

Shrnutí zásad úschovy

Účinné od 5. 8. 2026

Čl.1: Úvod a účel dokumentu

Společnost MP Developers s.r.o. (dále jen „**Poskytovatel**“) v tomto dokumentu dle článku 70 odst. 1 až 3 a článku 75 odst. 1 a 3 Nařízení shrnuje základní zásady nakládání s peněžními prostředky a kryptoaktivity Klientů, svěřenými Poskytovateli Klientem nebo jinak držеныmi nebo kontrolovanými Poskytovatelem v souvislosti s poskytováním Služeb Klientům prostřednictvím Rozhraní Banky, a jejich úschovy a správy.

Pojmy uvedené v tomto Shrnutí zásad úschovy mají význam definovaný v Obchodních podmínkách (dále jen „**Obchodní podmínky**“) a Smlouvě o poskytování služeb platformy (dále jen „**Smlouva o poskytování služeb platformy**“).

V případě rozporu tohoto Shrnutí zásad úschovy s Obchodními podmínkami nebo Smlouvou o poskytování služeb platformy mají Obchodní podmínky a Smlouva o poskytování služeb platformy přednost.

Veškeré takto poskytnuté informace zůstávají v platnosti po dobu trvání Smlouvy o poskytování služeb platformy nebo po dobu platnosti příslušné verze Shrnutí zásad úschovy, dojde-li během trvání Smlouvy o poskytování služeb platformy ke změně aktuálního Shrnutí zásad úschovy.

Čl.2: Opatření k oddělení kryptoaktiv a peněžních prostředků Klientů a zajištění ochrany vlastnických práv Klientů

Poskytovatel uchovává, eviduje a spravuje odděleně kryptoaktiva a peněžní prostředky Klientů od vlastních kryptoaktiv a peněžních prostředků Poskytovatele, zajišťuje ochranu vlastnických práv Klientů a předchází použití kryptoaktiv a peněžních prostředků na svůj vlastní účet kombinací zejména následujících opatření:

Oddělené peněženky

Poskytovatel využívá odlišnou sadu peněženek pro úschovu a správu kryptoaktiv v majetku Poskytovatele a odlišnou sadu peněženek pro úschovu a správu kryptoaktiv v majetku Klientů. Ve vztahu k peněženkám pro úschovu a správu kryptoaktiv Klientů navíc Poskytovatel uplatňuje striktní hierarchii peněženek.

Oddělené bankovní účty

Poskytovatel využívá provozní účty pro evidenci svých vlastních peněžních prostředků a samostatný bankovní účet pro shromažďování a evidenci peněžních prostředků Klientů.

Oddělená evidence u Partnerských burz

Poskytovatel v rámci Partnerských burz zakládá a udržuje dva typy uživatelských profilů a na to navazující evidence v rámci bankovních účtů a interní evidence Partnerské burzy — účet Poskytovatele jako poskytovatele služeb souvisejících s kryptoaktivity dle Nařízení, jednající na účet Klientů, a účet Poskytovatele samotného, při jednání na vlastní účet.

Politika přístupových práv ve vztahu k peněženkám

Poskytovatel uplatňuje politiku přístupových a podpisových práv a procesů, stanovenou odlišně pro peněženky pro úschovu a správu kryptoaktiv v majetku Poskytovatele a peněženky pro úschovu a správu kryptoaktiv v majetku Klientů.

Politika dispozičních oprávnění ve vztahu k bankovním účtům

Poskytovatel uplatňuje politiku dispozičních oprávnění ve vztahu k samostatnému bankovnímu účtu.

Účetní oddělení

Systém vedení účetnictví Poskytovatele zajišťuje účetní oddělením kryptoaktiv a peněžních prostředků v majetku Poskytovatele a kryptoaktiv a peněžních prostředků v majetku Klientů, a oddělené účetní zachycením souvisejících transakcí, stavů a pohledávek.

Právní oddělení

Na základě Obchodních podmínek mají kryptoaktiva a peněžní prostředky v majetku Klientů ve vztahu k Poskytovateli povahu cizího majetku, a tyto prostředky tak na základě právního řádu České republiky jako rozhodného právního řádu v případě platební neschopnosti (úpadku) Poskytovatele nevstupují do majetkové podstaty Poskytovatele.

Evidenční oddělení

Poskytovatel dosahuje evidenčního oddělení kryptoaktiv a peněžních prostředků v majetku Poskytovatele a kryptoaktiv a peněžních prostředků v majetku Klientů, stejně jako kryptoaktiv a peněžních prostředků v majetku jednoho Klienta od kryptoaktiv a peněžních prostředků v majetku jiného Klienta, na základě interní evidence vedené Poskytovatelem, která podléhá pravidelné kontrole shody dat (rekonciliaci).

Organizační uspořádání

Poskytovatel nastavil působnosti a pravomoci jednotlivých organizačních útvarů pracovníků Poskytovatele při poskytování Služeb tak, aby bylo minimalizováno riziko použití kryptoaktiv nebo peněžních prostředků Klientů na vlastní účet Poskytovatele.

Vnitřní kontrola a audit

Poskytovatel podrobuje oblast nakládání s majetkem Klientů výkonu vnitřní kontroly včetně vnitřního auditu a pravidelného externího auditu, ověřujících přiměřenost opatření přijatých za účelem oddělení a ochrany kryptoaktiv a peněžních prostředků Klientů.

Čl.3: Nakládání s peněžními prostředky a uchování peněžních prostředků

3.1 Samostatný bankovní účet

Poskytovatel eviduje peněžení prostředky Klientů svěřené Poskytovateli v rámci poskytování Služeb na samostatném bankovním účtu vedeném pro tento účel Bankou.

3.2 Peněžní prostředky pro udržení likvidity na Partnerských burzách

Poskytovatel za účelem zajištění dostatečné likvidity pro včasné poskytování Služeb, konkrétně služby Provádění pokynů udržuje v nezbytném rozsahu peněžní prostředky Klientů v podobě záloh na provedení Pokynů na bankovních účtech Partnerské burzy. Převod peněžních prostředků Klientů na bankovní účty Partnerské burzy Poskytovatel zajišťuje prostřednictvím poskytovatele platebních služeb. Na základě smluv s Partnerskými burzami jsou peněžní prostředky Klientů, evidované na těchto bankovních účtech, odděleny od peněžních prostředků Poskytovatele. K oddělení peněžních prostředků Klienta od peněžních prostředků jiných Klientů, stejně jako od peněžních prostředků Poskytovatele rovněž slouží interní evidence, vedená Poskytovatelem ve vztahu k účtům Partnerských burz. Partnerské burzy podléhají požadavkům Nařízení a dalších souvisejících právních předpisů v obdobném rozsahu, jakým jim podléhá Poskytovatel, což zajišťuje srovnatelný standard ochrany peněžních prostředků Klientů.

Čl.4: Nakládání s kryptoaktivy a uchování kryptoaktiv

4.1 Základní principy uchovávání kryptoaktiv

Poskytovatel pro evidenci, úschovu a správu kryptoaktiv Klientů používá několik typů adres, resp. peněženek (tzv. wallets) k uložení kryptoaktiv Klientů.

Poskytovatel pro uložení kryptoaktiv Klientů využívá v rámci peněženek souhrnné účty (tzv. omnibus wallets), tedy na jedné peněžence jsou souhrnně uložena kryptoaktiva více Klientů. Oddělení kryptoaktiv jednotlivých Klientů Poskytovatel zajišťuje vedením interní evidence ve vztahu k jednotlivým peněženkám, zajišťující soustavnou a jednoznačnou identifikaci kryptoaktiv konkrétního Klienta.

Poskytovatel v rámci poskytovaných Služeb nedrží prostředky přístupu Klientů ke kryptoaktivům (tj. klíče Klientů). Systém uchování kryptoaktiv Klientů vychází z principu hromadné evidence kryptoaktiv Klientů na jednotlivých peněženkách, kdy tyto peněženky jsou ovládány klíči v držení Poskytovatele.

4.2 Hierarchie peněženek

Poskytovatel využívá vícestupňovou hierarchii peněženek v zájmu zajištění ochrany a současně likvidity uchovávaných kryptoaktiv Klientů. Konkrétně se jedná o následující:

- 1. **Peněženky (účty) Partnerských burz**, které Poskytovatel využívá pro operativní uložení kryptoaktiv Klientů v minimálním objemu nezbytném pro provádění Pokynů Klientů. Partnerské burzy při poskytování služby Úschovy a správy podléhají požadavkům Nařízení a dalších souvisejících právních předpisů v obdobném rozsahu, jakým jim podléhá Poskytovatel, což zajišťuje srovnatelný standard ochrany kryptoaktiv Klientů.
- 2. **Hot wallets**, tedy on-line peněženky, které slouží k operativním účelům včetně výběrů a vkladů kryptoaktiv. Objem kryptoaktiv na peněženkách tohoto typu je omezen politikou řízení likvidity.
- 3. **Cold wallets (střednědobé)**, tedy off-line peněženky, které Poskytovatel využívá pro střednědobé uložení kryptoaktiv. Objem kryptoaktiv na peněženkách tohoto typu je omezen politikou řízení likvidity.
- 4. **Cold wallets (dlouhodobé)**, tedy off-line peněženky, které Poskytovatel využívá pro dlouhodobé uložení kryptoaktiv. Na tomto typu peněženek jsou uložena kryptoaktiva v maximálním možném objemu, který není v souladu s politikou řízení likvidity uložen na peněženkách ostatních kategorií.

4.3 Využití Partnerských burz v rámci služby Úschovy a správy

Poskytovatel v souladu s příslušnými právními předpisy využívá za účelem řádného a včasného poskytování služby Provádění pokynů uložení části kryptoaktiv Klientů na adresách (peněženkách) Partnerských burz, oprávněných k poskytování úschovy a správy kryptoaktiv jménem Klienta dle Nařízení.

Poskytovatel při výběru Partnerských burz uplatňuje proces due diligence zahrnující faktory, které zajišťují standard ochrany kryptoaktiv Klientů dle Nařízení. Plnění těchto faktorů Poskytovatel každoročně přezkoumává. Okruh Partnerských burz stanoví tabulka níže.

Obchodní značka Partnerské burzy	Provozovatel Partnerské burzy	Stát povolení dle Nařízení
Kraken	Payward Europe Solutions Limited	IE
Bybit	Bybit EU GmbH	AT

S výjimkou využití adres (peněženek) Partnerských burz dle tohoto článku Shrnutí zásad úschovy Poskytovatel nevyužívá pro úschovu a správu kryptoaktiv Klientů jiného poskytovatele služeb souvisejících s kryptoaktivy.

Čl.5: Evidence peněžních prostředků a kryptoaktiv Klientů a opatření k usnadnění výkonu práv Klientů

Poskytovatel systémem interní evidence zajišťuje soustavnou a jednoznačnou identifikaci kryptoaktiv a peněžních prostředků každého Klienta způsobem umožňujícím kdykoliv odlišit kryptoaktiva a peněžní prostředky držené pro jednoho Klienta od kryptoaktiv a peněžních prostředků držených pro ostatní Klienty, stejně jako od peněžních prostředků a kryptoaktiv Poskytovatele. Interní evidence zahrnuje rovněž peněženky, resp. účty Partnerských burz, u kterých jsou kryptoaktiva a peněžní prostředky každého Klienta evidovány. Interní evidence plní rovněž roli rejstříku pozic ve smyslu Nařízení.

Poskytovatel zobrazuje Klientovi prostřednictvím Rozhraní Banky stav interní evidence ve vztahu ke Klientovi, a jednou za 3 měsíce generuje výpis z interní evidence, který plní rovněž roli prohlášení o pozici kryptoaktiv ve smyslu Nařízení.

V případě, že je ve vztahu k evidovaným kryptoaktivům nutná reakce Klienta (např. se může jednat o výkon hlasovacích práv v případě úschovy kryptoaktiv charakteru governance tokenů nebo o případ hard forku užitého DLT), Poskytovatel zpřístupní Klientovi tuto informaci prostřednictvím Rozhraní Banky a současně dle Obchodních podmínek zajistí odpovídající reakci.

Došlo-li k události, která pravděpodobně vytvoří nebo změní práva Klienta ve vztahu k danému kryptoaktivu (např. změna užitého DLT = fork, nebo vznik odměny za staking), Poskytovatel informuje Klienta a současně zajistí odpovídající reakci.

Interní evidence Poskytovatele podléhá pravidelné každodenní rekonsiliaci.

Čl.6:

Postupy a lhůty pro vrácení kryptoaktiv

Poskytovatel umožňuje vrácení, resp. vyplacení evidovaných kryptoaktiv Klientovi následujícími dvěma způsoby:

- **Formou Provedení pokynu** k prodeji kryptoaktiv a následným vyplacením peněžních prostředků Klientovi, a
- **Přímým Převodem kryptoaktiv** (výběrem kryptoaktiv) na základě Pokynu **na externí peněženku, resp. adresu Klienta**, hostovanou i nehostovanou, technicky kompatibilní s Platformou, včetně peněženky jiného poskytovatele služeb souvisejících s kryptoaktivy, přičemž tato možnost je dostupná pouze v případě ukončení Smlouvy o poskytování služeb platformy a dalších případů uvedených v Obchodních podmínkách.

Poskytovatel v rámci poskytovaných Služeb nedrží prostředky přístupu Klientů ke kryptoaktivům (tj. klíče Klientů).

Poskytovatel provede Pokyn k výběru kryptoaktiv ve lhůtě 20 pracovních dnů ode dne podání tohoto Pokynu k výběru kryptoaktiv Klientem. V případě výjimečných okolností technické povahy, z důvodů stanovených vnitřními předpisy Poskytovatele, nebo z jiných závažných důvodů, může být tato lhůta překročena, o čemž je Klient Poskytovatelem informován.

Čl.7:

Odpovědnost Poskytovatele za ztrátu kryptoaktiv

Poskytovatel nese odpovědnost vůči Klientovi za ztrátu kryptoaktiv Klienta v důsledku incidentu, který mu lze připsat, a to do výše tržní hodnoty ztraceného kryptoaktiva v době, kdy ke ztrátě došlo.

Incidenty, které nelze připsat Poskytovateli, zahrnují jakoukoli událost, u níž Poskytovatel prokáže, že k ní došlo nezávisle na poskytování služby Úschovy a správyno nezávisle na transakcích Poskytovatele, jako je například problém spojený s vlastním fungováním DLT, kterou Poskytovatel neovládá. Podrobnosti stanoví Obchodní podmínky.

Čl.8:

Řízení provozních rizik a rizik v oblasti IKT v rámci úschovy a správy majetku Klientů

Poskytovatel v rámci úschovy a správy majetku Klientů řídí související provozní rizika, včetně rizik v oblasti IKT. Podrobné postupy stanoví vnitřní předpisy Poskytovatele.

Provozní rizika

Provozní rizika mohou vzniknout v důsledku nedostatečných nebo selhávajících interních procesů Poskytovatele, lidských chyb, selhání systému nebo vnějších událostí. Mezi hlavní zdroje provozních rizik patří:

- **Lidské chyby:** Chyby pracovníků Poskytovatele při správě klíčů, provádění transakcí nebo vedení interní evidence.
- **Selhání procesů:** Slabiny vnitřních postupů pro schvalování transakcí, vedení interní evidence nebo procesů rekonciliace.
- **Fyzická bezpečnost:** Rizika spojená s fyzickým přístupem k významné infrastruktuře, jako jsou servery nebo hardwarové bezpečnostní moduly (HSM).

IKT rizika

IKT rizika zahrnují zranitelnosti infrastruktury pro úschovu a správu kryptoaktiv a peněžních prostředků Klientů. Mezi identifikované zdroje patří zejména:

- **Kybernetická bezpečnost:** Pokusy o hackerství, malware, phishingové útoky nebo jiné formy kybernetických útoků zaměřené na kompromitaci soukromých klíčů nebo přístupových údajů.
- **Výpadky systému:** Neplánované výpadky nebo odstávky systémů používaných ke zpracování transakcí nebo úschově.
- **Rizika integrity dat:** Poškození nebo ztráta dat v důsledku selhání systému, softwarových chyb nebo neoprávněných změn.
- **Rizika třetích stran:** Rizika spojená s využíváním služeb třetích stran pro úschovu, zpracování transakcí nebo IKT infrastrukturu.

Řízení operačních a IKT rizik

Pro řízení operačních a IKT rizik uplatňuje Poskytovatel zejména následující opatření:

- **Rámec kybernetické bezpečnosti:** Poskytovatel využívá víceúrovňový rámec kybernetické bezpečnosti, který zahrnuje brány firewall, systémy detekce narušení a šifrovací protokoly na ochranu před neoprávněným přístupem a kybernetickými útoky.
- **Kontrola přístupu:** Poskytovatel uplatňuje opatření pro kontrolu přístupu, včetně použití hardwarových bezpečnostních modulů (HSM), vícefaktorového ověřování (MFA) a řízení přístupu na základě rolí (RBAC), která omezují přístup k citlivým systémům a údajům.
- **Plán reakce na incidenty:** Poskytovatel zavedl plán reakce na incidenty. Tento plán zahrnuje předem definované role, komunikační strategie a protokoly obnovy, aby se minimalizoval dopad jakéhokoli incidentu.

Čl.9:

Přezkum a audit zásad a systémů úschovy a správy majetku klientů

Poskytovatel zajišťuje roční audit systému úschovy a správy majetku Klientů prováděný nezávislým externím auditorem dle zákona o auditorech. Roční audit zajišťuje nezávislé potvrzení, že systém úschovy a správy majetku Klientů využívá přiměřených opatření, odolá aktuálním hrozbám a konfigurace klíčových komponent splňuje tržní standardy. Zaměření auditu cílí zejména na následující oblasti:

1. logická konfigurace hierarchie peněženek;
2. zabezpečení práce s privátními klíči;
3. proces správy oprávnění pracovníků Poskytovatele.