněných aktivit zpracování informací.
b. Veškeré systémy, které uchovávají, zpracovávají nebo předávají informace Správce, musí zavést systém pro audit událostí bezpečnosti systému, jakož i veškeré činnosti spojené s přístupem, úpravou, zpracováním a/nebo vymazáním informací Správce.
c. Systém auditu musí pro každou událost zapsat minimálně následující informace:
   - Typ události
   - Načasování události (přesný datum a čas);
   - Zdroje události;
   - Výsledek události (úspěch nebo neúspěch);
   - Identitu uživatele spojeného s událostí.
d. Záznamy auditu by měly být chráněny před neoprávněným přístupem a náhodnými změnami.
e. Záznamy auditu, které zaznamenávají události, události týkající se změny a/nebo vymazání informací Správce musí být poskytnuty Správci, pokud o to požádá.
f. U systémů, které jsou považovány za kritické, si Správce vyhrazuje právo požádat o přenos auditních protokolů na vlastní infrastrukturu (vzdálený syslog); technické podrobnosti a přenášené protokoly jsou uvedeny v samostatné příloze.
g. Záznamy o auditu se uchovávají pro záznam nejméně 90 dnů.
h. Zpracovatel musí provést proces revizního protokolu (ruční nebo automatický), aby zjistil jakýkoli neoprávněný přístup k informacím Správce.

14. **Prevence škodlivých kódů**
a. Zpracovatel musí implementovat pravidla, která řídí rizika pro podnikové procesy ze škodlivého kódu a zahrnout ochranu proti malwaru
b. Zpracovatel implementuje zdokumentovaný systém správy aktualizací systému (správa opravy), který by měl zajišťovat implementaci všech potřebných aktualizačních balíčků v systémech, které uchovávají, zpracovávají nebo předávají informace Správce.

15. **Bezpečný rozvoj**
a. Zpracovatel zavede příslušné osvědčené postupy pro bezpečný životní cyklus vývoje.
b. Zpracovatel musí do architektury IT systémů zahrnout odpovídající bezpečnostní řešení (např. firewally, řešení IDS/IPS, šifrování).
c. V případě veřejných systémů (webových serverů apod.) musí Zpracovatel implementovat návrhová řešení, která by měla vyhovovat dobré praxi zabezpečení systému; jako doporučený minimální standard by měly veřejné systémy chránit informace před bezpečnostními riziky v Top 10 OWASP („Open Web Security Project“)

16. **Fyzická bezpečnost a bezpečnost prostředí**
a. Zpracovatel zajistí, aby byly zavedeny příslušné bezpečnostní hranice a vstupní kontroly, aby se zabránilo neoprávněnému fyzickému přístupu, poškození a interferenci do prostor Zpracovatele a informací včetně všech zařízení koncového uživatele.
b. Zpracovatel zajistí, aby bylo zařízení řádně udržováno, aby byla zajištěna jeho dostupnost a celistvost.