

Exit  5 Smlouvy o dílo – Exit řešení.

Samotný exit bude realizován dle dodavatelem vypracovaného Exit plánu. Exit plánem se rozumí vypracování dokumentace vymezující postup provedení **Služby exitu**.

1.1 Služba exitu

Službou exitu se rozumí poskytnutí veškeré potřebné součinnosti, dokumentace a informací, účastnění se jednání s ÚVČR a popřípadě třetími osobami za účelem plynulého a řádného převedení všech činností spojených s poskytováním služeb na ÚVČR nebo nového dodavatele tak, jak je uvedeno níže.

Cílem Služby exitu je převést veškeré činnosti, které jsou předmětem plnění ze smlouvy, umožnit převod a další užívání zpracovávaných dat, a zajištění plynulého přechodu na nový informační systém bez omezení činností ÚVČR. Výsledkem Služby exitu bude, že případný nový dodavatel zahájí svoji činnost poskytování služby po stávajícím dodavateli. Pro úspěšnost Služby exitu je esenciální součinnost ÚVČR.

Služby exitu zahrnují zejména:

- účast na jednáních s ÚVČR a popřípadě třetími osobami za účelem plynulého a řádného převedení všech činností spojených s poskytováním plnění,
- provedení analýzy a vypracování (dále jen „**Exit plán**“),
- poskytnutí plnění (součinnost, dokumentace, informace aj.) nezbytných k realizaci tohoto Exit plánu,
- poskytnutí veškeré dokumentace k provozovanému systému,
- na základě provedené analýzy zajištění předání všech dat ÚVČR v předem stanovených formátech. Smyslem migrace dat je převést kompletní data ze stávajícího systému do nového, nahrazujícího předchozí řešení.

1.2 Požadavky na součinnost ÚVČR pro Exit strategii

V rámci plánování, exekuce a dokončení Exit strategie předpokládáme součinnosti ÚVČR uvedené dále. Exit strategii principiálně řídí a implementuje dodavatel, nicméně role ÚVČR je zde nezbytná. A to nejen jako role kontrolní, ale vzhledem k faktu, že dodavatel nemá v rozsahu činností veškerá dotčená aktiva a prvky informačního systému či infrastruktury ÚVČR, tak i jeho role participační.

Detailní seznam potřebných součinností bude také součástí vypracování Exit plánu. Jedná se však primárně o:

- Participace na Exit plánu ve formě jeho schvalování, předpokládaných výstupů a analýzy rizik
- Součinnost na vytváření Exit plánu pro aktiva a prvky, které nejsou v rozsahu plnění dodavatele, ale přesto jsou součástí celkového rozsahu anebo se jedná o systémy související (integrované, závislé apod.)
- Součinnost na vytváření registru rizik pro Exit plán
- Součinnost při transferu znalostí a aktiv na nového dodavatele
- Součinnost dodavateli při ukončení smluvního vztahu (vypořádání, akceptace a finální ukončení)

1.3 Analýza rizik Exit plánu

Riziko	Dopady	Váha rizika	Návrh řešení
Výstupy Exit plánu	Nemožnost nebo obtížná proveditelnost tranzice na jiného dodavatele	Vysoká	Kontrola a odsouhlasení Exit plánu
Migrace nekompletnost předávaných dat	Chybějící entity nebo některé části agendy	Vysoká	Porovnání počtů jednotlivých entit zdrojového a cílového systému
Migrace – struktura předaných dat	Chybějící atributy některých entit, záměna atributů	Vysoká	Kontrola rozsahu migrovaných atributů u dokumentů, spisů, komponent, kontrola vazeb mezi entitami
Nedostatečné kapacity	Zpoždění Exit plánu nebo jeho částí	Střední	Definice součinností v rámci harmonogramu, jejich odsouhlasení a poskytnutí kapacit
Úroveň znalostí nového dodavatele	Kvalita poskytování plnění, SLA	Střední	Otestování zkušeností nového dodavatele objednatel
Součinnost nového dodavatele	Vliv na harmonogram a milníky, případně smluvní ujednání	Střední	Zajištění dostatečných kapacit
Součinnost objednatele nebo stávajícího dodavatele	Vliv na harmonogram a milníky, případně smluvní ujednání	Střední	Ve fázi plánování odsouhlasit rámce součinností a poskytnout zdroje dle schváleného plánu.

Tabulka 1: Analýza rizik exitu

1.4 Harmonogram Služby exitu

Dodavatel zahájí plnění Služby xitu a navrhne harmonogram na základě písemného zadání požadavku ÚVČR. Zde dodavatel předpokládá soulad s harmonogramem spuštění nového eSSL v prostředí ÚVČR. V rámci harmonogramu budou definovány součinnosti za objednatele, dodavatele eSSL a dodavatele nového eSSL.

Při nasazení páteřního systému úřadu – eSSL, je potřeba mít zpracovány záložní plány činností, které mohou vzniknout při neočekávaných stavech u nasazování nového eSSL.

1.5 Realizace Služby exitu

- a) Kompletního převzetí provozu jiným provozovatelem,
- b) převzetí provozu do IT objednatele,
- c) migrace dat (výběr, příprava, extrakce, transformace, přenos) do jiného eSSL,
- d) zničení dat (v souladu s VKB).

1.5.1 Kompletní převzetí provozu jiným provozovatelem

V této variantě exitu je předpoklad na zachování stávající infrastruktury, která je na své základní úrovni ve správě IT ÚVČR.

Obecné předpoklady a součinnosti:

- Zachování stávající infrastruktury, která je na své základní úrovni ve správě OIT ÚVČR.
- Funkční Service Desk nového dodavatele.
- Zajištění režimu podpory provozu ze strany nového dodavatele.
- Nastavení správných procesů podpory u nového dodavatele.
- Možnost podporovat jak aplikační, tak infrastrukturní část předaného plnění.
 - Uskutečnění přechodu na novou infrastrukturu, pokud je přechod součástí předání plnění.
- Uvedení nového dodavatele jako hlavní kontakt v rámci maintenance u výrobců.
- Přesměrování notifikací z provozního monitoringu na nového dodavatele.
- Nový dodavatel musí zajistit přístupy administrátorům ÚVČR pro zakládání ticketů do jeho Service Desku.
- ÚVČR zajistí vytvoření přístupů a relevantních oprávnění pro nového dodavatele.
- Service Desk nového dodavatele musí umět kontrolovat plnění SLA a generovat potřebné reporty.
- Axians s.r.o. poskytne součinnost při předání otevřených ticketů v Service Desku.

Popis předání předmětu plnění:

Předmětem předání plnění jinému dodavateli se myslí předání všech služeb podpory dle Smlouvy o podpoře.

V rámci tohoto předání budou novému poskytovateli podpory provozu vygenerovány reporty všech aktuálně otevřených ticketů a požadavků na rozvoj k datu předání plnění.

1.5.2 Převzetí provozu do OIT objednatele

- Zachování stávající infrastruktury, která je na své základní úrovni ve správě OIT ÚVČR.
- Funkční Service Desk nebo jiný nástroj pro hlášení incidentů.
- Zajištění režimu podpory provozu ze strany ÚVČR.
- Nastavení správných procesů podpory na ÚVČR.
- Možnost podporovat jak aplikační, tak infrastrukturní část předaného plnění.
 - Uskutečnění přechodu na novou infrastrukturu, pokud je přechod součástí předání plnění.
- Uvedení ÚVČR jako hlavní kontakt v rámci maintenance u výrobců.
- Přesměrování notifikací z provozního monitoringu na odpovědné osoby ÚVČR.
- Axians s.r.o. poskytne součinnost při předání otevřených ticketů v Service Desku.

1.5.3 Migrace dat, služba migrace dat

1) Způsob předání dat – dodavatel dodá objednateli data formou exportu do tzv. datové konzervy. Jejím obsahem budou XML soubory jednotlivých entit. Datová konzerva bude předána na požadovanou složku aplikačního serveru hostujícího eSSL, na sdílenou složku nebo na připojené externí datové uložení.

2) Forma předání dat – struktura jednotlivých souborů bude odpovídat schématu XML pro výměnu dokumentů a jejich metadat dle aktuálně platného NSESSS.

3) Objem předaných dat – Součástí migrace budou všechna data od zahájení evidence v eSSL ke dni, který písemně sdělí ÚVČR dodavateli. Do exportu budou zahrnuty entity ve všech stavech

svého životního cyklu. Informace o množství exportovaných dat bude zanesena do dokumentu „Protokol o migraci“.

Objem dat bude popsán způsobem obsahující:

Počet spisů

Počet dokumentu

Počet komponent

Datový objem

Počet exportovaných/migrovaných entit je závislý na harmonogramu a datu zahájení exitu.

Protokol o migraci – dodavatel dodá protokol popisující proces předání dat, způsob předání dat, formu předání dat, objem předaných dat a výsledek kontroly struktury dat.

1.5.4 Zničení dat (v souladu s VKB)

Platí, že:

- 1) Zhotovitel se zavazuje pro likvidaci dat řídit VKB
- 2) Zhotovitel se zavazuje při zpracování osobních dat ze strany objednatele použít taková technická, organizační a personální opatření, aby ochránil důvěrnost těchto dat, jejich přístupnost objednateli na vyžádání a případně bezpečnou likvidaci
- 3) Zhotovitel zajišťuje migraci dat z předchozího (eSSL) do nového (eSSL).
- 4) Zhotovitel v rámci Exit strategie předá data, případně zajistí jejich likvidaci, zpět objednateli a novému dodavateli.
- 5) Zhotovitel se zavazuje informace a dokumenty související se Smlouvou držet po dobu deseti let od uhrazení poslední faktury objednatelem.
- 6) Zhotovitel se zavazuje dle znění Smlouvy ochraňovat důvěrná data objednatele jako svá vlastní, tj. uplatňuje příslušná organizační a technická opatření za účelem ochrany a případně likvidace těchto informací
- 7) Provozovatelem eSSL se po dovršení projektu stává objednatel, zhotovitel se stává dodavatelem, podílejícím se na provozu skrze servisní, vývojové a implementační požadavky, případně další školicí požadavky.

Předpokládá se v rámci plnění předmětu smlouvy výskyt množin informací:

- 1) Zákaznická data (ta tvoří primární aktivum (informace), které eSSL bude nadále zpracovávat),
- 2) osobní data zaměstnanců objednatele,
- 3) provozní data (IP rozsahy, informace o lokalitách atd.),
- 4) instalační, záložní a archivní média (zdrojový kód instance, instalační balíčky instance atd.),
- 5) důvěrné informace (definováno ve Smlouvě v kapitole „Ochrana důvěrných informací“).

Způsob vypořádání jednotlivých skupin dat:

- 1) Migrace zákaznických dat mezi systémy bude probíhat v provozním prostředí Objednatele. Pro likvidaci redundantních dat se předpokládá, že Objednatel poskytne vlastní digitální skartační řád, kterým se bude Zhotovitel po zakončení fáze migrace řídit.
- 2) Osobní data jsou především ta, kterých Zhotovitel nabyl nebo nabude pro účely plnění Smlouvy, kontaktní údaje styčných osob a administrátorů na straně Objednatele, případně

osobní data získaná pro účely školení. V rámci exit strategie vezme Zhotovitel v potaz taková data, která je povinen dle znění Smlouvy uchovat po dobu deseti let od poslední Objednatelem splacené faktury, a data, která je povinen držet v rámci nadcházející servisní podpory, ostatní data vyhodnocená jako irrelevantní pro další plnění, považuje Zhotovitel dle přílohy č.1 VKB za vysoké důležitosti a podle toho přistupuje k jejich ukládání, ochraně a likvidaci. Zvolený způsob uložení je Microsoft Sharepoint Cloud s aktivním opatřením DLP (Data Loss Prevention) pro ochranu Office dokumentů a souborů PDF. Likvidaci těchto dat obstarává DLP funkcionalita revokace platnosti certifikátů. Ostatní data uložená na on-premise file serveru Zhotovitele nebo na fyzických přenositelných nosičích jsou likvidována dle DoD 5220.22-M standardu.

- 3) Pro provozní data je využíván stejný proces šetření, ochrany a likvidace jako pro osobní data. K provozním datům se přistupuje jako k aktivu vysoké úrovně.
- 4) Instalační, záložní a archivní data budou ošetřena následovně: Ve fázi exit strategie budou veškeré nadpotřebné kopie těchto souborů uložené na systémech Zhotovitele zničeny. Funkční zdrojový kód a instalační soubory budou umístěny na speciálním datovém úložišti vývojové skupiny, která je určena a zabezpečena pro ukládání tohoto typu dat. K tomuto aktivu se přistupuje jako ke kritickému (jako vyplývá i z analýzy rizik v hodnocení zdrojového kódu aplikace).
- 5) Důvěrné informace budou dle znění Smlouvy uchovány až po dobu deseti od proplacení poslední faktury Objednatelem. Jde o data, kterých Zhotovitel nabyl po uzavření Smlouvy a během jejího plnění, která nepokrývají předchozí zmiňované množiny dat, ale lze je hodnotit jako důvěrná dle ujednání Smlouvy. Data budou umístěna na sharepoint cloudu pod ochranou DLP – chráněny budou soubory Office formátů a pdf soubory. V případě nutnosti předčasné likvidace vyvolané Objednatelem lze data pomocí funkcionality DLP zneplatnit. K této množině informací se přistupuje jako k aktivu vysoké úrovně.