Evidenční číslo smlouvy MPO: 149/25/31700

SMLOUVA O VYTVOŘENÍ, ROZVOJI INFORMAČNÍHO SYSTÉMU JePEK, SLUŽBÁCH PROVOZU A SLUŽBÁCH PODPORY

*ve smyslu ustanovení § 1746 odst. 2, § 2586 a násl. a § 2358 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů („**OZ**“ nebo „**Občanský zákoník**“)*

(„**Smlouva**“)

SMLUVNÍ STRANY:

Česká republika – Ministerstvo průmyslu a obchodu

se sídlem: Na Františku 1039/32, 110 00 Praha 1

IČO: 476 09 109

DIČ: CZ 476 09 109

zastoupená: Ing. Pavlem Vinklerem, Ph.D., LL.M., ředitelem odboru

(„**Objednatel**“)

a

ASD Software, s.r.o.

se sídlem: Žerotínova 2981/55A, 787 01 Šumperk

IČO: 62363930

DIČ: CZ62363930

Bankovní spojení: Komerční banka, a.s.

Číslo účtu: [redacted]

zapsaná v obchodním rejstříku vedeném u Krajského soudu v Ostravě, sp. zn: C7973

zastoupená: Ing. Petrem Poláchem, jednatelem společnosti

(„**Poskytovatel**“)

(Objednatel a Poskytovatel společně „**Smluvní strany**“ a jednotlivě „**Smluvní strana**“)

VZHLEDEM K TOMU, ŽE:

A. Objednatel je veřejným zadavatelem ve smyslu ustanovení § 4 odst. 1 písm. a) zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů („**ZZVZ**“);

B. Poskytovatel prohlašuje, že je:

a) právnickou osobou založenou podle některého z právních řádů členského státu Evropské unie zapsanou do příslušného rejstříku dle daného právního řádu;

b) splňuje veškeré podmínky a požadavky v této Smlouvě stanovené;

c) oprávněn podnikat v oboru činnosti poskytování software, poradenství v oblasti informačních technologií, zpracování dat, hostingové a související činnosti a webové portály podle přílohy č. 4 nařízení vlády č. 278/2008 Sb., o obsahových náplních jednotlivých živností, ve znění pozdějších předpisů; a

d) ke dni uzavření této Smlouvy vůči němu není vedeno řízení dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů, ani neví o skutečnostech, které by k jeho zahájení v době uzavření této Smlouvy vést mohly a zároveň se zavazuje Objednatele o všech skutečnostech o hrozícím úpadku bezodkladně informovat.

C. Objednatel v souladu s ustanovením § 2 odst. 3 ZZVZ vyhlásil dne 6. 5. 2025 zadávací řízení dle § 3 písm. b ZZVZ („**Zadávací řízení**“) na nadlimitní veřejnou zakázku na realizaci a dodání projektu s názvem „**JePEK**“, jehož předmětem plnění má být vytvoření *„Agendového informačního systému JePEK“* („**AIS JePEK**“ nebo „**AIS**“), vedenou pod č. N 006/23/V00017025 („**Veřejná zakázka**“). V rámci tohoto Zadávacího řízení proběhlo výběrové řízení v souladu s příslušnými ustanoveními ZZVZ, v němž Poskytovatel předložil v souladu se zadávacími podmínkami Veřejné zakázky nabídku („**Nabídka**“) a tato Nabídka byla Objednatelem s ohledem na hodnotící kritéria nabídek vybrána jako nejvhodnější. Nabídková cena byla v celkové výši **35 652 176 Kč bez DPH**;

D. Poskytovatel prohlašuje, že má know-how a technologie k vytvoření, realizaci, vývoji a následnému provozu předmětu Veřejné zakázky;

SE SMLUVNÍ STRANY DOHODLY TAKTO:

1. Účel Smlouvy

1.1. Účelem této Smlouvy je úprava a stanovení podmínek mezi Smluvními stranami tak, aby bylo ze strany Poskytovatele zajištěno plnění předmětu Veřejné zakázky, a aby ze strany Objednatele byla zajištěna úhrada odměny za řádné plnění této Smlouvy Poskytovatelem.

1.2. Účelem této Smlouvy je zejména úprava podmínek pro vytvoření a uvedení do provozu informačního systému JePEK Poskytovatelem. Dále je účelem této Smlouvy mimo jiné úprava podmínek pro zajištění oprávnění Objednatele k užití a rozvoji AIS JePEK tak, aby byl otevřený ve smyslu možnosti Objednatele zadávat jeho další podporu, provoz a rozvoj v otevřené soutěži co nejširšího počtu Poskytovatelů nebo možnosti Objednatele zajistit takovou další podporu, provoz a rozvoj svým vlastním personálem bez toho, aby byl Objednatel omezen výhradními právy Poskytovatele či třetích osob váznoucích bez řádného důvodu na informačním systému AIS JePEK, jakož i zajištění oprávnění sdílet zdrojové kódy informačního systému s dalšími určenými subjekty za účelem podílu těchto subjektů na rozvoji AIS JePEK. Mimo výše uvedené je účelem této Smlouvy také upravit a stanovit pravidla a podmínky pro poskytování služeb provozu, podpory a rozvoje AIS Poskytovatelem Objednateli.

1.3. Touto Smlouvou se Poskytovatel zavazuje vůči Objednateli dosáhnout účelu této Smlouvy a zavazuje se dále naplnit zadání Veřejné zakázky společně se všemi jejími podmínkami a povinnosti stanovenými v zadávací dokumentaci Veřejné zakázky Objednatelem („**Zadávací dokumentace**“), s níž se Poskytovatel seznámil v plném rozsahu.

2. Předmět Smlouvy

2.1. Předmětem této Smlouvy je provedení předmětu Veřejné zakázky, tj. AIS JePEK, dle Zadávací dokumentace. Předmětem této Smlouvy je dodání díla ve smyslu čl. 2.2. této Smlouvy a poskytování služeb ve smyslu čl. 2.3. a 2.4. této Smlouvy.

2.2. Poskytovatel se touto Smlouvou zavazuje dodat pro Objednatele dílo, a to dle Zadávací dokumentace a za podmínek stanovených v této Smlouvě spočívající v:

a) vytvoření AIS JePEK, tj. jeho vývoj, jeho realizace, jeho dodání a implementace v prostředí Objednatele a jeho testování. Poskytovatel zhotoví pro Objednatele AIS JePEK tak, aby odpovídal specifikaci technického řešení uvedeného v Příloze č. 4 – Technická dokumentace;

b) dodání kompletní uživatelské a provozní dokumentace vztahující se k AIS v souladu se zákonem č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších právních předpisů („**ZISVS**“) a udělení příslušných užívacích a souvisejících oprávnění („**Dokumentace**“);

c) poskytování součinnosti Objednateli nezbytné k ověřování funkčnosti dodávaného AIS; a zajištění systémové podpory pro zaškolení, školení, přeškolení a doškolení uživatelů AIS;

(společně „**Dílo**“).

2.3. Poskytovatel se dále touto Smlouvou zavazuje poskytnout Objednateli rozvoj AIS a k poskytování souvisejících konzultací, a to dle požadavků Objednatele po celou dobu účinnosti Smlouvy v rozsahu stanoveném v Příloze č. 2 této Smlouvy („**Služby rozvoje**“).

2.4. Poskytovatel se dále zavazuje poskytnout Objednateli dle této Smlouvy služby provozu a údržby AIS a podpory jeho uživatelů po uvedení AIS do provozu, a to v rozsahu a dle podmínek stanovených v Příloze č. 3 této Smlouvy („**Služby provozu**“ a „**Služby podpory**“) (Služby rozvoje, Služby provozu a Služby podpory společně „**Služby**“).

2.5. Objednatel se zavazuje zaplatit Poskytovateli dohodnutou cenu za:

a) řádně a včas provedené Dílo podle Harmonogramu uvedeného v Příloze č. 6 této Smlouvy, za podmínek sjednaných v Příloze č. 1 této Smlouvy v souladu se Specifikací ceny plnění uvedené v Příloze č. 5 této Smlouvy;

b) Služby rozvoje poskytnuté za podmínek stanovených v Příloze č. 2 této Smlouvy v souladu se Specifikací ceny plnění uvedené v Příloze č. 5 této Smlouvy; a

c) Služby provozu a Služby podpory za podmínek stanovených v Příloze č. 3 této Smlouvy v souladu se Specifikací ceny plnění uvedené v Příloze č. 5 této Smlouvy.

2.6. Objednatel se současně zavazuje poskytnout Poskytovateli potřebnou součinnost s realizací Díla a s poskytováním Služeb dle této Smlouvy, jakož i součinnost, která se ukáže být nezbytná k řádné realizaci plnění dle této Smlouvy a dále, bude-li to pro řádné poskytování plnění dle této Smlouvy nezbytné, zřídit ve prospěch Poskytovatele nezbytné přístupy do systémů Objednatele. Pokud by zřízení nezbytných přístupů bylo v rozporu s právními předpisy či jinými vnitřními a organizačními předpisy Objednatele, či jiné osoby s Objednatelem spojené v rámci jeho obchodní činnosti, upozorní na tuto skutečnost Poskytovatele. Poskytovatel se v takovém případě zavazuje poskytnout Objednateli nejpozději do 5 pracovních dnů informace o důvodu nutnosti zřízení takového přístupu, možných alternativních řešeních a možných negativních dopadech na realizaci plnění podle této Smlouvy v případě, že nebude takový přístup povolen. Splní-li Poskytovatel svou informační povinnost dle předchozí věty, nezapočítává se doba procesu podle tohoto článku do doby prodlení Poskytovatele s plněním. Po obdržení nezbytných informací od Poskytovatele vyvine Objednatel nezbytné úsilí pro projednání podkladů obdržených od Poskytovatele za účelem nalezení možného řešení situace.

3. Závazky Poskytovatele

3.1. Poskytovatel se zavazuje poskytovat plnění dle této Smlouvy vlastním jménem, na vlastní odpovědnost sám, nebo s využitím subPoskytovatelů uvedených v Příloze č. 8 této Smlouvy, byli-li takoví subPoskytovatelé uvedeni v Nabídce v souladu s ustanovením čl. 12 Zadávací dokumentace („**SubPoskytovatelé**"), v souladu s pokyny Objednatele řádně a včas dle Harmonogramu stanoveného v Příloze č. 6 této Smlouvy, a to v nejvyšší možné kvalitě pro relevantní trh poskytovaných služeb.

3.2. Poskytovatel se zavazuje postupovat při plnění této Smlouvy tak, aby nedošlo k poškození dobrého jména Objednatele, a to ani v případě, bude-li plnění Smlouvy zajišťovat prostřednictvím svých SubPoskytovatelů, za jejichž plnění vždy odpovídá, jako by jej poskytoval sám.

3.3. Poskytovatel se zavazuje na plnění dle této Smlouvy alokovat pracovní kapacitu osob realizačního týmu uvedeného v Příloze č. 7 této Smlouvy a k plnění dle této Smlouvy využít výhradně těchto osob. Objednatel je oprávněn požadovat nahrazení člena realizačního týmu jinou osobou spolu s uvedením relevantního důvodu; za relevantní důvod se pro tyto účely považují případy, kdy nenahrazení člena realizačního týmu by bylo odůvodněně způsobilé zapříčinit (i) ohrožení řádného a včasného plnění této Smlouvy ze strany Poskytovatele, (ii) újmu na pověsti Objednatele. Objednatel je rovněž oprávněn požadovat nahrazení člena realizačního týmu jinou osobou z důvodu nemožnosti spolupráce takového člena realizačního týmu s Objednatelem. Poskytovatel se v takovém případě zavazuje nahradit osobu realizačního týmu takovou osobou, která disponuje obdobnými znalostmi, zkušenostmi a kvalifikací, a to do 10 pracovních dnů, nedohodnou-li se Smluvní strany na jiné lhůtě. Čas a prostředky investované do zaškolení takové osoby nese výlučně Poskytovatel. Jakákoliv změna člena realizačního týmu je možná pouze po předchozím písemném oznámení takto zamýšlené změny Poskytovatelem Objednateli a jejím schválení Objednatelem.

3.4. Poskytovatel je povinen upozorňovat Objednatele včas na všechny hrozící vady či výpadky svého plnění a neprodleně oznámit písemnou formou Objednateli překážky, které mu brání v plnění předmětu Smlouvy, a to na kontaktní e-mailové adresy Objednatele uvedené v Příloze č. 9 k této Smlouvě (odpovědnost Poskytovatele za škodu a vznik nároku Objednatele na uplatnění smluvních pokut za podmínek uvedených v této Smlouvě tímto nejsou dotčeny). Poskytovatel je povinen předcházet vzniku jakékoliv škody ve vztahu k Objednateli.

3.5. Poskytovatel je povinen informovat Objednatele o plnění svých povinností dle této Smlouvy a důležitých skutečnostech, které mohou mít vliv na výkon práv a povinností Smluvních stran, a to na kontaktní e-mailové adresy Objednatele uvedené v Příloze č. 9 této Smlouvy.

3.6. Poskytovatel se zavazuje dodat příslušnou Dokumentaci s náležitostmi dle příslušných právních předpisů v takovém rozsahu a na takové úrovni, aby odpovídala požadavkům potřebným

pro dokumentaci infomačního systému typu AIS JePEK a splňuje dále všechny tržní standardy pro obdobné projekty. Dokumentace sestává mimo jiné nikoliv však výlučně z:

a) Technické dokumentace obsahující zejména, nikoliv však výlučně:

(i) High-level a low-level design systému,

(ii) Architekturu skutečného stavu po implementaci,

(iii) Dokumentaci API a integračních vazeb,

(iv) Datový model a popis databázových struktur, a

(v) Zdrojové kódy včetně verzování a dokumentace.

b) Provozní a administrátorské dokumentace obsahující zejména, nikoliv však výlučně:

(i) Manuál pro správu systému,

(ii) Provozní příručku a postupy údržby,

(iii) Bezpečnostní opatření a řízení přístupů, a

(iv) Zálohovací a obnovovací procedury (Disaster Recovery Plan).

c) Dokumentace testování obsahující zejména, nikoliv však výlučně:

(i) Záznamy o provedených akceptačních testech (FAT, UAT, penetrační testy),

(ii) Testovací scénáře a jejich výsledky, a

(iii) Výsledky zátěžových testů a stress testů.

d) Uživatelské dokumentace obsahující zejména, nikoliv však výlučně:

(i) Uživatelskou příručka pro běžné uživatele, a

(ii) Školící materiály pro administrátory a provozní tým.

3.7. Poskytovatel se zavazuje provést aktualizaci příslušné Dokumentace a zdrojových kódů při předání každé jednotlivé fáze Díla a v případě uskutečnění jakékoliv změny Díla po dokončení Díla v rámci Služeb rozvoje na základě této Smlouvy.

3.8. Poskytovatel se zavazuje zajistit plnou funkčnost Díla i jen jeho částí v době jejich předání a akceptace v souladu s touto Smlouvou. AIS musí být optimalizován pro stabilní a nepřerušovaný provoz, přičemž Poskytovatel odpovídá za odstranění jakýchkoli vad nebo nedostatků, které by bránily jeho řádnému fungování.

3.9. Poskytovatel je povinen zajistit dostatečný serverový prostor pro provoz AIS na serveru v prostředí cloud computingu v minimální úrovni 2 (střední) v souladu s požadavky dle ZISVS a v souladu se

Zadávací dokumentací, a to na základě dohody Smluvních stran. Server, na kterém bude AIS provozován, musí splňovat mimo jiné následující bezpečnostní standardy:

a) použití aktuálních verzí softwaru a pravidelné bezpečnostní aktualizace,

b) ochrana proti neoprávněnému přístupu, včetně šifrované komunikace (SSL/TLS), dvoufaktorové autentizace a řízení přístupových práv,

c) pravidelné bezpečnostní audity a monitoring provozu za účelem prevence a detekce bezpečnostních hrozeb,

d) dostatečná ochrana proti DDoS útokům a jiným typům kybernetických hrozeb, a

e) fyzická bezpečnost serveru včetně kontroly přístupu do datového centra, redundantního napájení a záložních mechanismů pro případ výpadku elektřiny či síťového připojení.

3.10. Poskytovatel se zavazuje vytvořit AIS tak, aby jej bylo možné plnohodnotně provozovat a testovat v testovacím prostředí, jehož parametry, technické specifikace a rozsah jsou definovány v Příloze č. 4 této Smlouvy („**Testovací prostředí**“). Funkcionalita AIS v Testovacím prostředí musí odpovídat funkcionalitě určené pro produkční prostředí v rozsahu potřebném pro provedení testování v souladu s ustanoveními této Smlouvy, zejm. pak Přílohy č. 4.

3.11. Poskytovatel se zavazuje udržovat v platnosti a účinnosti po celou dobu trvání této Smlouvy pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou Poskytovatelem třetí osobě (zejména Objednateli), a to tak, že limit pojistného plnění vyplývající z pojistné smlouvy nesmí být nižší než 10.000.000 Kč za rok. Pojistný certifikát dle tohoto odstavce tvoří Přílohu č. 11 k této Smlouvě. Poskytovatel je kdykoliv po písemném vyžádání Objednatele povinen předložit aktuální pojistný certifikát.

3.12. Poskytovatel se zavazuje při zhotovování Díla ke konci každého kalendářního roku zaslat Objednateli report o postupu prací na Díle, ve kterém alespoň stručně popíše současný stav Díla a zhodnotí plán jeho realizace v porovnání s Harmonogramem, který tvoří Přílohu č. 6 této Smlouvy.

3.13. Poskytovatel se zavazuje zajistit po celou dobu trvání této Smlouvy, ať už půjde o realizaci Díla nebo poskytování Služeb, aby byla kybernetická ochrana a veškeré další zákonné povinnosti v souvislosti s kybernetickou bezpečností AIS JePEK v souladu s platnou a účinnou legislativou týkající se kybernetické bezpečnosti, zejména, nikoliv však výlučně se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů („**ZoKB**“), a to i za okolností, že dojde ke změně legislativy týkající se kybernetické bezpečnosti v průběhu trvání této Smlouvy. Smluvní strany se dohodly, že veškerá opatření, která v souvislosti s touto svou povinností podnikne jsou zahrnuty v ceně Díla a v cenách Služeb. Poskytovatel se zavazuje postupovat při plnění předmětu této Smlouvy v souladu s Přílohou č. 12 této Smlouvy (Smluvní ujednání v rámci zákona o kybernetické bezpečnosti).

3.14. Poskytovatel je v souvislosti se zhotovením Díla dle této Smlouvy povinen učinit veškerá opatření směřující ke spolehlivé ochraně AIS a dat obou Smluvních stran. Poskytovatel je povinen poskytovat Objednateli veškeré relevantní údaje a další informace související s realizací Díla (AIS), poskytováním Služeb a bezodkladně informovat Objednatele o hrozícím nebo vzniklém ohrožení řádného výkonu činnosti Poskytovatele podle této Smlouvy, jakož i o jakýchkoliv okolnostech, které by mohly mít negativní vliv na schopnost Poskytovatele řádně a včas plnit povinnosti dle této Smlouvy, jakož i bezodkladně informovat Objednatele v případě, že dojde k narušení, prolomení či jiného incidentu ochranného systému Poskytovatele, a to včetně kybernetických bezpečnostních incidentů, či jiných obdobných rizik („**Bezpečnostní rizika**“). Poskytovatel je povinen v případě nastalého či hrozícího Bezpečnostního rizika Objednateli poskytnout veškeré Objednatelem vyžádané informace či podklady vztahující se k takovému Bezpečnostnímu riziku. Poskytovatel se zavazuje zajistit po celou dobu trvání této Smlouvy úroveň zabezpečení odpovídající aktuálnímu standardu na trhu, a dále je povinen mít připravený a implementovaný plán pro realizaci plnění podle této Smlouvy, pro zajištění kontinuity poskytování plnění v případě výskytu jakéhokoliv nežádoucího stavu, kybernetického útoku či jakékoliv jiné události, která by mohla ohrozit řádné a plnění podle této Smlouvy.

3.15. V případě předčasného ukončení této Smlouvy z jakéhokoliv důvodu se Poskytovatel zavazuje poskytnout veškerou nezbytnou součinnost při předání Díla nebo poskytování Služeb novému poskytovateli. Poskytovatel je povinen v přiměřené lhůtě stanovené Objednatelem a nebude-li toto datum stanoveno, pak k okamžiku ukončení Smlouvy:

a) předat Objednateli v elektronické podobě veškerá Poskytovateli dostupná provozní, vývojová či testovací data či uživatelské údaje obsažené AIS JePEK vytvořeném a/nebo provozovaném Poskytovatelem na základě Smlouvy, a/nebo na žádost Objednatele poskytnout součinnost k migraci těchto dat, a to i vůči třetím stranám určeným Objednatelem,

b) umožnit Objednateli provést migraci dat a poskytnout potřebnou součinnost při její přípravě a realizaci, a to i vůči třetím stranám určeným Objednatelem,

c) protokolárně vymazat nebo jinak zlikvidovat veškerá Poskytovateli dostupná data či uživatelské údaje, programy a elektronickou dokumentaci Objednatele, které byly Poskytovateli zpřístupněny na základě Smlouvy nebo v souvislosti s ní, a to dle písemných pokynů a termínů stanovených Objednatelem. Poskytovatel je povinen před likvidací dat zajistit úplné předání všech dat Objednateli. Poskytovatel je povinen upozornit Objednatele v případě, že Objednatel požaduje smazání dosud nepředaných dat na tuto skutečnost a bez opětovného potvrzení Objednatelem taková data nemazat,

d) předat Objednateli komplexní aktuální programy a dokumentaci dle Smlouvy v termínu Objednatelem stanoveném,

e) předat Objednateli všechna hesla, šifrovací klíče, certifikáty a další autentizační prostředky a rovněž také data ze svých podpůrných systémů, především Help Desk a Service Desk, které Objednateli umožní administrátorský přístup k veškerým datům, databázím, systémům a dalším technickým prostředkům potřebným pro poskytování služeb, a to v termínu Objednatelem stanoveném,

f) předat Objednateli všechny konfigurační soubory potřebné pro provoz AIS a provoz služeb v termínu Objednatelem stanoveném, a to do 15 pracovních dnů od požadavku Objednatele,

g) poskytnout konzultace Objednateli a případnému novému poskytovateli spojené zejména s přípravou nového poskytovatele na výkon služeb, a to do 3 pracovních dnů od požadavku Objednatele na poskytnutí těchto konzultací,

h) předat kompletní komunikační matice (poskytnutí přehledu všech nutných kontaktních/kompetentních osob pro poskytování služeb, včetně kontaktů na SubPoskytovatele Poskytovatele), a to do 15 pracovních dnů od požadavku Objednatele,

i) poskytnout požadované informace, data i dokumentaci, a to i opakovaně tak, aby mohla být bezproblémově zajištěna příprava migrace, test migrace i produkční migrace.

Dále k okamžiku ukončení Smlouvy vznikají Poskytovateli následující závazky:

a) předložit Objednateli konečné vyúčtování vzájemných pohledávek z plnění poskytnutého v souladu se Smlouvou, a to do třiceti (30) dnů od ukončení Smlouvy,

b) neprodleně uhradit všechny případné nedoplatky vůči Objednateli,

c) pokud v okamžiku ukončení Smlouvy nebyly některé poskytované Služby ukončeny a jejich okamžité ukončení není možné, neboť je Objednatel musí zajistit, neprodleně vypracovat za součinnosti Objednatele plán ukončení Služeb včetně jejich migrace („**Exit plán**“), jehož předmětem bude plán postupného ukončení služeb, které byly v okamžiku ukončení Smlouvy poskytovány Objednateli, dle požadavků Objednatele za účelem minimalizace dopadů jejich ukončení na činnost Objednatele zabezpečovanou Službami; uvedené se týká i rozpracovaných objednávek Služeb, kdy veškeré přijaté objednávky Služeb budou vyřízeny původním Poskytovatelem, nedohodnou-li se Smluvní strany jinak,

d) pokud v okamžiku ukončení Smlouvy nebyly některé poskytované Služby ukončeny a jejich okamžité ukončení není možné, neboť je Objednatel musí zajistit, a to od okamžiku ukončení Smlouvy až do akceptace splnění Exit plánu a způsobem definovaným ve Smlouvě, i nadále poskytovat tyto Služby v rozsahu, ve kterém byl Poskytovatel dle Smlouvy povinen je poskytovat v okamžiku ukončení Smlouvy, nestanoví-li Objednatel rozsah nižší; za tyto činnosti náleží Poskytovateli úplata ve výši adekvátní ceny, za kterou byl Poskytovatel tyto

Služby povinen poskytovat v okamžiku ukončení Smlouvy. Doba realizace Exit plánu nepřesáhne trvání 6 měsíců od ukončení Smlouvy,

e) poskytnout konzultace Objednateli nebo případnému novému poskytovateli Služeb nebo provozovateli infrastruktury po dobu 6 měsíců od ukončení Smlouvy. Poskytovateli náleží za takové konzultace úplata ve výši jednotkové sazby za člověkoden poskytování Služeb stanovené Smlouvou.

3.16. Poskytovatel podpisem této Smlouvy:

a) prohlašuje a zaručuje, že Poskytovatel, jakož i každá osoba jednající jeho jménem, není sankcionovanou osobou dle mezinárodních sankcí vůči Rusku a Bělorusku ve smyslu nařízení Rady (EU) č. 269/2014, nařízení Rady (EU) č. 208/2014 a nařízení Rady (ES) č. 765/2006 (vše ve znění pozdějších předpisů). Tzn., že se nenachází na tzv. sankčních seznamech;

b) prohlašuje a zaručuje se, že splňuje podmínky Nařízení Rady (EU) 2022/576 ze dne 8. dubna 2022, kterým se mění nařízení (EU) č. 833/2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, ve znění pozdějších předpisů;

c) prohlašuje a zaručuje se, že není subjektem, jejž veřejní zadavatelé dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, mají povinnost vyloučit ze zadávacího řízení;

d) prohlašuje a zaručuje se, že si není vědom skutečnosti, že by se výše uvedené mezinárodní sankce vztahovaly na SubPoskytovatelé, které budu v průběhu plnění veřejné zakázky využívat;

e) se zavazuje ověřit a zajistit, že veškeré subdodávky, které budou součástí plnění dle této Smlouvy i všichni SubPoskytovatelé Poskytovatele, kteří se budou podílet na plnění této Smlouvy, splní podmínky uvedené v tomto čl. výše.

Pokud Poskytovatel v průběhu účinnosti této Smlouvy zjistí, že prohlášení dle tohoto čl. nejsou pravdivá, nebo zjistí, že jeho SubPoskytovatelé či subdodávky nesplňují podmínky dle tohoto čl., je povinen o tom Objednatele bezodkladně informovat. V případě, že Poskytovatel poruší jakoukoli povinnost dle tohoto čl. a/nebo Objednatel zjistí, že prohlášení Poskytovatele dle tohoto čl. jsou nepravdivá a/nebo zjistí, že SubPoskytovatelé či subdodávky nesplňují podmínky dle tohoto čl., je Objednatel oprávněn od této Smlouvy odstoupit, a to s účinností ke dni doručení odstoupení Poskytovateli.

4. Závazky Objednatele

4.1. Objednatel je povinen řádně a včas hradit cenu Díla, Služeb rozvoje, Služeb provozu a Služeb podpory, a to dle pravidel stanovených v této Smlouvě na základě vystavených daňových dokladů – faktur.

4.2. Objednatel výlučně odpovídá za odbornou zdatnost osob spolupracujících za Objednatele s realizačním týmem Poskytovatele při plnění této Smlouvy.

4.3. Objednatel se touto Smlouvou zavazuje na základě žádosti Poskytovatele poskytnout Poskytovateli při provádění Díla, při poskytování Služeb potřebnou, avšak jen rozumně očekávatelnou součinnost, spolupráci („**Součinnost**“). U poskytování dat a informací ze strany Objednatele je třeba vždy brát v potaz, že Součinnost bude v tomto případě poskytována ve lhůtách s přihlédnutím k tomu, že taková podléhá vnitřním předpisům Objednatele jako ústředního správního úřadu; případné opakované prodloužení lhůty k poskytnutí součinnosti nebude považováno za porušení povinnosti ze strany Objednatele.

4.4. Objednatel je povinen informovat Poskytovatele o důležitých skutečnostech, které mohou mít vliv na plnění této Smlouvy ze strany Poskytovatele, a to na kontaktní e-mailové adresy Poskytovatele uvedené v Příloze č. 9 této Smlouvy.

4.5. Objednatel a Poskytovatel se zavazují každoročně formou dodatku k této Smlouvě upravit cenu Služeb o procentuální nárůst vykazované míry ročního růstu indexu spotřebitelských cen v České republice vyhlášený Českým statistickým úřadem za předcházející kalendářní rok, a to vždy k 1. 1., maximálně však o 5 %.

5. Platnost a trvání Smlouvy

5.1. Smlouva se uzavírá na dobu určitou, **a to ode dne nabytí účinnosti této Smlouvy do 31. března 2032.**

5.2. Smluvní vztah založený touto Smlouvou může být ukončen:

a) v části realizace Díla:

(i) řádným a včasným dokončením celého Díla a jeho předáním Poskytovatelem a akceptací Objednatele dle této Smlouvy,

(ii) písemnou dohodou obou Smluvních stran, jejíž nedílnou součástí bude dohoda Smluvních stran o vypořádání vzájemných závazků,

(iii) výpovědí Objednatele s výpovědní dobou 30 dnů, výpovědní doba začíná běžet dnem následujícím po doporučení výpovědi Poskytovateli,

(iv) odstoupením Objednatele s okamžitou účinností bez jakýchkoliv sankcí, porušuje-li Poskytovatel podstatným způsobem ujednání této Smlouvy, a přes písemné

upozornění na porušení ujednání této Smlouvy podstatným způsobem takovéhoto jednání nebo konání nezanechá nebo nezjedná nápravu, a to v rámci dodatečné lhůty ke splnění povinnosti, která nesmí být kratší než 5 dní. Za podstatné porušení této Smlouvy se považuje:

1. prodlení Poskytovatele s předáním jakéhokoliv dílčího plnění především dle Harmonogramu (Přílohy č. 6 Smlouvy) po dobu delší než 5 kalendářních dnů oproti termínu plnění stanovenému ve Smlouvě, především v Harmonogramu plnění nebo termínu stanovenému na základě této Smlouvy, pokud Poskytovatel nezjedná nápravu ani v dodatečné přiměřené lhůtě, kterou mu k tomu Objednatel poskytne v písemné výzvě ke splnění povinnosti, přičemž tato lhůta nesmí být kratší než 10 kalendářních dnů od doručení takovéto výzvy,
2. dosáhnutí celkové výše smluvních pokut, na jejichž zaplacení by měl Objednatel dle této Smlouvy nárok, dosáhne 5 % z ceny Díla,
3. trvání závady kategorie A, B nebo C po dobu delší, než je jedna a půl (1,5) násobek sjednané maximální doby pro její odstranění,
4. porušení povinnosti mlčenlivosti nebo ochrany důvěrných informací dle této Smlouvy ze strany Poskytovatele,
5. ukáže-li se jakékoliv prohlášení Poskytovatele v souvislosti s plněním dle této Smlouvy nepravdivým, a
6. že nebude schválena částka ze státního rozpočtu, či z jiných zdrojů (např. prostředků z Evropské unie), která je potřebná k úhradě plnění dle této Smlouvy.

b) v části poskytování Služeb rozvoje:

(i) písemnou dohodou obou Smluvních stran, jejíž nedílnou součástí bude dohoda Smluvních stran o vypořádání vzájemných závazků,

(ii) výpovědí Objednatele s výpovědní dobou 30 dnů, výpovědní doba začíná běžet dnem následujícím po doporučení výpovědi Poskytovateli,

(iii) odstoupením Objednatele s okamžitou účinností bez jakýchkoliv sankcí, porušuje-li Poskytovatel podstatným způsobem ujednání této Smlouvy, a přes písemné upozornění na porušení ujednání této Smlouvy podstatným způsobem takovéhoto jednání nebo konání nezanechá nebo nezjedná nápravu, a to v rámci dodatečné lhůty ke splnění povinnosti, která nesmí být kratší než 5 dní. Za podstatné porušení této Smlouvy v části poskytování Služeb rozvoje se považuje:

1. porušení povinnosti mlčenlivosti nebo ochrany důvěrných informací dle této Smlouvy ze strany Poskytovatele,

2. porušení ustanovení o kybernetické bezpečnosti dle Přílohy č. 12 této Smlouvy ze strany Poskytovatele,

3. ukáže-li se jakékoliv prohlášení Poskytovatele v souvislosti s plněním dle této Smlouvy nepravdivým.

c) v části poskytování Služeb provozu a Služeb podpory:

(i) písemnou dohodou obou Smluvních stran, jejíž nedílnou součástí bude dohoda Smluvních stran o vypořádání vzájemných závazků,

(ii) výpovědí Objednatele s výpovědní dobou 30 dnů, výpovědní doba začíná běžet dnem následujícím po doporučení výpovědi Poskytovateli,

(iii) odstoupením Objednatele s okamžitou účinností bez jakýchkoliv sankcí, porušuje-li Poskytovatel podstatným způsobem ujednání této Smlouvy, a přes písemné upozornění na porušení ujednání této Smlouvy podstatným způsobem takovéhoto jednání nebo konání nezanechá nebo nezjedná nápravu, a to v rámci dodatečné lhůty ke splnění povinnosti, která nesmí být kratší než 5 dní. Za podstatné porušení této Smlouvy v části Služeb provozu a Služeb podpory se považuje:

1. porušení povinnosti mlčenlivosti nebo ochrany důvěrných informací dle této Smlouvy ze strany Poskytovatele,

2. porušení ustanovení o kybernetické bezpečnosti dle Přílohy č. 12 této Smlouvy ze strany Poskytovatele,

3. ukáže-li se jakékoliv prohlášení Poskytovatele v souvislosti s plněním dle této Smlouvy nepravdivým.

5.3. Poskytovatel je oprávněn odstoupit od této Smlouvy v případě prodlení Objednatele se zaplacením jakékoliv splatné částky dle této Smlouvy po dobu delší než 60 dnů, pokud Objednatel nezjedná nápravu ani v dodatečné přiměřené lhůtě, kterou mu k tomu Poskytovatel poskytne v písemné výzvě ke splnění povinnosti, přičemž tato lhůta nesmí být kratší než 15 kalendářních dnů od doručení takovéto výzvy.

5.4. Odstoupení od Smlouvy se pro účely této Smlouvy považuje za výpověď ve smyslu § 1998 a násl. OZ. Odstoupení od Smlouvy má vždy účinky do budoucna; to znamená, že v případě odstoupení od Smlouvy nemají Smluvní strany povinnost vracet si již poskytnuté plnění; pro vyloučení případných pochybností Smluvní strany výslovně uvádí, že v případě realizace Díla uvedené pravidlo znamená, že Objednatel nemá povinnost vracet poskytnuté a akceptované fáze

Díla a současně Poskytovatel nemá povinnost za tyto poskytnuté a akceptované fáze Díla vracet Objednatelem uhrazené příslušné části ceny Díla. Odstoupení od Smlouvy nemá vliv na odpovědnost Poskytovatele za vady a nedotýká se povinnosti případné vady již akceptované fáze Díla odstranit. Smluvní vztah skončí dnem doručení odstoupení druhé Smluvní straně.

5.5. Objednatel je mimo jiné oprávněn bez jakýchkoliv sankcí odstoupit od této Smlouvy ve všech nebo jen některých jejích částech, tj. realizace Díla, Služeb rozvoje, Služeb provozu a Služeb podpory, pokud:

a) bylo příslušným orgánem vydáno pravomocné rozhodnutí zakazující plnění této Smlouvy,

b) na majetek Poskytovatele je prohlášen úpadek, Poskytovatel sám podá dlužnický návrh na zahájení insolvenčního řízení nebo insolvenční návrh je zamítnut proto, že majetek nepostačuje k úhradě nákladů insolvenčního řízení,

c) Poskytovatel vstoupí do likvidace, nebo

d) proti Poskytovateli je zahájeno trestní řízení.

5.6. V případě odstoupení od Smlouvy má Objednatel právo rozhodnout, zda si rozpracované plnění realizace Díla nebo Služby rozvoje ponechá. Rozpracovaným plněním se myslí jakákoli část Díla i Dílo jako celek až do okamžiku jeho řádného převzetí Objednatelem dle Smlouvy a také jakákoliv část, která představuje Službu rozvoje až do okamžiku řádného převzetí jejího předmětu dle této Smlouvy. Rozhodne-li se Objednatel, že si rozpracované plnění ponechá, platí, že Objednateli náleží veškerá práva dle této Smlouvy, jako kdyby došlo k řádnému předání a akceptaci Díla, jeho části nebo Služeb rozvoje; zejména pak, nikoliv však výlučně, práva dle čl. 9 této Smlouvy a Poskytovatel je dále povinen předat Objednateli zdrojové kódy dle čl. 8 této Smlouvy k příslušné části Díla nebo Službě rozvoje. V případě, že si Objednatel rozpracované plnění ponechá, náleží Poskytovateli cena, na kterou má nárok podle Smlouvy, ponížená o to, co Poskytovatel ušetřil neprovedením Díla v plném rozsahu a neposkytnutím Služby rozvoje dle objednávky Objednatele. V případě, že Objednatel nebude mít zájem ponechat si rozpracované plnění, má Poskytovatel nárok na náhradu účelně vynaložených nákladů na provedení Díla a na poskytnutí Služby rozvoje do doby doručení odstoupení od Smlouvy, výše náhrady těchto nákladů nesmí být vyšší, než by byla 1/2 výše ceny Díla a ceny Služeb rozvoje ponížené dle předchozí věty.

6. Odpovědnost za škodu a smluvní pokuty

6.1. Poskytovatel prohlašuje, že při plnění předmětu Smlouvy nebudou porušena práva třetích osob, z nichž by pro Objednatele vyplynul jakýkoliv finanční nebo jiný závazek ve prospěch třetí strany. Poskytovatel nahradí Objednateli prokazatelnou škodu vzniklou Objednateli z titulu porušení zákonné či smluvní povinnosti Poskytovatele dle této Smlouvy za podmínek uvedených dále v této Smlouvě.

6.2. Smluvní strany jsou povinny v maximální míře předcházet vzniku škod a učinit veškerá dostatečná opatření k zamezení vzniku škod. Žádná ze stran neodpovídá za škody vzniklé z důvodů okolností vylučujících odpovědnost dle platné právní úpravy. Smluvní strany nesou odpovědnost za skutečnou a majetkovou škodu způsobenou druhé smluvní straně v důsledku porušení svých povinností.

6.3. Smluvní strany se dohodly, že:

a) v případě prodlení Poskytovatele s předáním Díla jako celku dle čl. 1 Přílohy č. 1 této Smlouvy, vzniká Objednateli nárok na smluvní pokutu ve výši 0,2 % Kč z ceny Díla za každý i jen započatý den prodlení,

b) v případě prodlení Poskytovatele s předáním jakéhokoliv části Díla dle této Smlouvy, zejm. dle čl. 1 Přílohy č. 1 této Smlouvy, vzniká Objednateli nárok na smluvní pokutu ve výši 0,05 % Kč z ceny části Díla za každý i jen započatý den prodlení,

c) v případě prodlení Poskytovatele s předáním jakékoliv Služby rozvoje dle této Smlouvy, zejm. ve smyslu čl. 1 Přílohy č. 2 této Smlouvy, vzniká Objednateli nárok na smluvní pokutu ve výši 0,01 % Kč z ceny Služby rozvoje za každý i jen započatý den prodlení,

d) v případě prodlení Poskytovatele s odstraněním vady kategorie I. dle čl. 7 této Smlouvy vzniká Objednateli nárok na smluvní pokutu ve výši 0,05 % Kč z ceny Díla za každý i jen započatý den prodlení,

e) v případě prodlení Poskytovatele s odstraněním vady kategorie II. a III. dle čl. 7 této Smlouvy vzniká Objednateli nárok na smluvní pokutu ve výši 0,01 % Kč z ceny Díla za každý i jen započatý den prodlení.

6.4. Poskytovatel je povinen zaplatit Objednateli smluvní pokutu ve výši 100.000 Kč za každé jednotlivé porušení jakékoliv jeho povinnosti stanovené mu v čl. 3 této Smlouvy.

6.5. Poskytovatel je povinen zaplatit Objednateli smluvní pokutu ve výši 500.000 Kč za každé jednotlivé porušení jakékoliv jeho povinnosti stanovené mu v čl. 8 a v čl. 10 této Smlouvy.

6.6. V případě nedodržení minimální garantované funkčnosti AIS JePEK za kalendářní měsíc dle Technické dokumentace je Poskytovatel povinen uhradit Objednateli smluvní pokutu ve výši 10.000 Kč za každých 0,1% snížení dostupnosti AIS v daném měsíci.

6.7. Smluvní pokuta dle čl. 6.6. této Smlouvy může být aplikována, a tedy nárok Objednatele na její uplatnění vzniká až po uplynutí prvních třech měsíců počítaných od úspěšného dokončení Díla jako celku potvrzeného podpisem akceptačního protokolu Díla jako celku.

6.8. Úhradou smluvní pokuty podle této Smlouvy není dotčen nárok na náhradu škody zvlášť a v plné výši, ani povinnost Poskytovatele odstranit závadný stav. V případě škody či újmy vzniklé v důsledku

činnosti třetí strany je Objednatel oprávněn, avšak nikoliv povinen, uplatňovat své nároky přímo vůči těmto třetím stranám.

7. Záruka

7.1. Poskytovatel poskytuje záruku, že každá část Díla má ke dni její akceptace funkční vlastnosti stanovené touto Smlouvou a je způsobilá k použití pro účely stanovené v této Smlouvě nebo v souladu s touto Smlouvou.

7.2. Poskytovatel poskytuje záruku za jakost každé jednotlivé části Díla od okamžiku její akceptace po dobu 24 měsíců od akceptace Díla jako celku.

7.3. Není-li v této Smlouvě nebo v souladu s touto Smlouvou stanoveno jinak:

a) Poskytovatel zahájí řešení odstranění vady kategorie I., tj. vady, která zcela nebo podstatným způsobem znemožňuje užívání AIS, okamžitě po jejím nahlášení, s tím, že vadu do **8 hodin** od jejího nahlášení odstraní nebo poskytne akceptovatelné náhradní řešení,

b) Poskytovatel zahájí řešení odstranění vady kategorie II., tj. vady, která nebrání užívání AIS, ale omezuje jeho provoz, maximálně **do 4 hodin** od jejího nahlášení, s tím, že vadu do **5 dnů** od jejího nahlášení odstraní nebo poskytne akceptovatelné náhradní řešení,

c) Poskytovatel zahájí řešení odstranění vady kategorie III., tj. vady, která není vadou kategorie I. ani II., maximálně **do 2 dnů** od jejího nahlášení, s tím, že termín odstranění vady bude předmětem dohody smluvních stran, nepřekročí však dobu **10 dnů** od jejího nahlášení,

d) náhradní řešení vady kategorie I. se považuje za nahlášenou vadu kategorie II. a náhradní řešení vady kategorie II. se považuje za nahlášenou vadu kategorie III., přičemž náhradní řešení vady je výjimečným postupem a Poskytovatel je povinen je Objednateli řádně písemně zdůvodnit;

e) pokud Objednatel dodatečně dojde k závěru, že ve stanovené lhůtě poskytnuté náhradní řešení vady není akceptovatelné, oznámí tuto skutečnost Poskytovateli a vada se od tohoto okamžiku opět klasifikuje jako vada původní (vyšší) kategorie.

7.4. Pro účely tohoto článku definuje kategorie vad Příloha č. 10 k této Smlouvě.

7.5. Pro vyloučení pochybností se uvádí, že (i) lhůty uvedené v tomto článku Smlouvy, zejm. lhůty v čl. 7.3. této Smlouvy, jsou lhůtami stanovenými výlučně pro řešení odstranění vad v rámci záruky poskytnuté Poskytovatelem Objednateli v souladu s tímto článkem a že (ii) pro zahájení řešení odstranění vad a pro odstranění vad dle jednotlivých kategorií jsou počítány od momentu nahlášení Poskytovateli Objednatelem. Lhůty pro odstranění vad neběží po dobu, po kterou není odstranění vady Díla možné z důvodů na straně Objednatele, pokud o takové skutečnosti Poskytovatel

bezodkladně informoval Objednatele. Služby podpory Poskytovatele budou poskytovány dle pravidel dále stanovených touto Smlouvou.

7.6. Objednatel je oprávněn vady Díla nahlásit Poskytovateli kdykoli v průběhu záruční doby bez ohledu na to, kdy je zjistil, aniž by tím bylo jeho právo ze záruky či odpovědnosti za vady jakkoli dotčeno.

7.7. Doba od zjištění vady do jejího odstranění se do trvání záruční doby nezapočítává.

7.8. Poskytovatel prohlašuje, že veškeré jeho plnění dodané podle této Smlouvy bude prosté právních vad a zavazuje se odškodnit v plné výši Objednatele v případě, že třetí osoba úspěšně uplatní autorskoprávní nebo jiný nárok plynoucí z právní vady poskytnutého plnění. V případě, že by nárok třetí osoby vzniklý v souvislosti s plněním Poskytovatele podle této Smlouvy, bez ohledu na jeho oprávněnost, vedl k dočasnému či trvalému soudnímu zákazu či omezení užívání AIS či jeho části, zavazuje se Poskytovatele zajistit náhradní řešení a minimalizovat dopady takovéto situace, a to bez dopadu na cenu plnění sjednanou podle této Smlouvy, přičemž současně nebudou dotčeny ani nároky Objednatele na náhradu škody.

7.9. Poskytovatel prohlašuje, že je oprávněn vykonávat svým jménem a na svůj účet majetková práva autorů k autorským dílům, která budou součástí plnění podle této Smlouvy, resp. že má souhlas všech relevantních třetích osob k poskytnutí licence k autorským dílům podle čl. 9 této Smlouvy; toto prohlášení zahrnuje i taková práva, která by vytvořením autorského díla teprve vznikla.

7.10. Smluvní strany se dohodly, že Objednatel je oprávněn kdykoliv do uplynutí záruční doby k Dílu požádat Poskytovatele o posouzení Objednatelem zamýšlené změny Díla. Poskytovatel se v takovém případě zavazuje bez zbytečného odkladu posoudit zamýšlenou změnu Díla z hlediska zachování řádné funkčnosti ostatních součástí Díla a Díla jako celku a Objednatel se zavazuje uhradit Poskytovateli prokázané účelně vynaložené náklady takovéhoto posouzení. Provede-li Objednatel změnu Díla nad rámec posuzovaný Poskytovatelem, v rozporu s instrukcemi Poskytovatele a/nebo bez předchozího posouzení změny Poskytovatelem, záruka za vady Díla provedením změny Díla zaniká. Objednatel je povinen informovat Poskytovatele o každém zásahu do zdrojového kódu

8. Zdrojový kód

8.1. Nestanoví-li tato Smlouva jinak, je Poskytovatel povinen nejpozději v okamžiku akceptace dílčího plnění tvořícího AIS JePEK předat Objednateli zdrojový kód každého jednotlivého takového plnění, které je počítačovým programem, a které je Objednateli poskytováno jako součást provádění Díla. Zdrojový kód musí být spustitelný v prostředí Objednatele a zaručující možnost ověření, že je kompletní a ve správné verzi, tzn. umožňující kompilaci, instalaci, spuštění a ověření funkcionality, a to včetně podrobné dokumentace zdrojového kódu takovéto části AIS, na základě, které bude běžný kvalifikovaný uživatel Objednatele schopen pochopit veškeré funkce a vnitřní vazby software

a zasahovat do něj. Každý zdrojový kód bude Objednateli Poskytovatelem předán na samostatném nepřepisovatelném technickém nosiči dat s viditelně označeným názvem „Zdrojový kód“ a označením části AIS a jeho verze a dne předání zdrojového kódu. O předání technického nosiče dat dle předchozí věty bude oběma Smluvními stranami sepsán a podepsán písemný předávací protokol. Aktuální zdrojový kód bude Objednateli předán i při předání dokončeného Díla jako celku. Cena za technické nosiče dat je zahrnuta v celkové ceně Díla uvedené dle Přílohy č. 5 této Smlouvy.

8.2. Povinnost Poskytovatele uvedená v čl. 8.1. se přiměřeně použije i pro jakékoliv opravy, změny, doplnění, upgrade nebo update zdrojového kódu jednotlivého dílčího plnění tvořícího AIS, k nimž dojde při plnění této Smlouvy, zejm. při poskytování Služeb rozvoje nebo v rámci záručních oprav („**Změna zdrojového kódu**“). Dokumentace Změny zdrojového kódu musí obsahovat podrobný popis a komentář každého zásahu do zdrojového kódu.

8.3. Poskytovatel je povinen předat Objednateli zdrojový kód s Dokumentací nebo Dokumentaci Změny zdrojového kódu nejpozději v den předání a převzetí příslušného plnění podle této Smlouvy. V případě předčasného ukončení této Smlouvy je Poskytovatel povinen předat Objednateli aktuální zdrojové kódy s příslušnou Dokumentací a koncepční přípravné materiály všech součástí AIS tak, aby byl Objednatel držitelem zdrojového kódu minimálně v dané chvíli aktuální verze AIS.

9. Právo užití

9.1. Objednatel uznává, že autorská práva a práva průmyslového vlastnictví k plnění dodanému a vyvinutému Poskytovatelem na základě této Smlouvy v jakékoli formě, zahrnující zejména počítačové programy nebo moduly, náleží Poskytovateli nebo k nim má Poskytovatel právo užívání na základě licence poskytnuté třetí stranou, která je nositelem autorského práva nebo práva průmyslového vlastnictví, které je Poskytovatel současně oprávněn legálně poskytnout Objednateli ve formě sublicence nebo jiného práva.

9.2. Poskytovatel touto Smlouvou poskytuje Objednateli výhradní licenci k Dílu, jako konečnému výsledku činnosti Poskytovatele dle této Smlouvy, a k výstupům Služeb rozvoje představující konečný výstup naplňující znaky autorského díla ve smyslu autorského zákona, a to okamžikem úhrady ceny za Dílo nebo příslušnou část Služeb rozvoje. K ostatním částem Díla či Služeb rozvoje, které nepředstavují konečný výsledek činnosti Poskytovatele dle této Smlouvy poskytuje Poskytovatel Objednateli nevýhradní licenci.

9.3. Udělením licence dle čl. 9.2. této Smlouvy je Objednatel oprávněn užít autorské dílo v neomezeném množstevním a územním rozsahu po dobu trvání majetkových práv Poskytovatele k takovému autorskému dílu. Součástí licence je neomezené oprávnění Objednatele provádět modifikace, úpravy a změny Díla nebo výsledku Služeb rozvoje, dle svého uvážení do něho zasahovat, zapracovávat do dalších autorských děl či do databází, a to i prostřednictvím třetích osob; v takovém případě však Objednatel pozbude práva na odstraňování vad k těm částem Díla, u kterých takovými

modifikacemi, úpravami a změnami dojde ke změně Díla ve větším rozsahu a nebude možné uplatnit jakékoliv sankce dle této Smlouvy u těch částí Díla, u kterých takovými modifikacemi, úpravami a změnami dojde k změně Díla ve větším rozsahu. Pro vyloučení pochybností Smluvní strany prohlašují, že za takové modifikace, úpravy či změny se nepovažují drobné zásahy do Díla, které nemají významný vliv na Dílo či jeho jednotlivé části, nebo jakékoliv modifikace, úpravy či změny, které jsou schváleny Poskytovatelem. Objednatel je oprávněn udělit třetí osobě podlicenci k užití takového autorského díla.

9.4. V případě, že součástí Díla bude software třetích stran, u něhož poskytnutí oprávnění dle čl. 9.3. této Smlouvy není možné („**Standardní software**"), může být součástí Díla pouze při splnění některé z následujících podmínek (pro vyloučení veškerých pochybností Smluvní strany uvádí, že v případě, kdy je vývoj počítačového programu hrazen Objednatelem na základě této Smlouvy, může Objednatel vždy požadovat udělení oprávnění dle čl. 9.3. této Smlouvy):

a) software musí být v době uzavření Smlouvy prokazatelně nasazen v produkčním prostředí u nejméně deseti vzájemně nezávislých a nepropojených subjektů. Zároveň musí být běžně dostupný na trhu, tedy nabízený na území České republiky minimálně třemi vzájemně nezávislými a nepropojenými subjekty, a to za splnění jedné z následujících podmínek:

(i) tyto subjekty mají oprávnění software implementovat, upravovat a poskytovat jeho údržbu, nebo

(ii) udělení licence v rozsahu podle čl. 9.3. této Smlouvy není účelné a nebrání dalšímu rozvoji AIS ze strany Objednatele (zejména se jedná o vývojový software, databázový software apod.).

Poskytovatel je povinen tuto skutečnost doložit písemným prohlášením a na žádost Objednatele ji dále prokázat;

b) software je veřejně dostupný zdarma a zahrnuje detailně okomentované zdrojové kódy, kompletní uživatelskou, provozní a administrátorskou dokumentaci, stejně jako právo na jeho úpravy. Poskytovatel je povinen tuto skutečnost doložit písemným prohlášením a na žádost Objednatele ji dále prokázat; a

c) software, k němuž Poskytovatel poskytne nebo zprostředkuje poskytnutí kompletních okomentovaných zdrojových kódů nejpozději do 30 dnů od dokončení celého Díla, a zároveň zajistí bezpodmínečné právo Objednatele provádět jakékoli modifikace, úpravy a změny tohoto softwaru dle vlastního uvážení.

9.5. K naplnění účelu v čl. 9.3. této Smlouvy Poskytovatel poskytne Objednateli přiměřené přístupy a veškerou technickou dokumentaci k autorským dílům, které jsou výsledkem činnosti Poskytovatele dle této Smlouvy (zdrojové kódy).

9.6. Odměna za poskytnutí licence k autorským dílům je zahrnuta v ceně Díla a Služeb rozvoje.

10. Mlčenlivost a ochrana osobních údajů

10.1. Poskytovatel není oprávněn bez předchozího písemného souhlasu Objednatele zveřejnit či sdělit třetí osobě skutečnosti týkající se této Smlouvy nebo jakékoli informace o skutečnostech, o kterých se Poskytovatel dozvěděl při plnění předmětu této Smlouvy nebo v souvislosti s ním. Tato povinnost mlčenlivosti trvá i po ukončení trvání této Smlouvy.

10.2. Osobní údaje uživatelů AIS JePEK nebudou v žádné fázi trvání této smlouvy zpřístupněny Poskytovateli a Poskytovatel je tedy nebude, jakkoliv zpracovávat ve smyslu Nařízení Evropského parlamentu a Rady (EU) 2016/679, ve znění pozdějších předpisů („**GDPR**"). Výjimkou mohou být pouze případy, kdy je takové zpřístupnění nezbytné pro plnění této Smlouvy a je výslovně schváleno Objednatelem, a to pouze za zákonných podmínek a důvodů stanovených příslušnými právními předpisy o ochraně osobních údajů, zejm. čl. 6 odst. 1 písm. b), c), e) nebo f) GDPR. Mělo-li by ke zpracování osobních údajů dojít, je Poskytovatel takovou skutečnost bezodkladně oznámit Objednateli, který rozhodne o dalším postupu.

11. Okolnosti vylučující odpovědnost

11.1. Objednatel není v prodlení v případě, že po vzniku závazku nastanou okolnosti vylučující odpovědnost, jak jsou definovány v § 2913 odst. 2 OZ.

11.2. Za okolnosti vylučující odpovědnost se považují takové překážky, které nastaly po vzniku závazku nezávisle na vůli stran, mají mimořádnou povahu, jsou neodvratitelné, nepředvídatelné, nepřekonatelné a brání objektivně splnění povinností Objednatele dle této Smlouvy (např. válečný stav, občanské nepokoje, požár, záplavy, epidemie, karanténní opatření).

11.3. Jestliže překážky odpovídající okolnostem vylučujících odpovědnost nastanou, je povinná strana povinna bez zbytečného odkladu informovat druhou stranu o povaze, počátku a konci takovéto překážky, která brání splnění povinností dle této Smlouvy. Termín plnění se v tomto případě prodlužuje o dobu trvání překážky. Po dobu trvání okolností vylučujících odpovědnost není Poskytovatel ani Objednatel v prodlení s plněním dle této Smlouvy.

11.4. Odpovědnost povinné strany však není vyloučena a termín plnění se neprodlužuje, pokud okolnosti vylučující odpovědnost nastaly až v době, kdy povinná strana již byla v prodlení s plněním závazku dle této Smlouvy nebo pokud povinná strana nesplnila svoji povinnost neprodleně informovat druhou stranu o povaze a počátku takové okolnosti.

12. Ustanovení společná a závěrečná

12.1. Tato Smlouva je závazná i pro případné právní nástupce obou Smluvních stran.

12.2. Veškerá práva a povinnosti Smluvních stran stanovená v této Smlouvě se uplatní na všechny právní vztahy mezi Poskytovatelem a Objednatelem v souvislosti s předmětem této Smlouvy, neodporují-li účelu této Smlouvy a není-li v přílohách této Smlouvy nebo v jiném smluvním či jiném ujednání mezi Smluvními stranami stanoveno jinak. Ustanovení obsažená v Přílohách č. 1, č. 2 a č. 3 této Smlouvy mají aplikační přednost před obecnými ustanoveními této Smlouvy.

12.3. Práva a povinnosti vyplývající z této Smlouvy představují pro další právní jednání Smluvních stran týkající se provozu a rozvoje Díla a poskytování Služeb provozu a Služeb podpory obchodní podmínky ve smyslu § 1751 odst. 1 OZ a budou proto pro taková právní jednání aplikována podpůrně. Smluvní strany se dohodly, že uvedené pravidlo neplatí pro přílohy této Smlouvy jako specifická a technická ujednání, která se vztahují výhradně k Dílu poskytovanému dle této Smlouvy.

12.4. V případě prodlení kterékoliv Smluvní strany se zaplacením peněžité částky dle této Smlouvy vzniká oprávněné Smluvní straně nárok na úrok z prodlení ve výši stanovené nařízením vlády č. 351/2013 Sb., ve znění pozdějších předpisů. Tím není dotčen ani omezen nárok na náhradu vzniklé škody.

12.5. Objednatel je oprávněn kdykoliv v průběhu plnění této Smlouvy i po dobu trvání záruky dle čl. 7 této Smlouvy provést nebo nechat třetí osobou provést audit dodaného Díla nebo poskytnuté Služby. Zejména jen Objednatel oprávněn provést nebo nechat provést bezpečností audit nebo kontrolu licenční čistoty. Poskytovatel je povinen při takovém auditu poskytnout veškerou potřebnou součinnost.

12.6. Tuto Smlouvu lze měnit nebo doplňovat pouze písemnými vzestupně očíslovanými dodatky podepsanými oběma Smluvními stranami.

12.7. V případě rozporu jakéhokoliv ustanovení Technické dokumentace, která je Přílohou č. 4 této Smlouvy, se Smlouvou nebo jakoukoliv její jinou přílohou, má aplikační přednost před ustanoveními Technické dokumentace ustanovení obsažené v této Smlouvě nebo v jakékoliv její další příloze.

12.8. Pokud se kterékoliv ustanovení této Smlouvy ukáže jako neplatné, neúčinné nebo nevykonatelné, nebude tím dotčena platnost, účinnost ani vykonatelnost ostatních ustanovení této Smlouvy; popř. bude kterékoliv ustanovení této Smlouvy v rozporu se Zadávacím řízením nebo ZZVZ, zavazují se Smluvní strany nahradit neplatné, neúčinné nebo nevykonatelné ustanovení novým ustanovením, které nejlépe odpovídá původnímu účelu a záměru Smluvních stran. Do doby nahrazení takového ustanovení se bude Smlouva vykládat a plnit v souladu s jejím celkovým smyslem a účelem tak, aby byla zachována rovnováha práv a povinností Smluvních stran.

12.9. Pro účely této Smlouvy se za písemnou formu komunikace považuje i komunikace prostřednictvím e-mailů uvedených v Příloze č. 9 této Smlouvy.

12.10. Právní vztahy výslovně neupravené touto Smlouvou, nebo upravené pouze částečně, se řídí právním řádem České republiky, zejména pak příslušnými ustanoveními Občanského zákoníku a zákona č. 121/2000 Sb. (Autorský zákon) v platném znění a předpisy souvisejícími.

12.11. Veškeré spory z této Smlouvy se Smluvní strany zavazují pokusit nejdříve řešit smírnou cestou. Nelze-li spor mezi Smluvními stranami vyřešit smírnou cestou, budou rozhodovat obecné soudy místně příslušné dle sídla Objednatele, nestanoví-li zákon něco jiného.

12.12. Smluvní podmínky dohodnuté v této Smlouvě se rámcově použijí pro budoucí smluvní vztahy mezi Objednatelem a Poskytovatelem obdobného obsahu, pokud se ve výjimečných případech Smluvní strany výslovně písemně nedohodnou jinak.

12.13. Smluvní strany přebírají riziko změny okolností ve smyslu § 1765 odst. 2 OZ.

12.14. Tato Smlouva se uzavírá elektronicky, a to pouze v jednom elektronickém vyhotovení, které je podepsáno platnými kvalifikovanými elektronickými podpisy Smluvních stran.

12.15. Tato Smlouva nabývá platnosti dnem jejího podpisu všemi Smluvními stranami a účinnosti dnem jejího zveřejnění v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv). Uveřejnění této Smlouvy v registru smluv zajistí Objednatel.

Přílohy, které tvoří nedílnou součást této Smlouvy:

Příloha č. 1 – Provedení Díla

Příloha č. 2 – Služby rozvoje Díla

Příloha č. 3 – Služby provozu AIS a Služby podpory AIS

Příloha č. 4 – Technická dokumentace (v rámci zadávací dokumentace označeno jako Příloha č. 3)

Příloha č. 5 – Specifikace ceny plnění

Příloha č. 6 – Harmonogram

Příloha č. 7 – Realizační tým Poskytovatele

Příloha č. 8 – Seznam subPoskytovatelů

Příloha č. 9 – Oprávněné osoby a kontaktní údaje

Příloha č. 10 – Typy vad Díla

Příloha č. 11 – Pojistný certifikát

Příloha č. 12 - Smluvní ujednání v rámci zákona o kybernetické bezpečnosti

PODPISOVÁ STRANA

V Praze dne *dle elektronického podpisu*

Česká republika – Ministerstvo průmyslu a obchodu

[redacted]

Ing. Pavel Vinkler, Ph.D., LL.M.

V Praze dne *dle elektronického podpisu*

ASD Software, s.r.o.

Ing. Petr Polách

Příloha č. 1 – Provedení Díla

Smluvní ujednání o provedení Díla a o souvisejících právech a povinnostech Smluvních stran

1. Realizace Díla

1.1. Realizace Díla je rozdělena do jednotlivých fází specifikovaných v Harmonogramu, který je uveden v Příloze č. 6; fáze Díla představují dílčí plnění Poskytovatele. Akceptace jednotlivých fází Díla bude probíhat podle Harmonogramu, tj. Přílohy č. 6, na základě písemné výzvy Poskytovatele zaslané Objednateli alespoň 5 pracovních dní před předáním příslušné fáze či předvedení její funkčnosti.

1.2. Objednatel je povinen akceptovat jednotlivou fázi v případě, že neobsahuje žádnou vadu A, maximálně 2 vady B a současně maximálně 5 vad C; ve smyslu vymezení v Příloze č. 6. Má se za to, že nedodání kompletní příslušné Dokumentace náležící ke každé jednotlivé fázi Díla, je vadou A. Objednatel je oprávněn jednotlivou fázi převzít i v případě, kdy počet vad překračuje maximální počet vad podle tohoto odstavce. Akceptace jednotlivé fáze Objednatelem nemá vliv na povinnost Poskytovatele odstranit veškeré vady takové fáze, a to i v případě, že nejsou Objednatelem při převzetí příslušné fáze či dílčího plnění označeny (např. dozví-li se o takové vadě dodatečně), a to nejméně po dobu 24 měsíců od akceptace dané fáze Díla. Pokud jednotlivé fáze nesplňují podmínky pro převzetí Objednatelem, je Poskytovatel povinen odstranit vady A nejpozději do 1 pracovního dne, vady B do 5 pracovních dní a vady C do 10 pracovních dní, nedohodnou-li se Smluvní strany na jiných lhůtách k odstranění, od jejich vytčení Objednatelem. V takovém případě se opakuje akceptační proces podle tohoto odstavce Smlouvy. Akceptace nebo nepřevzetí jednotlivých fází probíhá na základě písemného akceptačního protokolu, ve kterém jsou případně vyznačeny výhrady Objednatele k jednotlivým zjištěným vadám.

1.3. Poskytovatel je povinen vytvořit AIS v takovém programovacím jazyce, který je běžně používaným v prostředí evropského trhu informačních technologií („**Programovací jazyk**“), přičemž takový Programovací jazyk musí být široce podporován odbornou komunitou, stabilní a udržovaný, přičemž musí umožňovat budoucí rozšíření a podporu třetími stranami a realizace AIS musí probíhat v souladu s aktuálními standardy a doporučeními v oblasti informačních technologií, zejména s ohledem na bezpečnost, výkon a kompatibilitu s běžně užívanými operačními systémy a systémy veřejné správy, nedohodnou-li se Smluvní strany písemně jinak.

1.4. Pro vyloučení pochybností se Smluvní strany dohodly, že se Poskytovatel zavazuje předávat Objednateli Dílo, resp. jednotlivé jeho fáze, v takovém stavu a rozsahu, aby bylo v případě ukončení této Smlouvy možno bez dalšího pokračovat v realizaci plnění podle této Smlouvy jiným Poskytovatelem. Pokud nový Poskytovatel zvolený Objednatelem zjistí, že Dílo, resp. některá z jeho fází, trpí vadami, případně nedodělky, a to v porovnání se specifikací Díla a požadavky na něj zejm. dle Přílohy č. 4 této Smlouvy, které nebyly Poskytovatelem při předání příslušné fáze Díla sděleny, je Poskytovatel povinen takové vady či nedodělky zdarma odstranit v případě, že jej k tomu

Objednatel vyzve do 24 měsíců od předání příslušné fáze Díla. Poskytovatel je povinen při předání Díla a jeho částí poskytnout Objednateli veškerou možnou potřebnou součinnost.

1.5. Dílo jako celek se považuje za dokončené:

a) akceptací a zároveň protokolárním předáním a převzetím poslední fáze bez vad a nedodělků; a

b) akceptací a protokolárním předáním a převzetím příslušné Dokumentace,

Díla jako celku oběma Smluvními stranami.

2. Cena a platební podmínky

2.1. Celková cena Díla („**Celková cena Díla**“), je stanovena dle ceníku uvedeného v Příloze č. 5. Ceny jsou uvedeny bez sazby DPH, která bude k cenám připočtena v zákonné výši. Ceny sjednané v Příloze č. 5, odpovídají rozsahu Díla definovanému v této Smlouvě a jsou sjednány jako nejvyšší možné, obsahují veškeré související náklady a nemohou být přesaženy. **V případě rozporu celkové ceny Díla uvedené sjednané v Příloze č. 5 s cenou uvedenou v Nabídce má přednost cena uvedená v Nabídce, ledaže Objednavatel rozhodne jinak.**

2.2. Cena Díla zahrnuje veškeré náklady Poskytovatele včetně odměny za udělení práv užití autorských děl vytvořených Poskytovatelem při plnění této Smlouvy a za poskytnutí majetkových práv k AIS JePEK. Smluvní strany výslovně sjednávají, že celková cena Díla zahrnuje odměnu za licence k Standardním softwarům dle čl. 9.4. této Smlouvy, jehož má být v rámci realizace Díla užito.

2.3. Cena Díla bude zaplacena následovně:

a) část ceny Díla ve výši odpovídající 10 % ceny Díla bez DPH bude uhrazena do 5 pracovních dnů po předání a akceptaci části Díla Objednatelem odpovídající klíčovému milníku A dle Přílohy č. 6;

b) část ceny Díla ve výši odpovídající 30 % ceny Díla bez DPH bude uhrazena do 5 pracovních dnů po předání a akceptaci části Díla Objednatelem odpovídající klíčovému milníku B dle Přílohy č. 6;

c) část ceny Díla ve výši odpovídající 30 % ceny Díla bez DPH bude uhrazena do 5 pracovních dnů po předání a akceptaci části Díla Objednatelem odpovídající klíčovému milníku C dle Přílohy č. 6;

d) část ceny Díla ve výši odpovídající 30 % ceny Díla bez DPH bude uhrazena do 5 pracovních dnů po předání a akceptaci části Díla Objednatelem odpovídající klíčovému milníku D dle Přílohy č. 6.

2.4. Každá konkrétní část ceny Díla bude Poskytovateli vyplacena pouze za předpokladu, že daná část Díla byla předána a akceptována v souladu s akceptačními testy a akceptačními kritérii dle Přílohy č. 6.

2.5. Smluvní strany tímto ve vztahu k určení a zvýšení ceny Díla výslovně vylučují aplikaci ustanovení § 2622 OZ.

2.6. Platby dle této Přílohy budou hrazeny na základě daňových dokladů – faktur vystavovaných Poskytovatelem v částkách a termínech určených v této Smlouvě bezhotovostním převodem na účet Poskytovatele uvedený v těchto daňových dokladech – fakturách. Splatnost jednotlivých faktur bude vždy 60 dní ode dne doručení této faktury Objednateli. Poskytovatel odešle Objednateli fakturu elektronicky na e-mailovou adresu: [redacted] alternativně doporučenou poštou na adresu uvedenou v záhlaví této Smlouvy, a to ten stejný den, ve kterém byla faktura vystavena. Má se za to, že faktura byla doručena Objednateli. Pro vyloučení pochybností se uvádí, že prodlení Poskytovatele s odesláním faktury neznamená vzdání se práva na úhradu příslušné ceny.

2.7. Faktura je považována za uhrazenou dnem, kdy bude odpovídající částka připsána na účet Poskytovatele. Nebude-li faktura obsahovat všechny náležitosti a přílohy, které jsou vyžadovány touto Smlouvou (zejm. rozpis práce, kopie akceptačního protokolu), je Objednatel oprávněn fakturu reklamovat u Poskytovatele, a to do 10 dnů od dne jejího doručení Objednateli. Nová lhůta splatnosti začne plynout dnem doručení opravené faktury Objednateli.

2.8. Změna ceny Díla dle této Smlouvy je přípustná pouze v případě změny zákonem stanovené sazby daně z přidané hodnoty. Dojde-li v průběhu plnění dle této Smlouvy ke změně výše příslušné sazby DPH, bude cena s DPH upravena v rozsahu změn příslušné sazby DPH stanovené právními předpisy platnými ke dni uskutečnění zdanitelného plnění, a to formou písemného dodatku k této Smlouvě, podepsaným k tomu oprávněnými zástupci obou Smluvních stran.

3. Doba a místo plnění

3.1. Poskytovatel se zavazuje provést pro Objednatele Dílo dle Harmonogramu, který je uveden v Příloze č. 6 této Smlouvy.

3.2. Řádné plnění dodané Poskytovatelem do 5 pracovních dní po termínu stanoveném v Příloze č. 6 této Smlouvy je považováno za plnění v souladu s touto Smlouvou a nebude považováno za prodlení na straně Poskytovatele. Pro vyloučení všech pochybností Smluvní strany sjednávají, že tolerance pro jednotlivá plnění po lhůtě se nesčítají, tedy maximální doba pro plnění po lhůtě v poslední fázi činí stále 5 pracovních dní. Řádné převzetí a předání konkrétních fází Díla dle Harmonogramu stanoveného v Příloze č. 6 této Smlouvy a v souladu s touto Smlouvou bude Objednatelem

potvrzeno podepsáním akceptačního protokolu za podmínek uvedených výše v čl. 1 a 2 Přílohy č. 1 této Smlouvy.

3.3. Místem plnění je sídlo Objednatele, pokud to však povaha plnění této Smlouvy, zejm. Přílohy č. 1 této Smlouvy umožňuje, je Poskytovatel oprávněn provádět části Díla také vzdáleným přístupem.

Příloha č. 2 – Služby rozvoje Díla

Smluvní ujednání o Službách rozvoje o souvisejících právech a povinnostech Smluvních stran

1. Předmět Služeb rozvoje

1.1. Předmětem plnění dle této smlouvy je v návaznosti na ustanovení čl. 2.3. Smlouvy také závazek Poskytovatele poskytovat Objednateli ad-hoc rozvoj Díla, resp. AIS JePEK, týkající se veškerých požadavků na rozvoj/úpravu AIS, tedy požadavků, které nejsou předmětem plnění dle bodů 2.2. a 2.4. Smlouvy, a to na základě samostatných objednávek Objednatele. Poskytovatel se zavazuje průběžně analyzovat potřeby Objednatele a uživatelů AIS v souvislosti s provozem AIS a navrhovat vylepšení. Poskytovatel se zavazuje na základě požadavku Objednatele vytvořit roadmapu s navrhovanými zlepšeními, a to v čase po vzájemné dohodě. Službami rozvoje se pro účely této Přílohy č. 2 Smlouvy a této Smlouvy rozumí průběžná aktualizace AIS JePEK na základě změn legislativního prostředí, technologických požadavků nebo změny na základě požadavků Objednatele. Dále se Službami rozvoje rozumí:

a) integrace s dalšími informačními systémy;

b) další rozvoj a zlepšení uživatelského rozhraní;

c) rozšíření funkcionality;

d) aplikace umělé inteligence (AI);

e) školení a podpora uživatelů AIS v souvislosti s rozvojem;

f) konzultační služby ve vztahu k rozvoji AIS a kybernetické bezpečnosti AIS; pravidelné konzultace s klíčovými uživateli za účelem pochopení a jejich potřeb a požadavků, na jejichž základě poskytne Poskytovatel návrhy na další úpravy a rozvoj AIS;

g) zajištění kontinuálního vývoje AIS, které Poskytovatel zajistí (i) průběžnou údržbou a rozvojem AIS v souladu s novými legislativními a technologickými požadavky, a (ii) sledováním změn relevantních pro AIS a navrhnutím jejich implementace Objednateli tak, aby bylo zajištěno dlouhodobé fungování a efektivita řešení; a

h) zajištění kontinuálního souladu s požadavky na kybernetickou bezpečnost AIS z důvodu legislativních změn v oblasti právních předpisů týkajících se kybernetické bezpečnosti.

1.2. Poskytovatel se zavazuje požadavek na úpravu AIS bez zbytečného odkladu po obdržení objednávky od Objednatele akceptovat. Poskytovatel musí u každého rozvojového požadavku ohodnotit jeho pracnost v člověkodnech a dobu realizace takového rozvojového požadavku, které předloží Objednateli ke schválení. Poskytovatel se zavazuje Objednateli dle bodu 2.3. této Smlouvy a této Přílohy č. 2 Smlouvy poskytnout Služby rozvoje v takovém rozsahu, aby byla zajištěna správná funkčnost AIS pro potřeby Objednatele, jednotlivých kontrolních orgánů a uživatelů AIS. Ad-hoc

Služby rozvoje AIS se vztahují k Dílu dodanému dle této Smlouvy Poskytovatelem Objednateli. Plnění dle tohoto bodu bude realizováno na základě výzvy Objednatele.

1.3. Celkový maximální možný rozsah Služeb rozvoje a maximální možný rozsah Služeb rozvoje v jednotlivých obdobích poskytování Služeb rozvoje dle této Smlouvy v člověkodnech, a to i s ohledem na jednotlivé oblasti Služeb rozvoje, je stanoven v Příloze č. 5 této Smlouvy. Poskytování Služeb rozvoje ve vyšším rozsahu Služeb rozvoje než stanoveném v Příloze č. 5 této Smlouvy je možný pouze po předchozím písemném souhlasu Objednatele. Odsouhlasení (potvrzení) objednávky Služeb rozvoje Objednatelem se považuje za souhlas podle věty předchozí. Poskytovatel se zavazuje vyhradit dostatečnou kapacitu osob k poskytování Služeb rozvoje dle tohoto článku. Souhlas Objednatele s poskytováním Služeb rozvoje nad rozsah stanovený v Příloze č. 5 Smlouvy se nepovažuje za souhlas s vyšší cenou Služeb rozvoje, ledaže by Objednatel s takovou výslovně souhlasil.

1.4. Pro kalkulaci Služeb rozvoje je uváděn rozsah služeb ve člověkodnech, Služby rozvoje však bude možné čerpat i prostřednictvím člověkohodin (1 člověkoden = 8 člověkohodin). Čerpání času konzultanta bude zaokrouhlováno na celé hodiny dolů. Akceptací objednávky vzniká dílčí smlouva na provedení konkrétních Služeb rozvoje. Dílčí smlouva se řídí ustanoveními v ní obsaženými a touto Smlouvou.

1.5. Služby rozvoje budou ze strany Objednatele akceptovány po jejich předání Poskytovatelem v termínu sjednaném Smluvními stranami. Akceptace nebo odmítnutí převzetí jednotlivých Služeb rozvoje probíhá na základě písemného (akceptačního) protokolu, ve kterém jsou případně vyznačeny výhrady Objednatele k jednotlivým zjištěným vadám dané Služby rozvoje a důvody odmítnutí převzetí.

2. Cena a platební podmínky

2.1. Cena Služeb rozvoje je stanovena dle ceníku sazeb uvedených v Příloze č. 5, bez DPH za 1 člověkoden Služeb rozvoje. Cena Služeb rozvoje bude hrazena vždy po akceptaci dílčího výstupu Služeb rozvoje Objednatelem. Ceny jsou uvedeny bez sazby DPH, která bude k cenám připočtena v zákonné výši.

2.2. Cena za 1 člověkoden dané Služby rozvoje dle Přílohy č. 5 zahrnuje veškeré náklady Poskytovatele včetně odměny za udělení práv užití autorských děl vytvořených Poskytovatelem při plnění této Smlouvy a za poskytnutí majetkových práv k AIS JePEK včetně všech jeho úprav v rámci poskytování Služeb rozvoje.

2.3. Platby dle této Přílohy budou hrazeny na základě daňových dokladů – faktur vystavovaných Poskytovatelem v částkách a termínech určených v této Smlouvě bezhotovostním převodem na účet Poskytovatele uvedený v těchto daňových dokladech – fakturách. Splatnost jednotlivých faktur bude

vždy 60 dní ode dne doručení této faktury Objednateli. Poskytovatel odešle Objednateli fakturu elektronicky na e-mailovou adresu: [redacted] alternativně doporučenou poštou na adresu uvedenou v záhlaví této Smlouvy, a to ten stejný den, ve kterém byla faktura vystavena. Má se za to, že faktura byla doručena Objednateli. Pro vyloučení pochybností se uvádí, že prodlení Poskytovatele s odesláním faktury neznamená vzdání se práva na úhradu příslušné ceny.

2.4. Faktura je považována za uhrazenou dnem, kdy bude odpovídající částka připsána na účet Poskytovatele. Nebude-li faktura obsahovat všechny náležitosti a přílohy, které jsou vyžadovány touto Smlouvou (zejm. rozpis práce, kopie akceptačního protokolu), je Objednatel oprávněn fakturu reklamovat u Poskytovatele, a to do 10 dnů od dne jejího doručení Objednateli. Nová lhůta splatnosti začne plynout dnem doručení opravené faktury Objednateli.

2.5. Změna ceny Služeb rozvoje dle této Smlouvy je přípustná pouze v případě změny zákonem stanovené sazby daně z přidané hodnoty. Dojde-li v průběhu plnění dle této Smlouvy ke změně výše příslušné sazby DPH, bude cena s DPH upravena v rozsahu změn příslušné sazby DPH stanovené právními předpisy platnými ke dni uskutečnění zdanitelného plnění, a to formou písemného dodatku k této Smlouvě, podepsaným k tomu oprávněnými zástupci obou Smluvních stran.

3. Doba a místo plnění

3.1. Poskytovatel se zavazuje poskytnout pro Objednatele Služby rozvoje ve lhůtě, která bude stanovena vždy Objednatelem v každé jednotlivé objednávce dle čl. 1.1. této Přílohy č. 2, nejméně však do 15 dnů.

3.2. Řádné plnění dodané Poskytovatelem do 5 pracovních dní po termínu stanoveném v každé jednotlivé objednávce je považováno za plnění v souladu s touto Smlouvou a nebude považováno za prodlení na straně Poskytovatele. Řádné převzetí a předání konkrétních Služeb rozvoje a v souladu s touto Smlouvou bude Objednatelem potvrzeno podepsáním akceptačního protokolu.

3.3. Místem plnění je sídlo Objednatele, pokud to však povaha plnění této Smlouvy, zejm. Přílohy č. 2 této Smlouvy umožňuje, je Poskytovatel oprávněn provádět části Díla také vzdáleným přístupem.

4. Výhrada změny závazku

4.1. Objednatel si v souladu s § 100 odst. 2 ZZVZ vyhrazuje možnou změnu v osobě Poskytovatele Služeb rozvoje, a to v případě, že budou splněny následující podmínky:

a) tato Smlouva bude předčasně ukončena z důvodu odstoupení od Smlouvy v části realizace Díla nebo v části Služeb rozvoje, a to za podmínek v této Smlouvě uvedených,

b) dojde k převedení práv a povinností ze Smlouvy z Poskytovatele na jiného poskytovatele (postoupení smlouvy),

c) práva a povinnosti ze Smlouvy mohou být převedena pouze na poskytovatele, který v zadávacím řízení na tuto veřejnou zakázku podá nabídku, a o němž Objednatel (nebo jím jmenovaná hodnotící komise) v dokumentaci k Veřejné zakázce prohlásí, že splnil podmínky účasti v Zadávacím řízení,

d) k převzetí práv a povinností ze Smlouvy mohou být Objednatelem postupně vyzýváni poskytovatelé v pořadí, v jakém se umístili v rámci hodnocení jejich nabídek,

e) nový poskytovatel bude při plnění smlouvy vázán cenami, které uvedl ve své nabídce v rámci Veřejné zakázky,

f) nový poskytovatel na základě výzvy Objednatele předloží doklady o kvalifikaci v rozsahu dle čl. 6 Zadávací dokumentace; doklady prokazující základní způsobilost podle § 74 ZZVZ a profesní způsobilost podle § 77 odst. 1 ZZVZ musí prokazovat splnění požadovaného kritéria způsobilosti nejpozději v době 3 měsíců přede dnem doručení výzvy k předložení dokladů novému poskytovateli.

Příloha č. 3 – Služby provozu AIS a Služby podpory AIS

Smluvní ujednání o Službách provozu AIS a Službách podpory AIS o souvisejících právech a povinnostech Smluvních stran

1. Předmět Služeb provozu a Služeb podpory

1.1. Předmětem plnění dle této smlouvy je v návaznosti na ustanovení čl. 2.4. Smlouvy také závazek Poskytovatele poskytovat Objednateli Služby provozu AIS a Služby podpory AIS, tedy takových služeb, které nejsou předmětem plnění dle bodů 2.2. a 2.3. Smlouvy. Plnění dle tohoto bodu bude realizováno na základě výzvy Objednatele.

2. Cena a platební podmínky

2.1. Cena Služeb provozu a Služeb podpory je stanovena dle ceníku sazeb uvedených v Příloze č. 5, bez DPH za 1 kalendářní měsíc poskytování Služeb provozu a Služeb podpory. Cena Služeb provozu a Služeb podpory bude hrazena vždy zpětně po skončení příslušného kalendářního měsíce, ve kterém byly Služby provozu a Služby podpory poskytovány. Ceny jsou uvedeny bez sazby DPH, která bude k cenám připočtena v zákonné výši.

2.2. Platby dle této Přílohy budou hrazeny na základě daňových dokladů – faktur vystavovaných Poskytovatelem v částkách a termínech určených v této Smlouvě bezhotovostním převodem na účet Poskytovatele uvedený v těchto daňových dokladech – fakturách. Splatnost jednotlivých faktur bude vždy 60 dní ode dne doručení této faktury Objednateli. Poskytovatel odešle Objednateli fakturu elektronicky na e-mailovou adresu: [redacted] alternativně doporučenou poštou na adresu uvedenou v záhlaví této Smlouvy, a to ten stejný den, ve kterém byla faktura vystavena. Má se za to, že faktura byla doručena Objednateli. Pro vyloučení pochybností se uvádí, že prodlení Poskytovatele s odesláním faktury neznamená vzdání se práva na úhradu příslušné ceny.

2.3. Faktura je považována za uhrazenou dnem, kdy bude odpovídající částka připsána na účet Poskytovatele. Nebude-li faktura obsahovat všechny náležitosti a přílohy, které jsou vyžadovány touto Smlouvou (zejm. rozpis práce, kopie akceptačního protokolu), je Objednatel oprávněn fakturu reklamovat u Poskytovatele, a to do 10 dnů od dne jejího doručení Objednateli. Nová lhůta splatnosti začne plynout dnem doručení opravené faktury Objednateli.

2.4. Změna ceny Služeb provozu a Služeb podpory dle této Smlouvy je přípustná pouze v případě změny zákonem stanovené sazby daně z přidané hodnoty. Dojde-li v průběhu plnění dle této Smlouvy ke změně výše příslušné sazby DPH, bude cena s DPH upravena v rozsahu změn příslušné sazby DPH stanovené právními předpisy platnými ke dni uskutečnění zdanitelného plnění, a to formou písemného dodatku k této Smlouvě, podepsaným k tomu oprávněnými zástupci obou Smluvních stran.

3. Doba a místo plnění

3.1. Poskytovatel se zavazuje poskytovat Objednateli Služby provozu a Služby podpory každý kalendářní měsíc počínaje dnem, kdy dojde k předání a akceptaci poslední části Díla, tj. předání díla jako celku dle této Smlouvy, a to po dobu 72 kalendářních měsíců.

3.2. Místem plnění je sídlo Objednatele, pokud to však povaha plnění této Smlouvy, zejm. Přílohy č. 3 této Smlouvy umožňuje, je Poskytovatel oprávněn provádět části Díla také vzdáleným přístupem.

4. Rozsah poskytování Služeb provozu a Služeb podpory

4.1. Poskytovatel se zavazuje poskytovat po dobu stanovenou touto Smlouvou Objednateli Služby provozu a Služby podpory, a to v souladu a dle podmínek stanovených v Příloze č. 4 této Smlouvy.

Příloha č. 4 – Technická dokumentace *(v rámci zadávací dokumentace označeno jako Příloha č. 3)*

1. Manažerské shrnutí

Tento dokument je pracovní verzí vybraných kapitol pro Technickou dokumentaci, která je předmětem dodávky v rámci projektu JePEK – Jednotný portál evidence kontrol.

Tento dokument popisuje procesy a funkční obsah systému, shrnuje závěry a též základní technologické komponenty, avšak s možností navrhnout technickou implementaci alternativním způsobem v částech, které nejsou předmětem Aplikace JePEK ve fázi 1.

JePEK přináší významné výhody pro všechny kategorie uživatelů. Podnikatelé získají lepší přehled o historicky provedených kontrolách a také možnost se připravit na budoucí kontroly, které lze dopředu podnikateli sdělit bez ohrožení účelu kontroly. Kontroloři mohou efektivněji plánovat a koordinovat své aktivity – lépe stanovit tzv. rizikový profil kontrolovaného subjektu. Administrátoři z MPO budou mít nástroje pro komplexní analýzu a správu kontrolních procesů. Celkově systém přispívá k transparentnosti, efektivitě a kvalitě kontrolních aktivit v ČR.

1.1. Rekapitulace základního záměru

Stávající legislativa, především pak zákon č. 255/2012 Sb., o kontrole (kontrolní řád), ve znění pozdějších předpisů (dále jen “kontrolní řád”), předpokládá vzájemnou spolupráci kontrolních orgánů a koordinaci přípravy plánů kontrol, ale nejsou pro ni vytvořeny odpovídající celoplošně zavedené podmínky, například sdílené informační systémy.

Kontrolní orgány vzájemně nemají většinou přehled o činnosti dalších kontrolních orgánů u konkrétního podnikatele, zároveň však vůči konkrétnímu podnikateli vykonává kontrolní činnost více orgánů najednou. Ač neplánovaně, může tak docházet k nadměrnému zatěžování podnikatelů v případech, kdy jsou podnikatelé povinni podstoupit více kontrol různými kontrolními orgány v relativně krátkém čase.

Kontrolní orgány neví, co bylo u podnikatele kontrolováno a jaké podklady byly ke kontrole použity. Přitom se znalostí těchto informací a lepší dostupnosti v minulosti již zajištěných podkladů by výkon kontrol mohl být efektivnější jak pro samotné kontrolní orgány, tak pro podnikatelské subjekty.

Pro následující 1. fázi vývoje komplexního řešení agendového informačního systému JePEK bylo v součinnosti s oddělením kybernetické bezpečnosti Ministerstva průmyslu a obchodu vytvořeno hodnocení kyberbezpečnostních aktiv, které v tuto chvíli nezahrnuje zhodnocení některých prvků celkové zamýšlené aplikace, jelikož v době tvorby tohoto dokumentu nebylo Objednateli zřejmé případné technické provedení těchto funkčních prvků. Z pohledu kybernetické bezpečnosti jsou tedy všechny funkcionality, mimo ty, které se týkají 1. fáze, vnímány jako rozvojové.

Popis bezpečnostního aktiva v 1. fázi se týká následujícího:

- Označení kontrolního orgánu
- Označení kontrolované osoby
- Označení předmětu kontroly
- Datum zahájení kontroly
- Datum ukončení kontroly
- Kontrolní zjištění (zjištěny nedostatky ANO/NE bez detailu)

Do informačního systému bude umožněno přihlašování úředníků přes JIPKAAS/CAAIS a podnikatelé přes NIA+REZA. Informační systém bude disponovat následujícími rozhraními (Interface):

1) Web pro MPO, Kontrolní orgány a Podnikatelé

2) API pro informační systémy kontrolních orgánů

3) Rozhraní pro nahrávání excelových souborů s daty

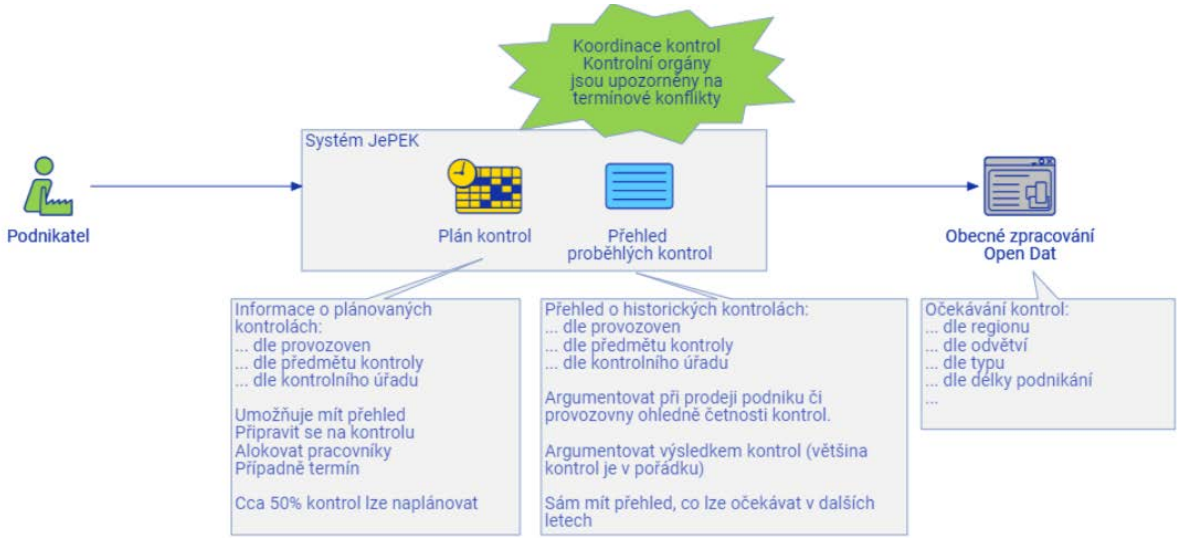
Vazba na systémy kontrolních orgánů bude přes EGON Service bus, resp. ISSS. Očekává se, že provoz informačního systému bude zajištěn jako komplexní služba v cloudu odpovídajícím požadavkům dle specifikací eGC.

V rámci procesu řízení změn, před započetím fáze vývoje, která bude obsahovat prvky mimo ty, jenž byly zhodnoceny pro 1. fázi, bude provedeno následné zhodnocení z pohledu kybernetické bezpečnosti (hodnocení aktiva, analýza rizik, definice plánu zvládání rizik apod.) a do 2. fáze budou následně promítnuty bezpečnostní opatření vyplývající z provedené analýzy tak, aby byla pokryta všechna neakceptovatelná rizika. Hodnocení kybernetické bezpečnosti bude

provedeno v souladu s platnou legislativou ZoKB a VoKB v době provedení analýzy, a přípravu tohoto hodnocení zajistí Objednatel ve spolupráci s oddělením kybernetické bezpečnosti.

1.2. Systém JePEK

Řešením pro lepší koordinaci a sdílení informací je vytvoření nového informačního systému označovaného jako Jednotný portál evidence kontrol (JePEK). Hlavním cílem projektu je zvýšit efektivitu přípravy a průběhu kontrol podnikatelských subjektů, především pak snížit administrativní zátěž spojenou s kontrolní činností na straně podnikatelů, zlepšit spolupráci kontrolních orgánů a zdokonalit komunikaci mezi nimi a podnikateli a případně i veřejností.



Prostřednictvím zamýšleného portálu by mělo dojít k vytvoření prostoru, kde:

1. Kontrolní orgány budou moci sdílet:
   - plán kontrol neboli individualizovaný kalendář kontrol jednotlivých subjektů, za předpokladu, že tento naplánovaný druh kontroly neohrozí účel kontroly, pokud by ji mohl zmařit, pak i anonymně s cílem umožnit koordinaci,
   - průběh kontroly a kategorizované výsledky kontrol.

2. Podnikatelé získají:
   - Každý podnikatel získá individualizovaný přehled naplánovaných kontrol své provozovny (pouze ty co lze dopředu ohlásit, aby nebyl zmařen účel kontroly) a zároveň přehled kontrol, které již kontrolní orgán
   - komunikoval kontrolovanému subjektu, budou do systému JePEK zaznamenány zpětně.
   - Kontrolní orgány se budou moci na základě sdílení plánů kontrol lépe organizovat a plánovat kontroly u podnikatelů.
3. Veřejnost získá:
   - Obecné informace o kontrolní činnosti v České republice a tím (po zpracování například datovými novináři) lepší povědomí o úsilí orgánů veřejné zprávy o zajištění stability podnikatelského prostředí a dalších aspektech vykonávání kontrolní činnosti.

1.3. Flexibilita a zobecnění specifických postupů

Systém JePEK bude připraven respektovat různou situaci jednotlivých kontrolních orgánů co do způsobu provádění kontrol, evidence kontrol, míry evidovaných informací, způsobu plánování a v neposlední řadě technické i personální vybavení. Systém JePEK neaspiruje na unifikaci kontrolních orgánů, ale vychází vstříc jejich potřebám, jazyku,

zvyklostem a tyto generalizuje do podoby, která bude srozumitelná jak ostatním kontrolním orgánům, tak podnikatelům, kteří na kontroly pohlíží ze zcela jiného úhlu pohledu.

1.3.1. Struktura dat v JePEK

Budou jimi vybrané údaje o provedené kontrole podle zákona č. 255/2012 Sb., zákon o kontrole (kontrolní řád) [KŘ]:

- označení kontrolního orgánu dle §12 odst. 1 písm. a), KŘ;
- označení kontrolované osoby dle §12 odst. 1 písm. d), KŘ a kontrolované provozovny (ID provozovny ze základních registrů);
- označení předmětu kontroly a právního předpisu kontroly dle §12 odst. 1 písm. e), KŘ;
- datum zahájení kontroly dle §12 odst.1 písm. f), KŘ;
- datum ukončení kontroly dle §18 KŘ;
- kontrolní zjištění dle §12 odst. 1 písm. h) KŘ.

Vybrané údaje u bodů a), b) jsou podrobněji specifikovány referenčními údaji ze zákona č. 111/2009 Sb., o základních registrech [ZZR].

Doplnění k výše uvedenému písmenu f) tzn. „kontrolní zjištění“:

Vzhledem k tomu, že diskuse o tomto konkrétním parametru se stále vyvíjí, protože je třeba vyhovět požadavkům na ochranu osobních údajů, bude hledáno takové technické a legislativní řešení (současné nebo budoucí), které umožní poskytovat, za předem definovaných podmínek, „výsledek“ kontrolního zjištění spolupracujícím kontrolním orgánům, a to ve stručné formě.

Tento údaj bude nabývat dvou hodnot, a to buď „zjištěné nedostatky – ANO“ (s odkazem na porušené ustanovení § zákona) nebo „zjištěné nedostatky – NE“.

JePEK přináší významné výhody pro všechny kategorie uživatelů. Podnikatelé získají lepší přehled o historicky provedených kontrolách a také možnost se připravit na budoucí kontroly, které lze dopředu podnikateli sdělit bez ohrožení účelu kontroly. Kontroloři mohou efektivněji plánovat a koordinovat své aktivity – lépe stanovit tzv. rizikový profil kontrolovaného subjektu. Administrátoři z MPO budou mít nástroje pro komplexní analýzu a správu kontrolních procesů. Celkově systém přispívá k transparentnosti, efektivitě a kvalitě kontrolních aktivit v ČR.

2. Obsah

3. Úvod a odkazy

3.1. Odkazy na související dokumenty

Následující dokumenty jsou nedílnou součástí projektu JePEK:

- Právní:
  - Usnesení vlády,
  - Opatření ministra,
  - Nařízení vlády,
  - Kontrolní řád.

- Popis Aplikace ve fázi 1,
- Žádost na OHA,
- Zdrojové kódy první verze systému, včetně dílčí dokumentace.

3.2. Použité pojmy a zkratky

Pojem	Význam
AIS	agendový informační systém
browse	zobrazení seznamu formou tabulky, typicky s posuvníkem
bulk load	způsob nahrání větších objemů dat
credentials	typicky jméno a heslo
DB	databáze, úložiště dat softwarového řešení
deeplink	webový odkaz směřující přímo na diskutovanou skutečnost v rámci informačního systému
DIP	Databáze informačních povinností podnikatelů
eGON	eGoverment, používáno jako označení sady webových služeb informačního systému základních registrů
eOP	elektronický občanský průkaz
ETL	Extraction, transformation, load, užívání pro označení operace s daty
Frontend	Část softwarového řešení, které zajišťuje interakci uživatele se systémem, tedy typicky grafické uživatelské rozhraní systému

grace perioda	typicky časová úleva od plnění vybrané povinnosti
GUI	Grafické uživatelské rozhranní
JePEK	Jednotný portál evidence kontrol
JIP	Jednotný indentitní prostor – název informačního systému
job	dávková zpracování bez uživatelského rozhraní
KO	Kontrolní orgán, typicky orgán veřejné moci určený k dominantně prováděné kontrolní činnosti
KŘ	Kontrolní řád, zákon č. 255/2012 Sb.
MPO	Ministerstvo průmyslu a obchodu
NIA	Národní identitní autorita
OHA	Odbor hlavního architekta eGovermentu
On behalf	V zastoupení, jednání za někoho jiného
Open Data	Standard popisu datových zdrojů, které jsou k dispozici veřejnosti
OTP	One time password
platforma	typ a vlastnost cloudového řešení
portlet	část portálového řešení dle standardu JSR168
Aplikace ve Fázi 1	Softwarové řešení části systému JePEK, které demonstruje předpokládané základní funkčnosti evidence kontrol a technologické aspekty integrací a provozu systému tak, aby byla ověřena realizovatelnost řešení v příslušných technologiích.
RBAC	Role Based Access Control - způsob řízení přístupu k systému pomocí business a aplikačních rolí
REZA	Registr zastoupení (připravované řešení)
ROB	Registr obyvatel, jeden ze základních registrů
ROS	Registr osob, jeden ze základních registrů
RŽP	Registr živnostenského podnikání
Touchpoint	Místo či prostředek interakce mezi uživatelem a řešením JePEK

4. Definice projektu

4.1. Důvod realizace

Cílem projektu JePEK je řešit problém nadměrné byrokracie, se kterou se podnikatelé často setkávají, zejména v souvislosti s různými kontrolami ze strany státních institucí a obecně orgánů veřejné moci. Hlavní myšlenkou je vytvořit **informační systém**, který umožní efektivní koordinaci kontrolních procesů, čímž by se výrazně snížila administrativní zátěž pro podnikatele.

Snížení byrokratické zátěže:

- Podnikatelé jsou často vystavováni opakovaným nebo duplicitním kontrolám různých orgánů, což vytváří zbytečnou administrativní zátěž. Cílem je tuto zátěž minimalizovat tím, že se kontroly sjednotí a optimalizují.

Koordinace kontrol:

- Informační systém by sloužil jako centralizovaná platforma, která by umožnila lepší koordinaci mezi kontrolními orgány. Tím by se zajistilo, že jednotlivé kontroly nebudou zbytečně opakované a budou lépe plánované zejména s ohledem na potřeby podnikatelů.

Transparentnost a předvídatelnost:

- Informační systém by umožnil poskytnout podnikatelům s předstihem informace o termínech plánovaných kontrol, jejich zaměření a potřebné dokumentaci, což by zlepšilo podnikatelům možnost se na tyto kontroly připravit a minimalizovat čas a náklady spojené s administrativou.

Automatizace a digitalizace procesů:

- Systém by mohl zahrnovat funkce pro automatické zasílání dokumentů a hlášení, což by usnadnilo a zrychlilo komunikaci mezi podnikateli a kontrolními orgány. Automatizace by rovněž mohla zahrnovat vytváření přehledů o minulých kontrolách, což by zjednodušilo sledování plnění povinností daných legislativou.

Zlepšení spolupráce mezi institucemi:

- Systém by mohl podpořit lepší spolupráci mezi různými státními orgány, které provádějí kontroly. Jednotlivé orgány by měly přístup k informacím o tom, které kontroly již byly provedeny, což by vedlo k efektivnějšímu využívání zdrojů (například personálních kapacit) kontrolních orgánů.

Naplňování digitální strategie státu

- Projekt reaguje také na digitální strategii EU: https://reform-support.ec.europa.eu/what-we-do/digital-transition_cs
- Evropská komise sleduje digitální pokrok členských států prostřednictvím zpráv indexu digitální ekonomiky a společnosti (DESI) od roku 2014. Od roku 2023 a v souladu s programem politiky digitální dekády 2030 je nyní DESI začleněn do zprávy o stavu digitální dekády a využíván ke sledování pokroku při plnění digitálních cílů.
- Projekt je zařazen v Národním plánu obnovy.

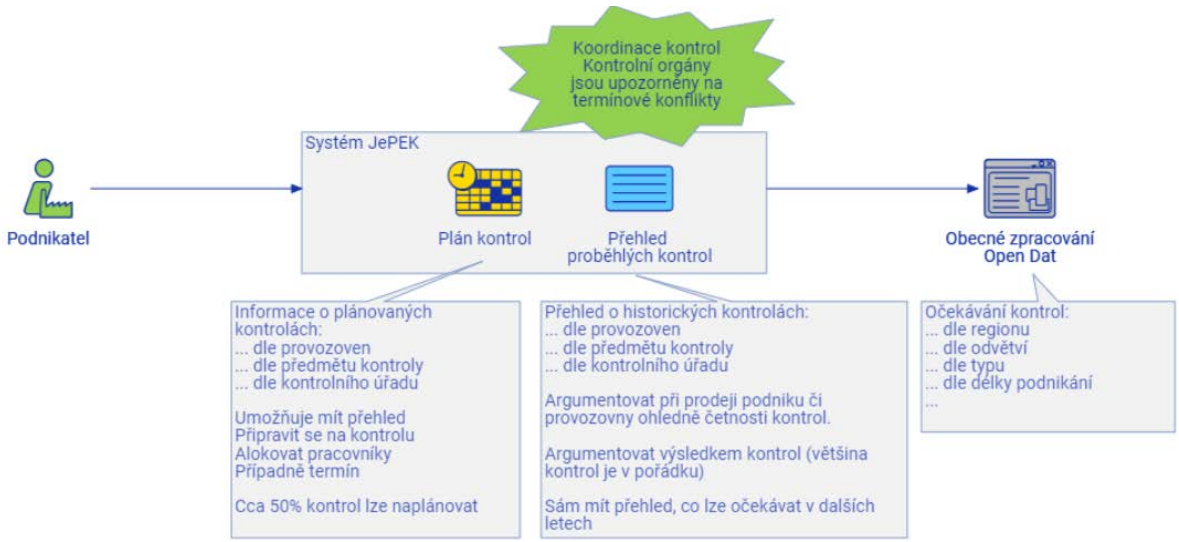
4.2. Cíle a přínosy projektu

Očekávané přínosy jsou:

- Úspora času a nákladů pro podnikatele díky méně častým či lépe koordinovaným kontrolám.
- Vyšší transparentnost podnikatelského prostředí a související úspora nákladů díky evidenci kontrol.
- Zvýšení efektivity kontrolních orgánů díky lepší výměně informací a zamezení duplicitnímu úsilí.
- Zlepšení právního povědomí podnikatelů, které by mohlo díky transparentnějšímu procesu kontrol vést podnikatele ke kvalitnějšímu dodržování předpisů.
- Celkové zlepšení vztahu veřejnosti vůči státní správě díky přehledovým údajům o kontrolní činnosti.

Cílem projektu je tedy vytvořit nástroj, který zjednoduší podnikatelské prostředí, podpoří efektivnější komunikaci mezi podnikateli a státními institucemi a zároveň zvýší celkovou transparentnost a efektivitu kontrolních procesů.

Měřitelnými výstupy pak budou informace o koordinaci kontrol, tedy procento koordinovaných kontrol.



4.3. Výstupy

I. Technická dokumentace – tento materiál včetně příloh.

II. Softwarový produkt v bazálním rozsahu funkčností (Aplikace ve fázi 1) společně se zdrojovými kódy.

III. Zavedení a provoz informačního systému JePEK v plné funkčnosti podporující:

- Systém pro správu a evidenci kontrol u podnikatelů navázanou na státní centrální registry podnikatelů (např. ROS)
- Koordinaci kontrol pro kontrolní orgány prostřednictvím:
  - GUI systému,
  - dávkové komunikace – předávání excelových souborů nahrávaných manuálně,
  - dávkové komunikace s vybranými systémy veřejné správy,
  - automatické vzdálené komunikace—integrace na systémy kontrolních orgánů,
- Datové zdroje
  - pro podnikatele,
  - kontrolní orgány,
  - širokou veřejnost prostřednictvím Open Data.

Systém JePEK pak umožní vytvořit po určité době zaběhnutí:

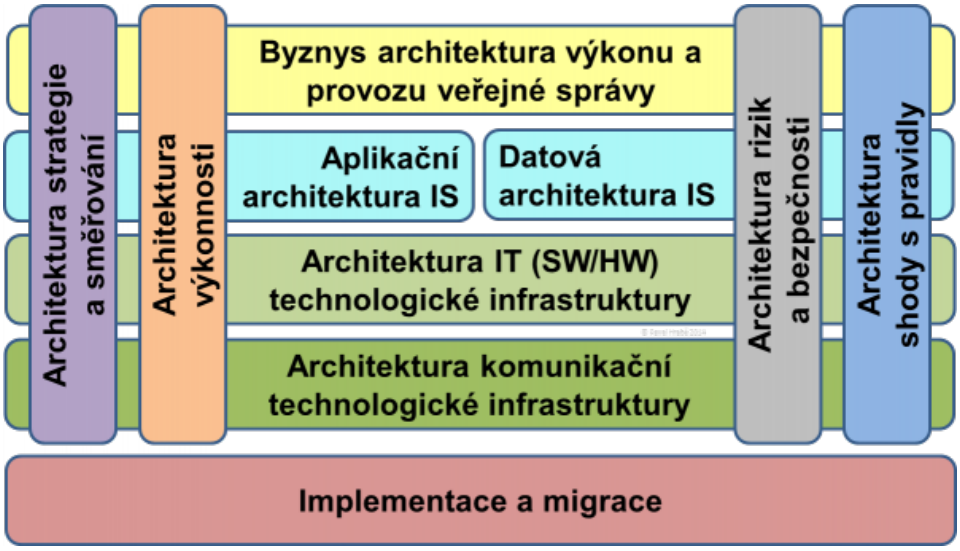
- Statistiky o kontrolní činnosti pro MPO, které mohou být obecně zveřejněné,
- Výstupy pro podnikatele, které mohou být použity pro analýzu a doložení reálné historické kontrolní činnosti podnikatele.

5. NÁVRH ŘEŠENÍ

Návrh vychází z doporučení ohledně modelovaných architektur dle https://archi.gov.cz/nar_dokument:struktura_modelovanych_architektur.

V podobě k 30.9. se dokument zaměřuje na Business architekturu, Aplikační architekturu a Datovou architekturu.

V podobě k 30.11. pak i na technologické a komunikační prvky architektury a projektové či implementační a provozní dopady.



5.1. Business architektura

Business architektura řešení sdružuje pohled na přidanou hodnotu řešení, identifikaci a plánovanou realizaci business procesů včetně vyjasnění participantů, aktérů a jejich primárních odpovědností a k popisu způsobu, jakým orgán veřejné moci plní své úkoly, řídí své procesy a jaké informační systémy využívá k podpoře svých funkcí, a to ve vztahu k předmětné funkčnosti, tedy vzájemné koordinaci v oblasti plánování, provádění kontrol, a v zpřístupňování evidenčních informací o provedených kontrolách. Business architektura pro orgán veřejné moci tedy slouží k zajištění že informační systémy a procesy jsou nastaveny tak, aby podporovaly efektivní fungování úřadu, naplňování zákonných povinností, transparentnost a odpovědnost vůči veřejnosti.

5.2. Jednotliví aktéři pro práci se systémem JePEK

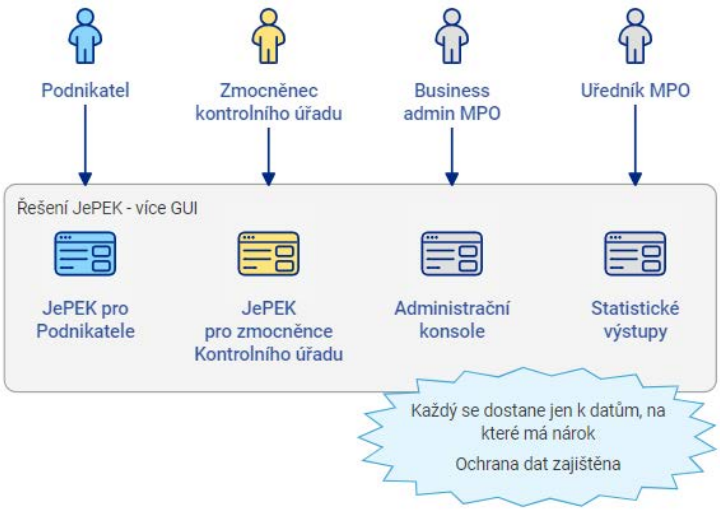
5.2.1. JePEK aktéři

Jednotliví aktéři budou pracovat s různými frontendy/touchpointy navrhovaného řešení Jednotného portálu evidence kontrol. Smysl rozdělení do více frontendů je dán:

a) typickými technologickými možnostmi, ve kterých může být JePEK realizován,

b) rozdělením funkcí a zabránění případným chybám v nastavení práv a konfigurací,

c) rozdílná logika přístupu k příslušnému frontendu.

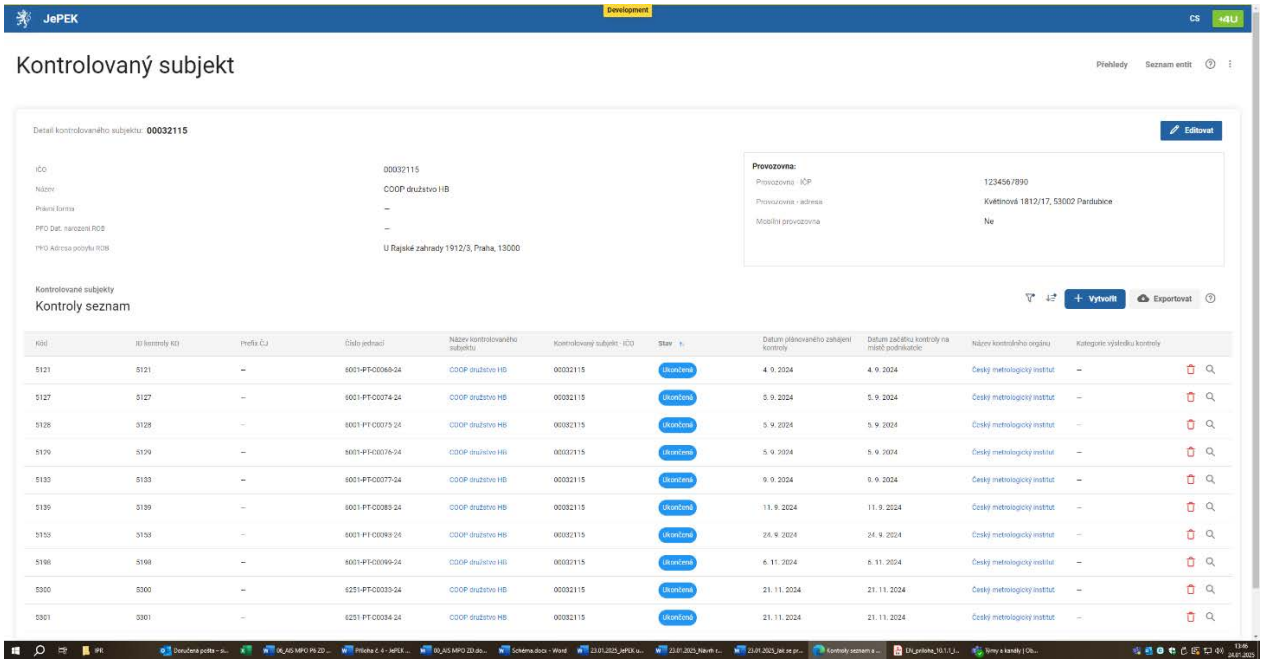


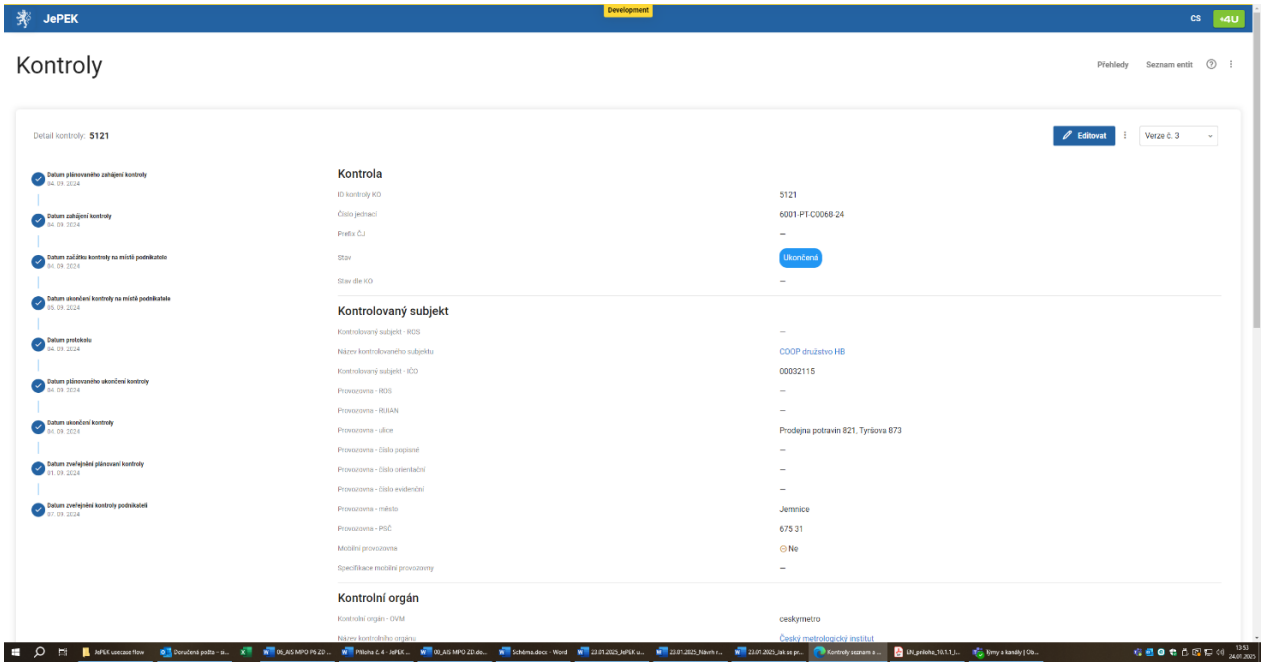
5.2.2. Podnikatelé

Podnikatelem je podle § 420 odst. 1 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen "občanský zákoník"), samostatně vykonává na vlastní účet a odpovědnost výdělečnou činnost živnostenským nebo obdobným způsobem se záměrem činit tak soustavně za účelem dosažení zisku. Současně definici podnikatele obsahuje i zákon č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů, podle § 5 odst. 1 živnostenského zákona ve spojení s § 2 téhož zákona. Podnikatelem dle živnostenského zákona je fyzická nebo právnická osoba, která provozuje činnost samostatně, vlastním jménem, na vlastní odpovědnost, za účelem dosažení zisku a za podmínek stanovených živnostenským zákonem. Ve vztahu k předmětu studie jsou podnikatelé zároveň kontrolovanými osobami (§ 1 kontrolního řádu).

Podnikatelé budou mít přístup do JePEK prostřednictvím **online portálu**, který jim poskytne přehled o jejich kontrolách. JePEK jim umožní vidět detaily kontrol, které jsou označeny jako viditelné pro kontrolované subjekty, včetně důvodu a termínu kontroly. Po přihlášení do JePEK podnikatelé **získají následující přehled:**

- Informace o plánovaných kontrolách: Uvidí seznam budoucích kontrol, které lze dopředu podnikateli sdělit, aniž by byl účel kontroly dopředu změřen, včetně datumu, typu kontroly a kontrolního orgánu.
- Zkontrolovat historii kontrol: Mají přístup k záznamům o všech minulých kontrolách, včetně jejich výsledků a zjištěných nálezů s odkazem na konkrétní paragraf předmětného zákona podle kterého byla kontrola realizována.
- Vyhledávat dle parametrů: JePEK umožní filtrování a vyhledávání podle času, druhu kontroly nebo jiných kritérií.





Výhody a přínosy:

Přehled provedených kontrol: Historie kontrol bude dostupná na jednom místě.

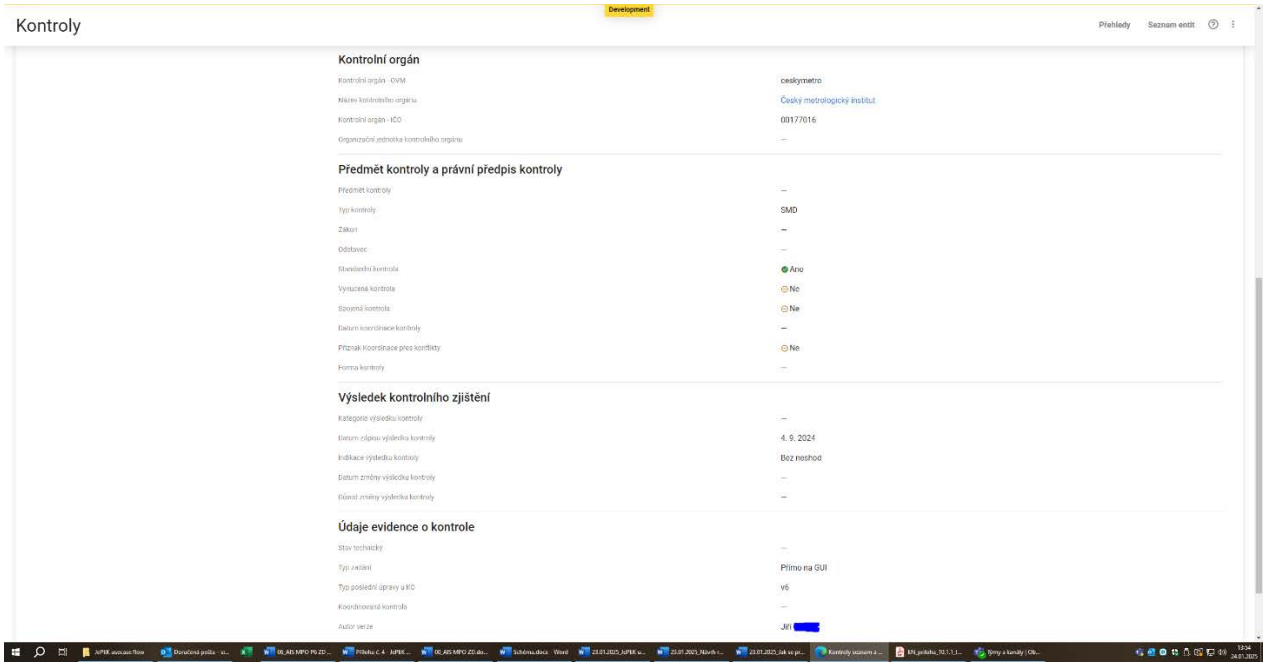
Transparentnost: Podnikatelé budou mít přehled o plánovaných kontrolách, což jim umožní lépe se připravit.

Snížení administrativní zátěže: Díky přehledu o kontrolách mohou podnikatelé efektivněji plánovat své aktivity a minimalizovat přerušení provozu.

Koordinace kontrol: Systém umožní podnikatelům vidět, které kontroly jsou plánovány ostatními kontrolními orgány a také dojde na straně podnikatele k eliminace nutnosti žádat o informace z různých kontrolních orgánů.

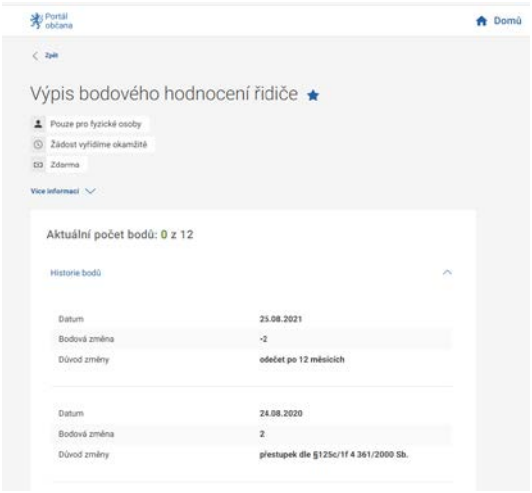
Zlepšení vztahů s kontrolními orgány: Transparentnost a předvídatelnost kontrol (tam kde dopředné nahlášení kontroly neohrozí účel kontroly) může vést k lepšímu vztahu mezi podnikateli a kontrolními orgány, což může přispět k hladšímu průběhu kontrol.

Pro zobrazení detailního stavu kontroly, je podnikateli umožněno například pomocí ikony lupy rozkliknout detail vybrané kontroly, kde bude možné vidět, zda je kontrola plánovaná, v jaký termín, jakým kontrolním orgánem, jaká součinnost bude od podnikatele vyžadována, případně zda kontrola již probíhá nebo je ukončená, a s jakým výsledkem.



Pro dokreslení představy, jak by se mohly informace o plánovaných a realizovaných kontrolách podnikateli vizualizovat, také uvádíme níže příklad již funkční služby na Portálu občana „Výpis bodového hodnocení řidiče“, kterou je JePEK z části inspirován. Zde je například vidět, že kontrolovaných řidič dostal dne 24. 9. 2020 sankci s odkazem na porušení konkrétního paragrafu zákona podle, kterého byla kontrola provedena.

V případě JePEK bude takových záznamů pochopitelně více, a to z titulu počtu jednotlivých kontrolních orgánů, od kterých budou data o plánovaných a historicky realizovaných kontrolách v JePEK shromažďovány. Též je požadováno, aby výsledek kontroly nabýval pouze dvou hodnot, a to buď „zjištěné nedostatky – ANO“ (s odkazem na porušené ustanovení § zákona) nebo „zjištěné nedostatky – NE“.



Rozpad usecase:

Uživatel - Podnikatel				
	BUC	**M**		Úvodní stránka/portál s obecnými informacemi (menu, patička atp.)
	SUC	L		Přihlášení pro podnikatele jako občana
	BUC	M		Zadání jména a hesla (JIP/KAAS CAAIS)
	SUC	M		Převedení na přihlášení vůči NIA - více možností
	SUC/BUC	L		Přihlášení přes datovou schránku
	SUC	M		Zpracování informace o poskytnutí souhlasu s poskytnutím údajů (jednorázově, trvale)
	SUC	M		Načtení/zpracování informací o organizacích, kam má osoba přístup - data z ROS, data z REZA, tranzitivní přístupy
	SUC	M		Načtení informace o zastupovaných právnických osobách na základě plné moci
	SUC	M		Načtení informace o zastupovaných právnických osobách na základě prokury
	BUC	S		Odhlášení
	BUC	S		Obrazovka: Neautorizováno
	BUC	S		Obrazovka: Odhlášeno
	BUC	L		Výběr organizace, pokud jich jedna FO osoba bude mít více FO/FOP/PO a to jak majitel, tak zastupování, případně taby pro organizace

	BL	L		Business logika: Ověření práv číst - dle stavu kontroly a konfigurace typu kontroly
	INTG	L		Integrační scénář: zjisti informace o přístupu k FO, FOP a PO, které příslušná FO může zastupovat
	INTG	L		Integrační scénář traverzování (tj. zjisti všechny uzly v rámci grafu zastupování, vyloučit zacyklení - v podstatě kostra grafu)
	BUC	S		Zobrazení individuálního nastavení notifikací
	BUC	M		Změna evidence požadavané notifikace vzhledem k subjektu, zadání emailu či mobilu, pokud není v ROS, tedy budu dostávat právě já (aby nedostávali ne nutně všichni vlastníci)
	BL	L		Výpočet zveřejnění pro notifikaci podnikatele (dle pravidel zveřejnění dle typu kontroly)

Subjekt PO/FO				
	BUC	M		Rychlé vyhledávání IČO, RČ, DIČ s posledním hledáním
	BUC	M		Vyhledání dle IČP nebo heuristikou město ulice číslo (popisné, orientační) - nalezne subjekty podle adresy
	INTG	L		Integrační scénář na RŽP, vyhledání podle IČP nebo jiného typu, způsobu
	BL	L		Heuristika pro vyhledávání poboček na částečnou shodu adresy, (když není zadánoIČO)
	BL	L		Vyhledání firmy podle více kritérií (subselect názvu, část adresy)
	BL	L		Ověřování přítupu k subjektu (od uživatele-úředníka) pro specifické uživatele (například policie)
	BUC	L		Zobrazení hitlistu s možností výběru, řazení, stránkovaný výpis (vyhledávání podle více kritérií a více zdrojů)
	INTG	M		Integrační scénář vyhledávání v základních registrech ROS
	INTG	L		Integrační scénář Načtení PO ze základních registrů
	INTG	L		Načtení FO/FOP ze základních registrů jako referenčního údaje v ROSu

	INTG	M		Načtení provozoven z základních registrů jako referenčního údaje v ROSu
	INTG	M		Načtení provozoven z RŽP
	SUC	L		Načtení specifických příznaků - insolvence aj., nucená správa … a dořešení přístupů ve specifických případech
	INTG	M		Načtení prokury z REZA
	BUC	L		Zobrazení detailu FO/FOP
	BUC	L		Zobrazení detailu PO
	BUC	L		Zobrazení majetkové struktury (vlastníci) a prokury
	BUC	S		Zobrazení kontaktů ze vlastníků a zástupců
	BUC	S		Zobrazení sídla a emailů a jiných kontaktů
	SUC	0		Zpracování provozoven z Živnostenského rejstříku (resp ROS dle toho, co je zapsaného)
	BUC	L		Zobrazení seznamu provozoven a a sídla z Živnostenského rejstříku, filtrování, třídění, zobrazení na mapových podkladech
	BUC	M		Zobrazení detailu provozovny
	INTG	M		Načtení historie PO v případě, kdy zpětně zadávaná kontrola odkazuje před platnost aktuálního záznamu (např.firma se před časem jmenovala jinak)
	BUC	L		Zobrazení historie subjektu PO (včetně referenčních údajů a provozoven)
	BUC	M		Zobrazení historie kontaktů
	SUC	M		Načtení adresního místa jako referenčního záznamu z RUIAN (z ROS)
	BL	L		Business logika - výpočet rizikového skóre (nebo alespoň semaforu) na subjektu
	BL	L		Business logika - Věcná koordinace kontrol na základě příbuzného předmětu kontroly
	BL	L		Business logika - Termínová koordinace kontrol na základě překryvů intervalů

5.2.3. Subtypy uživatelů typu Podnikatel

Podnikatel, pracující jako uživatel příslušného frontendu systému JePEK, přistupující k datům kontrolovaného subjektu, bude jedním z následujících subtypů:

- Podnikatel sám o sobě, pokud je zapsaný jako jednočlenný statutární orgán kontrolovaného subjektu.
- Podnikatel sám o sobě, pokud je zapsaný jako člen kolektivního statutárního orgánu kontrolovaného subjektu.

- Podnikatel, který je členem statutárního orgánu jiné právnické osoby, která je členem statutárního orgánu zobrazovaného kontrolovaného subjektu.
- Osoba s evidovanou plnou mocí v REZA, a to:
    - Zastoupení fyzických osob, které splňují výše uvedená pravidla,
    - Zastoupení právnických osob zapsaná do veřejného rejstříku a následně transformována na jednu z implicitních plných mocí, kterou bude systém REZA nabízet,
    - *Poznámka: technicky se nepřipouští jiné plné moci než ty, které jsou evidovány v REZA. Pokud ale předloží fyzická osoba plnou moc (mimo REZA) a úředník ji uzná jako relevantní, pak bude možné použít plnou moc z REZA, kterou tam zapíše úředník poté, co uzná předloženou plnou moc, že se vztahuje na přístup údajů z JePEK.*
    - *Postup realizace registrace plné moci úředníkem orgánu veřejné moci bude upřesněn v organizačním předpisu MPO.*

5.2.4. Kontrolní orgány

Zákonem č. 255/2012 Sb., o kontrole (kontrolní řád), ve znění pozdějších předpisů, jsou kontrolní orgány vymezeny jako orgány moci výkonné, orgány územních samosprávných celků, jiné orgány a právnické nebo fyzické osoby, pokud vykonávají působnost v oblasti veřejné správy při kontrole činnosti orgánů moci výkonné, orgánů územních samosprávných celků, jiných orgánů, právnických a fyzických osob.

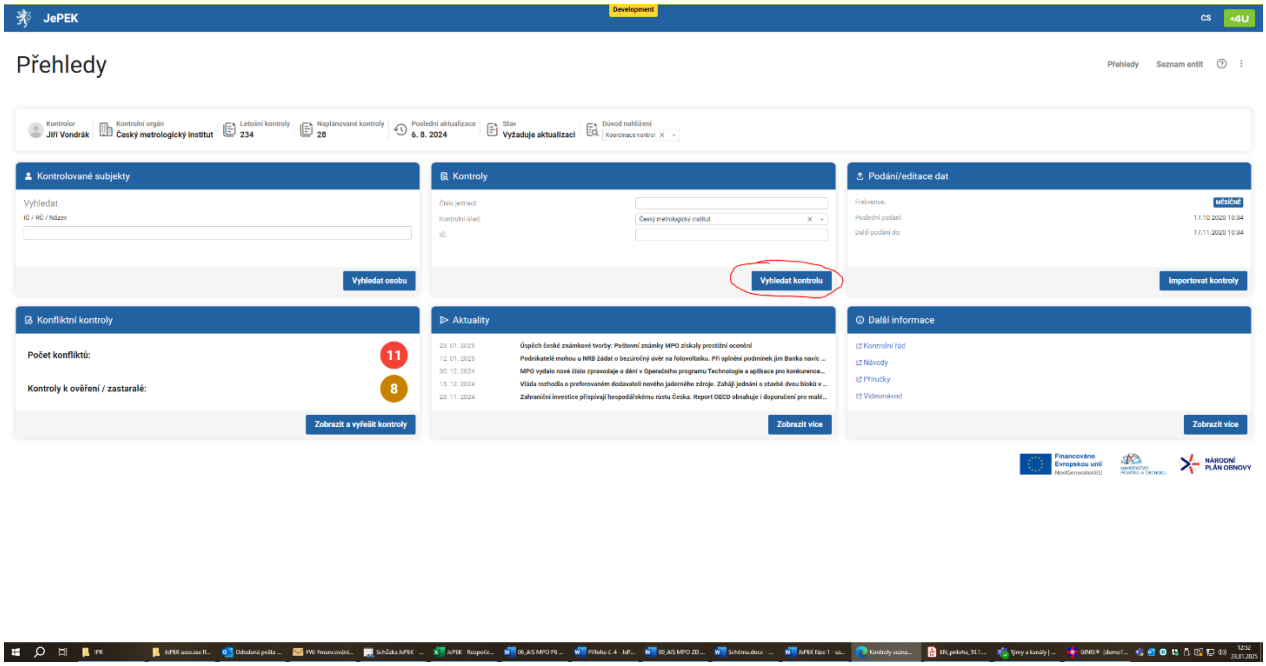
Za kontrolní orgány se systémem budou pracovat Reprezentanti kontrolních orgánů.

Kontrolorů se JePEK dotkne jako nástroje ke koordinaci jejich kontrolní činnosti. Po přihlášení prostřednictvím systému JIP/KAAS (nebo jeho náhrady CAAIS) budou mít přístup k funkcím JePeK, který jim umožní:

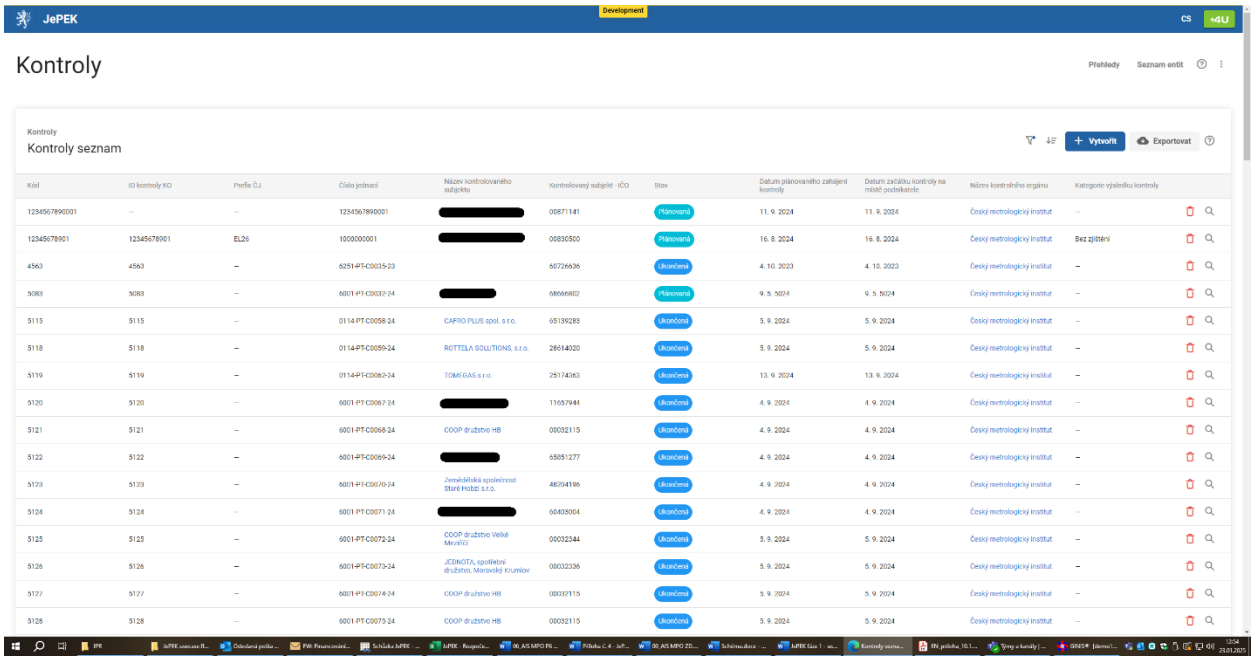
- Plánovat kontroly: Na základě sdílených informací o ostatních plánovaných kontrolách se vyhnout duplicitě a efektivně sladit termíny.
- Vidět výsledky kontrol jiných/spolupracujících kontrolních orgánů:
    - Podle zjištěného výsledku kontroly ve formátu: „zjištěné nedostatky – ANO“ (s odkazem na porušené ustanovení § zákona) nebo „zjištěné nedostatky – NE“, bude moci příslušný kontrolní orgán, který se chystá na kontrolu k podnikateli, lépe stanovit tzv. rizikový profil kontrolovaného subjektu, respektive podnikatele.
    - Například pokud je podnikatel z pohledu historických kontrol napříč všemi kontrolami od rozdílných kontrolních orgánů více problematický, tzn. z historických výsledků je evidentní, že každá kontrola končí zjištěním s odkazem na porušení konkrétního paragrafového ustanovení zákona, může kontrolní orgán lépe stanovit budoucí profil kontroly.
    - V opačném případě, tzn. kontrolovaný má napříč všemi kontrolními orgány historii výsledků převážně v úrovni: „zjištěné nedostatky – NE“, může kontrolní orgán od kontroly upustit a soustředit se na jiný subjekt, který vykazuje vyšší míru recidivy.

Příkladem takovéhoto úkonu může být vizualizace z aplikace v 1.fázi níže.

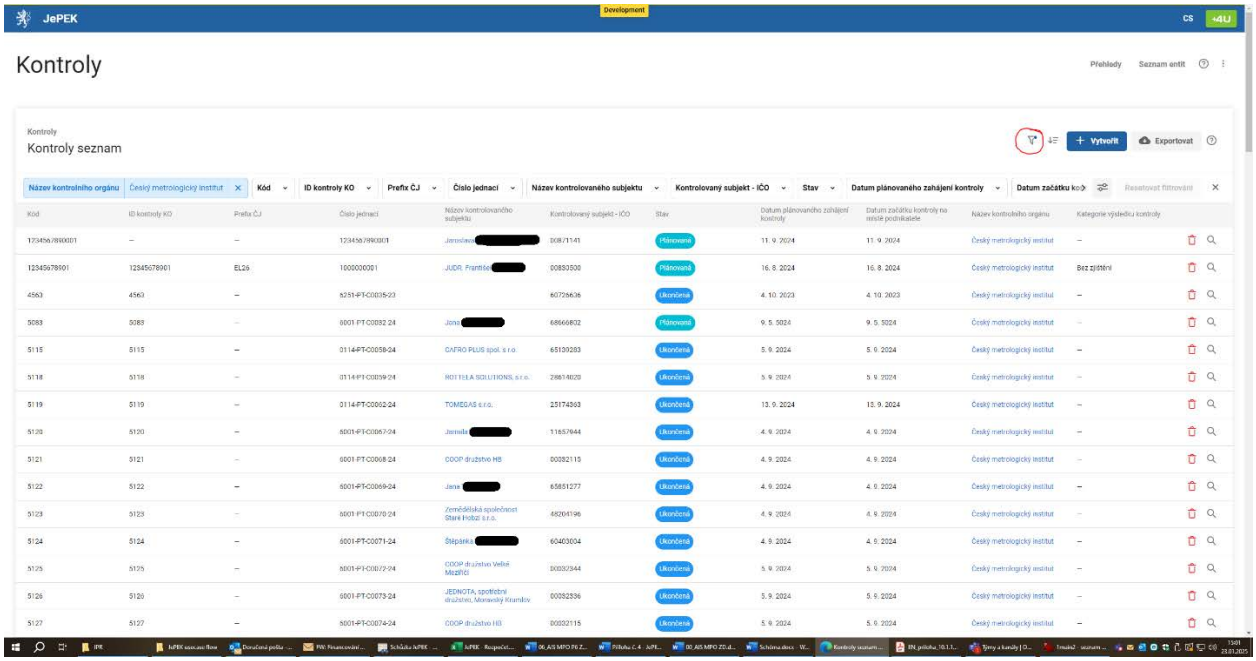
Stisknutím ikony Vyhledat kontrolu se úředník dostane na obrazovku Kontroly seznam, kde může filtrovat, řadit a hledat jednotlivé kontroly dle názvu kontrolovaného subjektu nebo kontrolního orgánu, a může si také zobrazit detaily o obou subjektech, především pak detail vyhledané kontroly.

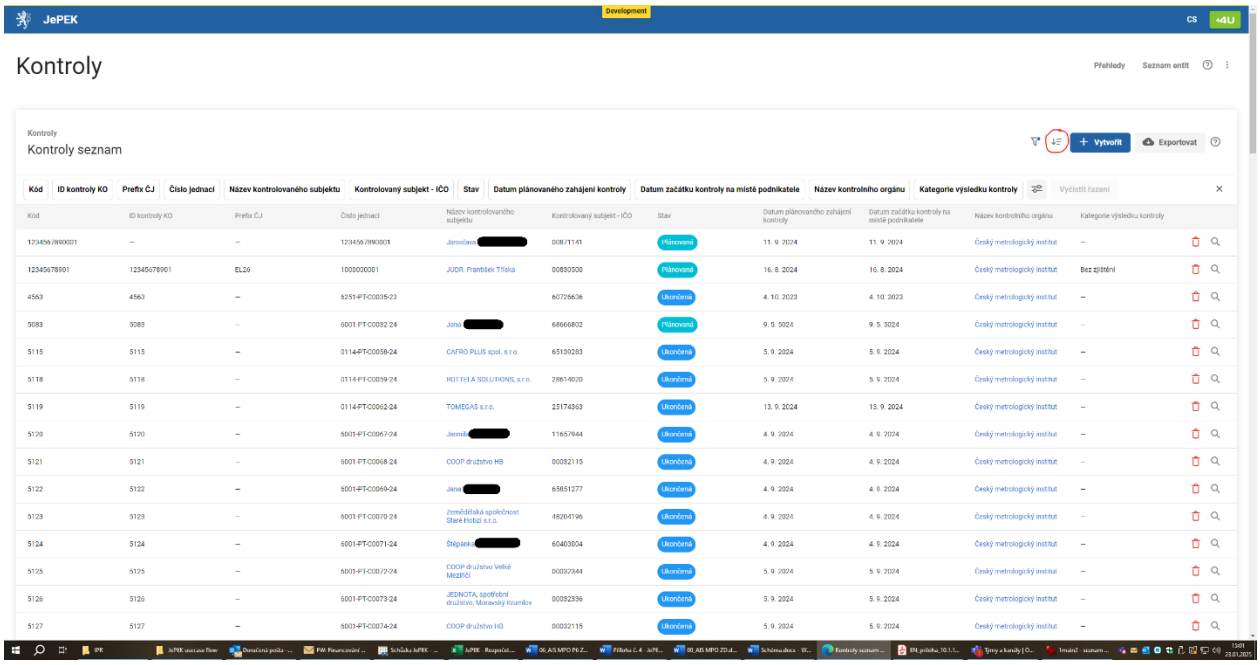


Přechod na „Vyhledat kontrolu“ z obrazovky Přehledy:



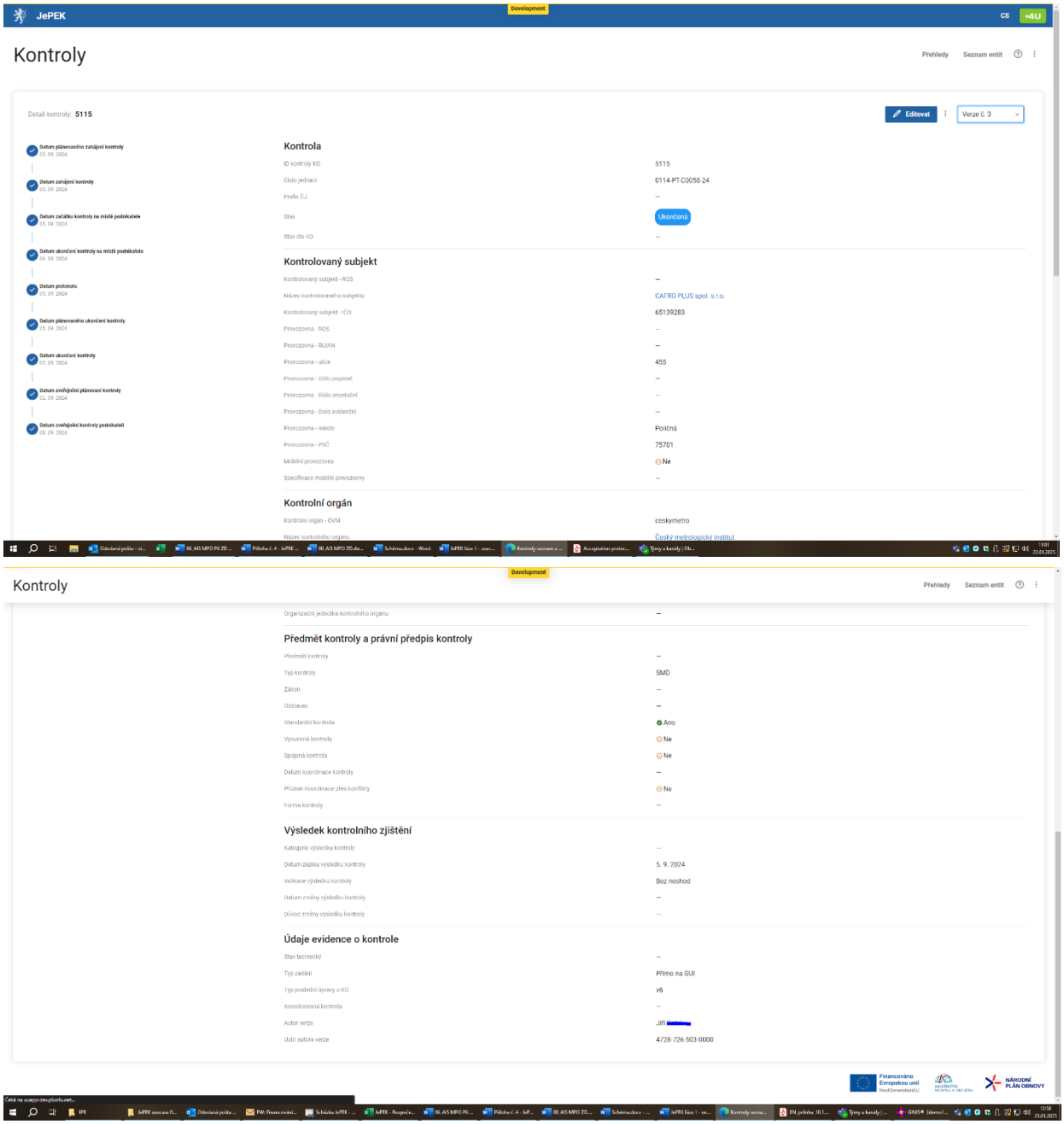
Zobrazení filtrů a řazení:



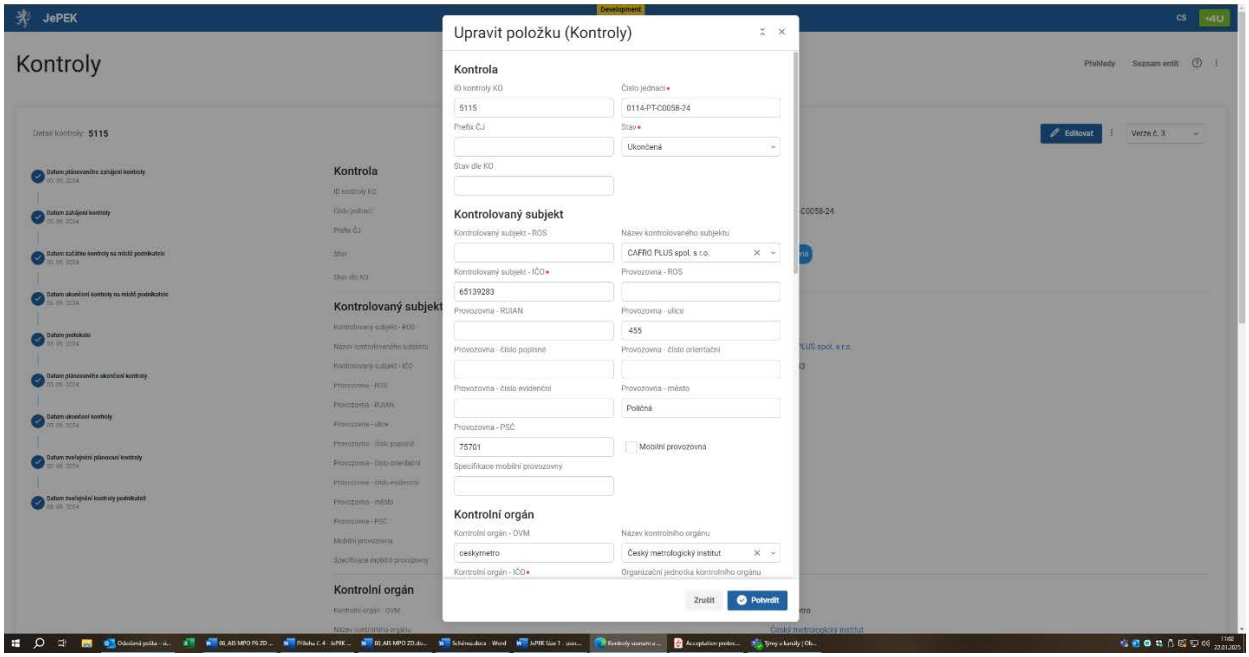


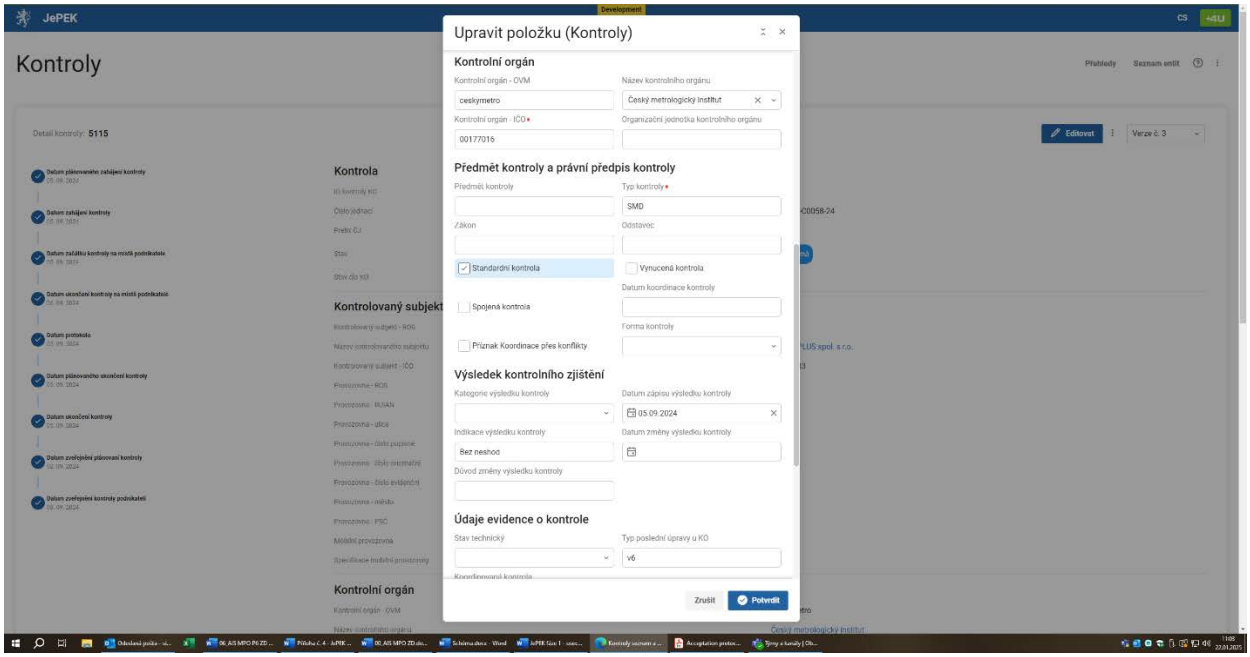
Přechod na detail kontroly stisknutím tlačítka lupy vpravo:

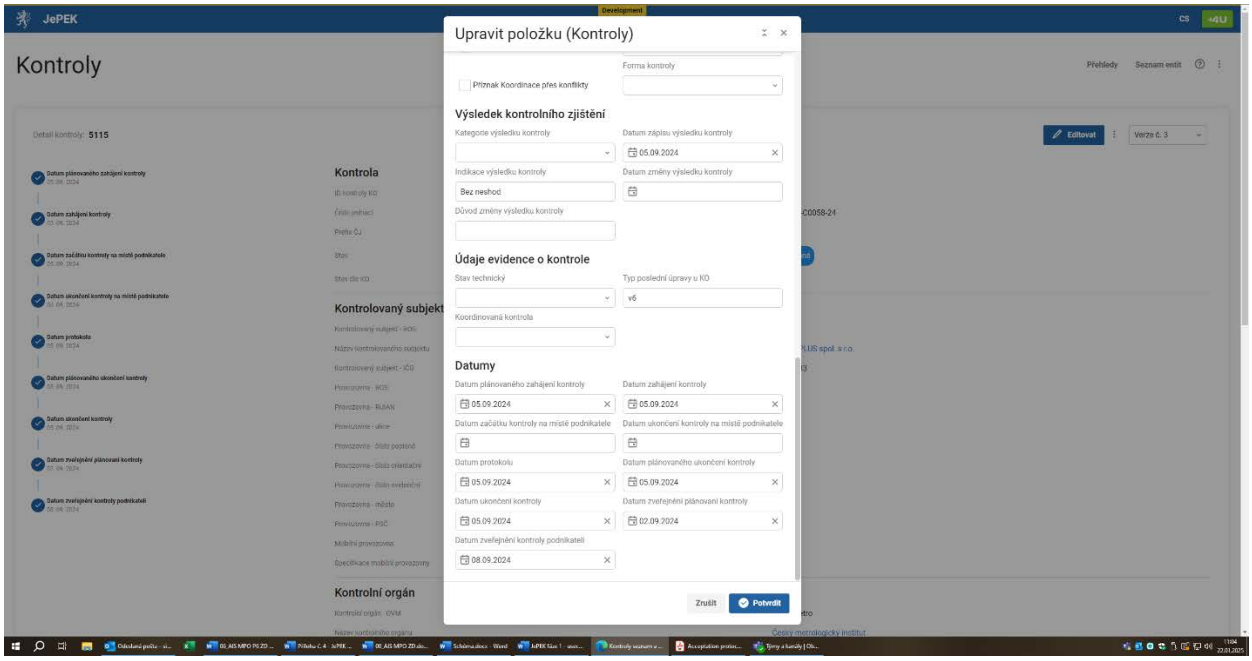
Na detailu kontroly lze vidět stav kontroly, kontrolu editovat, či nahlížet na její verze.



Přechod na editaci kontroly stisknutím tlačítka „Editovat“

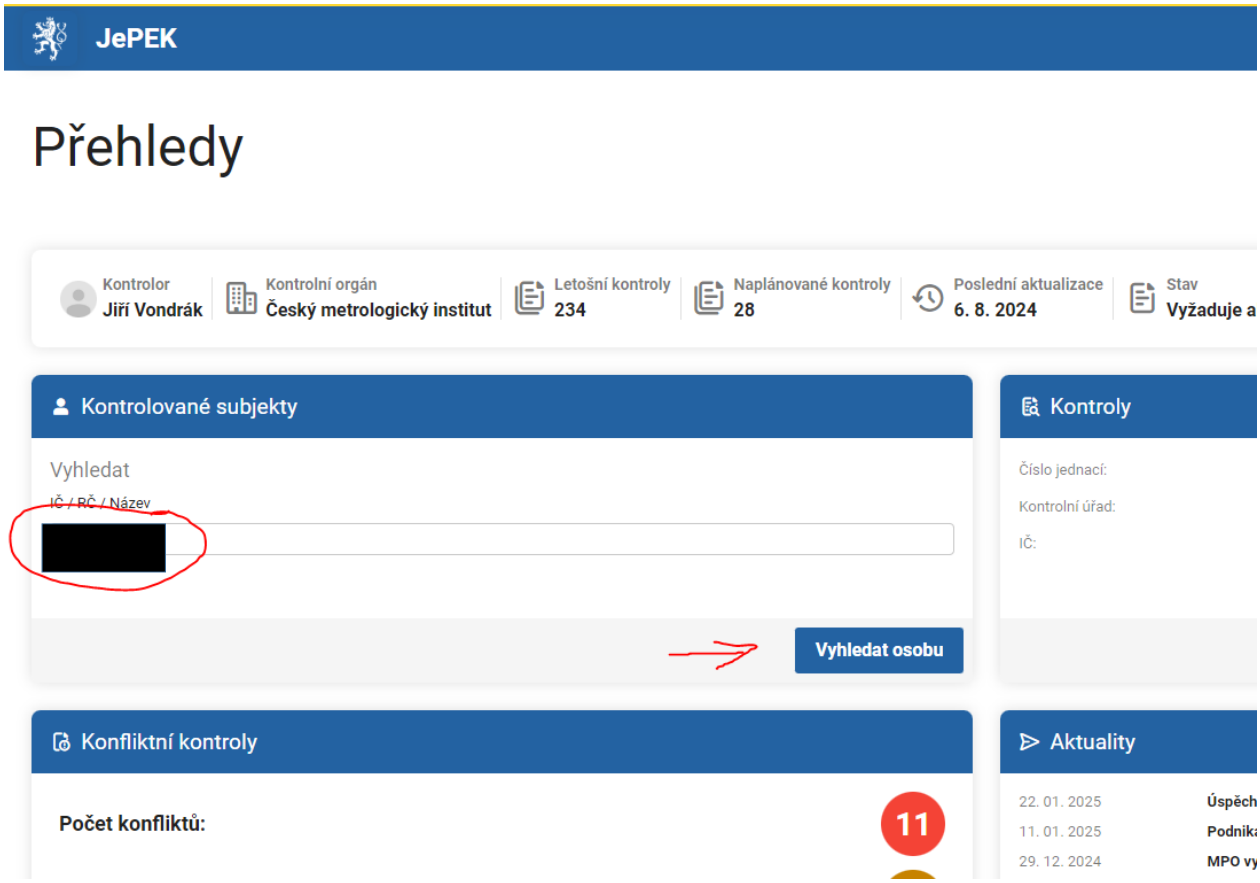

JePEK
Kontroly
Upravit položku (Kontroly)
Kontrola
Kontrolovaný subjekt
Kontrolní orgán
Zrušit
Potvrdit

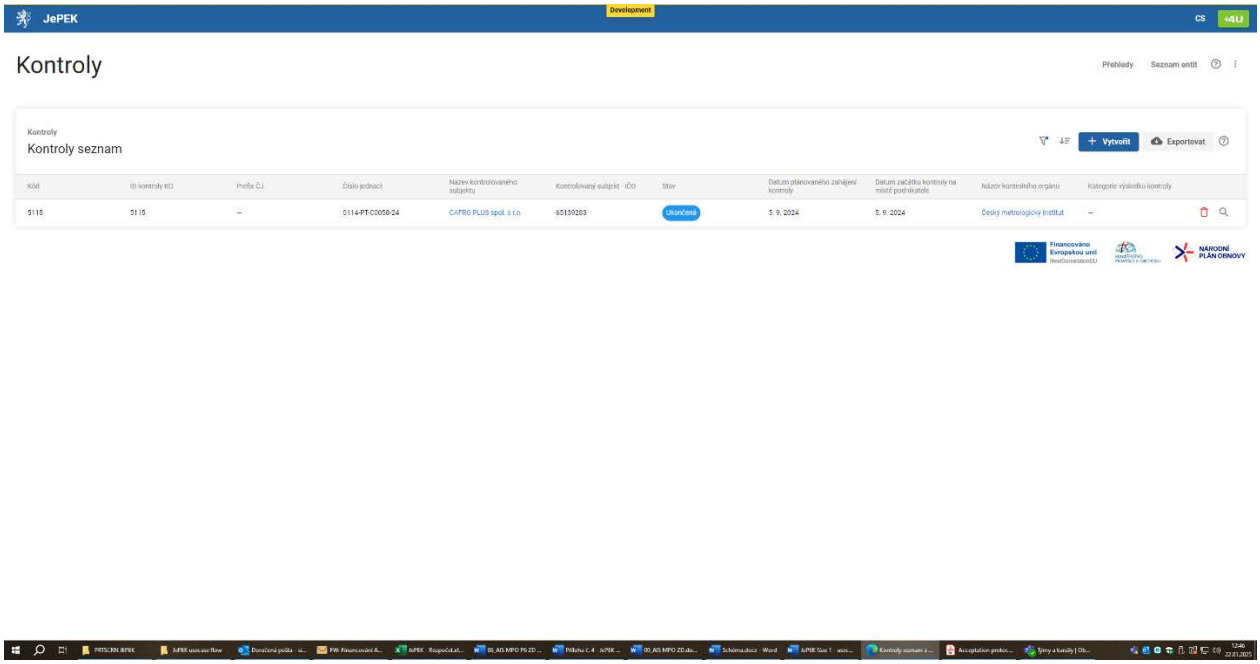

JePEK
Kontroly
Upravit položku (Kontroly)
Kontrolní orgán
Předmět kontroly a právní předpis kontroly
Výsledek kontrolního zjištění
Údaje evidence o kontrole
Zrušit
Potvrdit



Vyhledání kontroly na základě IČO, RČ, Název, případně jiný klíčových parametrů

Zadáním jednoho z parametrů lze rychle vyhledat specifický subjekt, a efektivně zobrazit kontroly a jejich stav.





Rozpad Usecases:

Uživatel - úředník				
	BUC	M		Zadání jména a hesla (pro případ nemožnosti autentizace nebo pro případ servisního přístupu)
	UC	S		Převedení na přihlášení vůči NIA
	SUC	M		Načtení/zpracování informací od NIA nebo jinak (zpracování tokenu, donačtení jména a dalších informací, Idčka, rolí, seznam organizací atp)
	SUC	M		Zpracování informace o poskytnutí souhlasu s poskytnutím údajů (jednorázově, trvale)
	SUC	L		Převzetí identifikace pro přihlášení a také informací pro ztotožnění v REZA nebo jinde.
	BUC	S		Odhlášení
	SUC	S		Auditní log přihlášení odhlášení
	SUC	M		SSO pro úředníky
	INTG	L		Integrační scénář komunikace na CAAIS
	SUC	S		Převzetí autorizace a přičlenění ke KO nebo MPO a další sady informací o přihlášeném uživateli
	BUC	S		Obrazovka: Neautorizováno

	BUC	S		Obrazovka odhlášeno
	SUC	M		Napočtení základních statistik pro zobrazení na portálu
	BUC	M		Základní portál/obrazovka/menu, které se zobrazí ihned po přihlášení/SSO - Dashboard

Kontrolní úřad				
	SUC	M		Verifikace souladu kontrolních orgánů (číselník kontrolních orgánů vs konfigurace vs data od CAAIS u přihlášeného uživatele)
	BUC	S		Zadání vyhledávacích kritérií pro vyhledání kontrolního orgánu
	BUC	M		Vyhledání a zobrazení výsledků hledání na částečnou shodu (filtrování, řazení)
	BUC	S		Zobrazení obecného přehledu kontrolních úřadů (filtrování, řazení)
	BUC	M		Zobrazení detailu a kontaktů kontrolního orgánu
	BUC	M		Konfigurace vazby eSbirky a účelu kontroly společně s deeplinkem na Databázi informačních povinností
	BUC	M		Zobrazení kontrol pro kontrolní úřad s filtrováním na organizační složky (textově)
	BUC	M		Zobrazení kontrol pro kontrolní úřad s filtrováním na organizační složky (Kalendářové zobrazení zoom-in)
	BUC	M		Zobrazení kontrol pro kontrolní úřad s filtrováním na organizační složky (kalendářové zobrazení zoom out)
	BUC	M		Zobrazení zjednonušených organizačních složek/útvarů kontrolního úřadu
	BUC	M		Konfigurace kontrolního úřadu (práva organizačních složek)
	BUC	M		Zobrazení organizační složky kontrolního úřadu
	BUC	M		Editace (nová, edit, smazání) organizační složky/útvaru

Zobrazení kalendáře kontrol				

	BUC	L		Zobrazení textového seznamu proběhlých kontrol
	BUC	L		Zobrazení textového plánu kontrol (budoucích) kontrol
	BUC	L		Zobrazení short range grafických proběhlých kontrol
	BUC	L		Zobrazení long range graficky proběhlých kontrol (heat mapa s výsledkem)
	BL	L		Business logika: Výpočty/nápočty statistik kontrol
	BUC	L		Dashboard: Zobrazení statistik kontrol (počty, podíly na udání, podíly OK/NOK, náprava, dle KO, Dle předmětu)
	SUC	M		Specifické datového úložiště pro Reportingový systém
	INTG	L		ETL-Export zjednodušeného datového modelu pro zpracování Reportingový systém, resp konfigurace databáze

Vyhledání a zobrazení kontrol				
	BUC	M		Vyhledání kontroly (číslo jednací, IČO, temíny pro kontrolu, termíny pro místní šetření …)
	BUC	M		Zobrazení hitlistu nalezených kontrol dle kritéria vyhledávání (řazení, stránkování)
	BL	M		Business logika: přístup ke kontrole (plánované nebo neuzavřené) - viditelnost (vše, jen KO, jen "blokace času")
	BL	M		Business logika: přístup ke kontrole, možnost editace dle uživatele
	BL	M		Business logika: Konfigurace typu kontroly (vlastnosti)
	BUC	L		Zobrazení detailu kontroly včetně místních šetření a došetření, úřadu, předmětu, typu, kontaktu na úředníka nebo úřad, čísla jednacího)
	BUC	S		Zadání důvodu pro zobrazení výsledku kontroly
	BL	L		Business logic: Konfigurace kontroly, které atributy jsou zobrazitelné pro můj úřad, policii …, pro ostatní KO, pro podnikatele

	BL	L		Business logika: Výpočet zjištění datové kvality ke kontrole
	BUC	M		Zobrazení historie kontroly (založena, modifikována, staré a nové údaje)
	SUC	M		Auditní logování přístupu a změn
	BL	M		Ověření práva editovat kontrolu a její atributy (na úřad nebo správce)
	BUC	L		Editace kontroly/Nová kontrola z ručního zadání
	BL			Konfigurace pravidel pro dopočet datumů kontroly
	BL			Realizace výpočtu/dopočtu datumových údajů na kontrole a úkonech kontroly
	BUC	S		Editace více úkonů/místních šetření na bázi jedné kontroly

Podání				
	BUC	M		Podání-Nahrání (výběr a potvrzení) excelu s kontrolami, formální kontrola na název a datumy a strukturu
	BUC	S		Přehled nahrávání/podání
	BUC	S		Zobrazení detailu Podání - pokud je relevantní, informace z stavu zpracování podání
	BUC	M		Zobrazení chybového protokolu u konkrétního podání
	BUC	S		Zobrazení historického datového souboru podání
	SUC	M		Uložení excelu s kontrolami pro asynchronní zracování a příladnou pozdější kontrolu nebo verifikaci
	SUC	M		Asynchronní zpracování excelu s kontrolami - aktualizace kontrol (včetně historizace a výpočtu zjištění na kontrolách)
	SUC	S		Vytvoření protokolu chyb (či potvrzení správnosti) pro zpětnou notifikaci
	SUC	S		Odeslání protokolu chyb nebo zobrazení protokolu chyb na přijatým excelem
	BUC	S		Zobrazení kontrol (mého úřadu, mé organizační složky) s nedostatečnou datovou kvalitou

Importy kontrol				

	INTG	L		Aktualizace záznamů finančních kontrol včetně organizační struktury úřadu
	SUC	L		Zpracování org struktury z finančních kontrol
	INTG	L		Aktualizace záznamů evropských kontrol včetně organizační struktury úřadů
	SUC	L		Zpracování org struktury z evroských kontrol
	SUC	M		Zpracování informace o finančních kontrolách (bez výpočtu zjištění, bez notifikací)
	SUC	M		Zpracování informace o evropských kontrolách (bez výpočtu zjištění, bez notifikací)

Plánování kontrol				
	BUC	M		Zobrazení a zpracování Informace o konfliktu
	SUC	M		Výpočet konfliktu ukládané kontroly
	INTG	L		Online služba pro plánování kontrol(verifikaci kontrol a změny kontrol

Kontrolní úřad funkčnosti pro úředníka				
	BUC	M		Zobrazení zjištění datové kvality
	BUC	M		Zobrazení historie
	BUC	M		Zobrazení posledních změn dle oprávnění (úřad nebo organizační jednotka)
	BUC	M		Zobrazení nálezů koordinace kontrol

5.2.5. Subtypy uživatelů typu Úředník

Dle doporučení v rámci https://www.czechpoint.cz/data/prirucky/files/prihlasovani_OTP.pdf a v souvislosti se zaváděním NIS2 je potřeba vytvořit vhodné přístupy pro následující typy uživatelů:

a) Administrátor řízení pro možnost realizace úprav i v případě odstávek jiných systémů nebo nějaké nestabilitě/nefunkčnosti nástrojů mimo správu MPO i v rámci MPO,
b) Lokální administrátor využívající Autenticitu potvrzenou v rámci MPO, k vybraným administrativním zásahům do systému,
c) Běžný uživatel úředník autentizovaný systémem CAAIS (pokud nebude systém CAAIS ve stádiu produkční zralosti, pak autentizovaný systémem JIP/KAAS), a to v různých rolích,
d) ... pro úplnost zbývá doplnit, že systémy jsou autentizovány systémovými uživateli a příslušnými certifikáty.

Pro přihlášení běžným uživatelem—úředníkem je pak vyžadováno – buď certifikát, nebo OTP (nestačí pouze jméno a heslo).

5.2.6. Veřejnost

Jelikož je projekt realizován orgánem veřejné správy, je relevantní cílovou skupinou i široká veřejnost. Ve vztahu k veřejnosti je nutné brát především v potaz problematiku poskytování informací o výkonu veřejné služby. Ta je ve vztahu ke kontrolní činnosti jednak upravena v obecné rovině samotným kontrolním řádem (§ 26) a dále existuje legislativní ukotvení práva na informace (dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů).

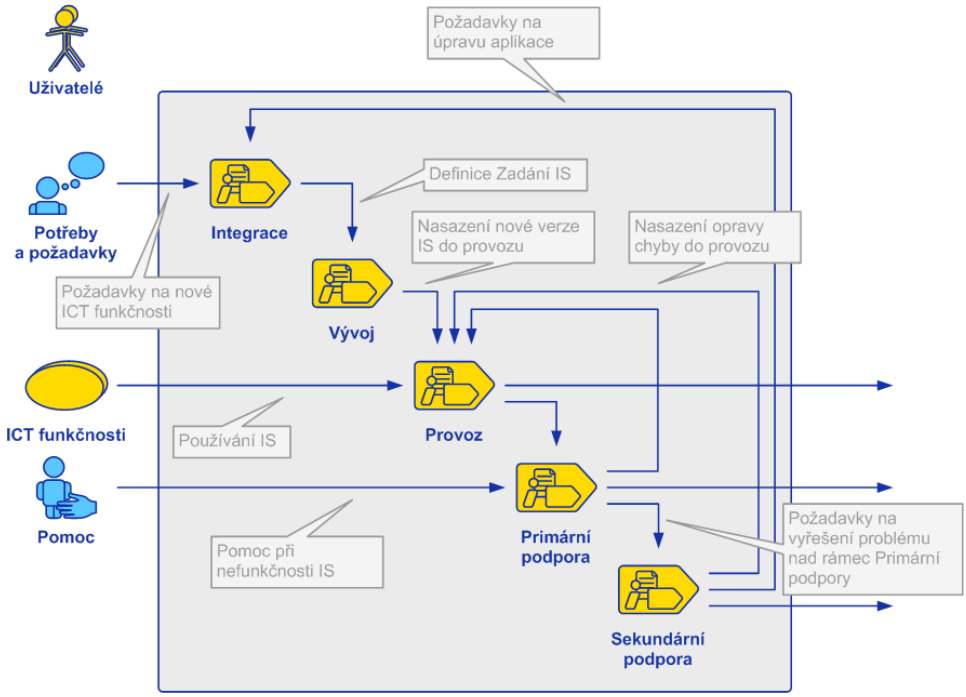
Veřejnost bude moci přistupovat k vybraným informacím v rámci systému JePEK na základě výstupů JePEK zpřístupněných pomocí státního systému pro poskytování Open Data, kam budou vybraná data ze systému JePEK poskytována.

5.2.7. MPO Reprezentant

MPO jako správce systému JePEK bude pracovat s informacemi o používání systému JePEK, a to nad rámec dat poskytovaných v rámci Open Data. MPO reprezentant bude využívat systémová data pomocí nástrojů v rámci infrastruktury MPO. Pro statistická zpracování bude použit specializovaný reportingový systém.

5.2.8. Business support/administrace

Systém JePEK bude podporován týmem business i IT pracovníků z MPO tak, aby se zajistil správný a korektní běh a rozvoj systému. Pro výkon části business suport úkonů bude použita administrační konsole. Pracovníci budou zajišťovat ve spolupráci s interními či externími IT útvary procesy péče o informační systém (Business provoz systému, IT provoz systému, Preventivní, adaptační a korektivní maintenance, Podporu a školení uživatelů, Systémovou integraci).



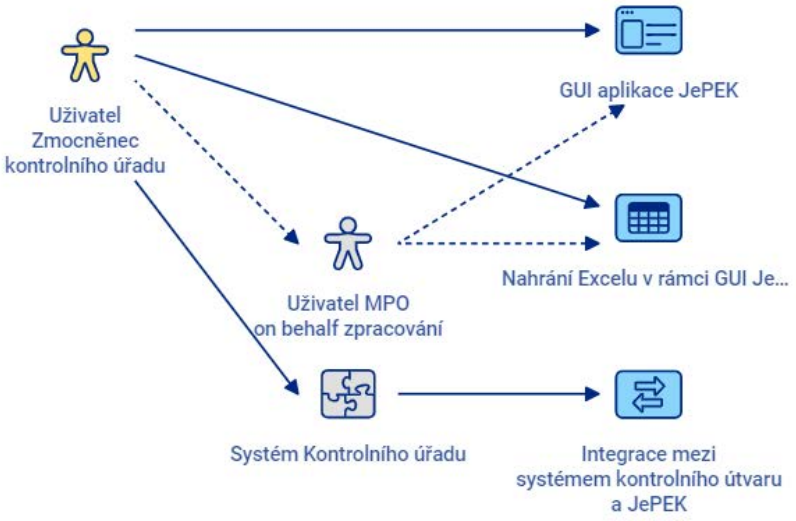
Obecně platí, že pro informační systém je potřeba zajistit:

1. aby byl informační systém funkční, dostupný a připravený k použití. To lze zajistit pomocí týmu IT a business specialistů,
2. pomoc uživateli ve chvíli, kdy si neví rady, nemůže pokračovat nebo potřebuje jinou pomoc,
3. aby nové požadavky, přizpůsobení změnám okolí a podobně byly vyhodnoceny, prioritizovány, a následně realizovány v nových verzích systému nebo jako korektivní či adaptivní údržba.

5.3. Způsoby práce Reprezentanta kontrolního orgánu

Reprezentant kontrolního orgánu bude moci pracovat se systémem vícekanálovým (omnichannel) způsobem, kdy povolené kanály jsou:

- Práce v systému JePEK napřímo s jednotlivými záznamy pomocí GUI JePEK (JePEK pro kontrolní orgány). Tento kanál se hodí pro malé počty kontrol pro kontrolní úřad/organizační útvar, za který je zmocněnec odpovědný, a dále pro situace oprav či změn individuálních záznamů. GUI kanál je dále vhodný pro nespecifikovaná prohlížení a analýzy v rámci kontrolního útvaru.
- Práce s excelem obsahujícím záznamy o kontrolách a tento excel nahrávat pomocí speciálních funkčností na GUI. Tento kanál je vhodný pro situace, kdy se pracuje až s tisíci záznamy kontrol za období, nebo pokud kontrolní úřad vede evidence v excelu nebo v informačním systému, který ale nechce na systém JePEK přímo integrovat, ale například pracovat formou exportu a importu.
- Vlastní informační systém kontrolního úřadu, který je ale integrován na systém JePEK a dochází k automatické výměně dat s tím, že míra integrace může být různá. Systém JePEK bude poskytovat několik webových metod, z nichž některé nemusí kontrolní úřad integrovat do svého informačního systému a využít v tom, jak plánuje, aktualizuje, zobrazuje a zveřejňuje informace o kontrolách.



Uživatel nebude omezen v maximální frekvenci užití systému, tedy může jej používat nepřetržitě (kromě avizovaných odstávek a případných neplánovaných odstávek). Naopak minimální požadovaná frekvence použití bude domluvena v rámci konfigurace přistoupení kontrolního orgánu k systému JePEK. Pokud nebude splněna minimální frekvence aktualizace dat kontrolního orgánu (editaci může provést jakýkoliv pracovník, tedy nebude záležet na tom, kdo konkrétně editaci provede), pak budou vybraní pracovníci upozorněni, že k minimální frekvenci editace nedošlo. K editaci budou moci pracovníci použít jakýkoliv kanál, a tedy do výpočtu frekvence užití budou vstupovat kterýmkoliv kanálem. (JePEK nebude zohledňovat míru editace či počet editovaných kontrol v rámci jednoho editačního zásahu.)

5.4. Procesy svázané se systémem JePEK

Systém JePEK bude podporovat procesy práce s evidencí a koordinací kontrol, zveřejnění historie kontrol a také další související (sub) procesy, které umožňují správnou funkci systému, poskytování informací a provozní procesy.

5.5. BPP01 Proces přihlášení podnikatele

Proces má za cíl přihlásit podnikatele jako fyzickou osobu do systému JePEK a zpřístupnit mu právě jen ty informace, které jsou určeny pro podnikatele a firmy, ke kterým je oprávněn sledovat informace o kontrolách (plánované kontroly, které lze sdělit podnikateli, aniž by byl zmařen účel kontroly, historické výsledky kontrol).

5.5.1. Základní kroky procesu:

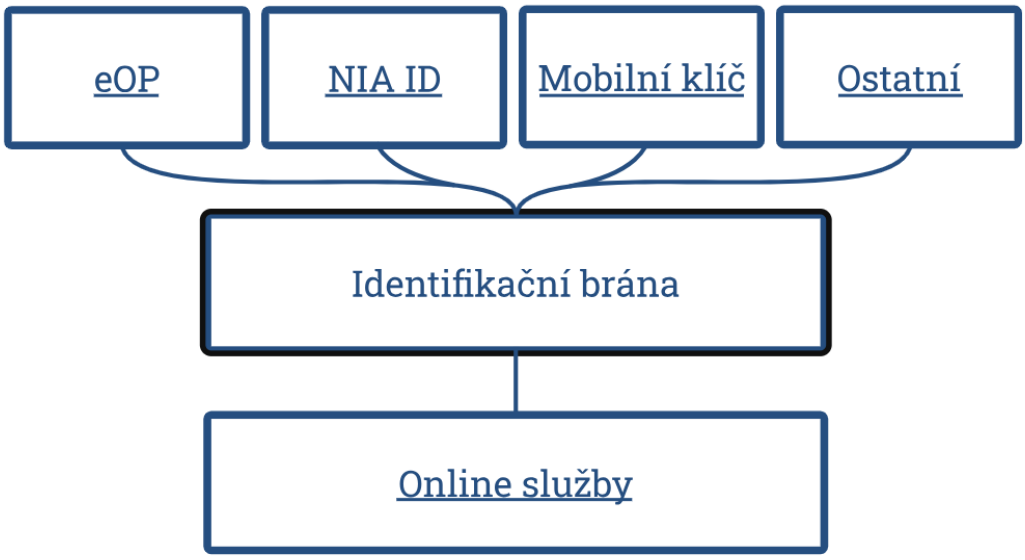
1. Impulz k přihlášení v JePEK, výběr autentizační metody
2. Autentizace prostřednictvím NIA
3. Alternativně autentizace prostřednictvím datových schránek
4. Zjištění zastoupených osob
5. Zjištění firem, u kterých je uživatel oprávněn nahlížet na data o kontrolách

5.5.2. Impulz k přihlášení, Výběr metody

Nepojmenovaný uživatel si na webové stránce pro JePEK vybere přihlášení a následně vybere autentizační metodu, kterou chce použít.

5.5.3. Podnikatel se přihlašuje pomocí NIA

Přihlášení podnikatele bude probíhat jednou z následujících možností:



5.5.4. Přihlášení pomocí datové schránky

Přihlášení pomocí datové schránky je realizováno formou přesměrování na přihlašovací stránku a následného převzetí tokenu.

Detaily pro krok 2 a krok 3 jsou popsány v dokumentu

https://info.identitaobcana.cz/download/SeP_PriruckaKvalifikovanehoPoskytovatele.pdf

5.5.5. Zjištění zastoupených osob

Systém JePEK se on-line dotáže na identifikaci přihlášené osoby jako zplnomocněné osoby do systému REZA na defaultní šablony plných mocí a na specifickou plnou moc pro JePEK. Pokud v systému REZA nějaké takové plné moci existují, jejich seznam pak systém JePEK použije pro nalezení či vyhodnocení firem, kam má uživatel přístup.

Pro každou z plných mocí systém vyhodnotí zplnomocňující osobu (fyzickou i právnickou). Pro fyzické osoby bude dále systém hledat implicitní plné moci k právnickým osobám v REZA a také členství v kolektivních orgánech i jednočlenných statutárních orgánech právnických osob.

Pro příslušné právnické osoby zajistí zpřístupnění dat o kontrolách viz dále.

5.6. BPP02 Proces Zobrazení kontrol

Cílem procesu je zjištění firem, kde je uživatel oprávněn vidět kontroly, a zobrazení kontrol u těchto firem.

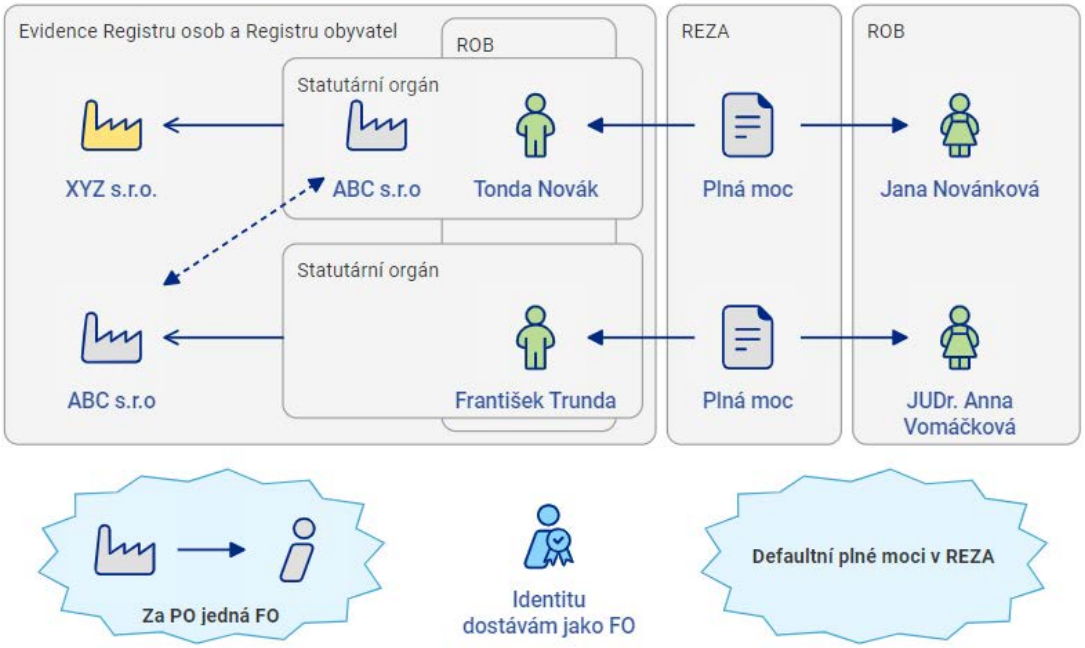
Systém pro identifikovanou osobu a všechny zastoupené fyzické osoby na základě platných plných mocí systematizovaných v REZA zjistí přístup k firmám pomocí služby https://www.szrcr.cz/images/dokumenty/v%C3%BDvoj%C3%A1%C5%99i/detailn%C3%AD_popisy_eGon_slu%C5%BEeb/SZR_popis_eGON_sluz%CC%8Ceb_E259_rosCtiPodleUdaju2.pdf s tím, že budou vybrány vhodné role / angažmá v konkrétních firmách.

Systém pak načte pro každou identifikovanou osobu jejich případné informace k fyzické osobě podnikateli pomocí https://www.szrcr.cz/images/dokumenty/v%C3%BDvoj%C3%A1%C5%99i/detailn%C3%AD_popisy_eGon_slu%C5%BEeb/SZR_popis_eGON_sluzeb_E257_rosCtiAifo2.pdf

Dále systém vyvolá služby pro každou zjištěnou právnickou osobu tak, aby byl sestaven celý strom vztahů (členů statutárních orgánů). Služby bude volat kde potřeby ve více situacích dle požadavků jednotlivých usecases.

1. Služba **„zjištění oprávnění fyzické osoby podle různých údajů, za které právnické osoby může jednat“**: eGON služba **rosCtiPodleUdaju2,**
2. Služba **„zjištění fyzických osob oprávněných jednat za právnickou osobu“**: eGON služba **rosCtiIco2,**
3. Služba **„zjištění oprávnění fyzické osoby podle jejího identifikátoru, za které právnické osoby může jednat“:** eGON služba **rosCtiAifo,**
4. Služba **„zákonní zástupci fyzické osoby – detailní informace“:** eGON služba **aiseoCtiAifo,**
5. Budoucí služba REZA pro načtení implicitních i explicitních plných mocí, bude doplněno, až bude služba skutečně zveřejněna.

Možný stav viz ilustrace.



Tím je vymezen seznam právnických osob a případně fyzických osob podnikatelů, ke kterým je přihlášený uživatel oprávněn vidět informace o kontrolách.

Pokud není uživatel oprávněn prohlížet žádnou firmu, systém mu zobrazí webovou stránku s vysvětlením účelu JePEK, principu zobrazení firem a doporučí mu buď zaevidovat plnou moc v REZA, nebo se obrátit na Business Helpdesk systému v případě, kdy má pocit, že informace nejsou v korektním stavu (což je možné).

Systém dále umožní uživateli vyhledat firmu a pokusit se tuto firmu zobrazit (řešení je určeno pro situaci, kdy nejsou podle všech údajů data k dispozici, systém zkusí provolat příslušnou firmu a identifikovat uživatele jako člena statutárního orgánu pomocí data narození, jména a příjmení a data narození nebo jiných vhodných údajů pro situace, kdy by nebylo přesné dohledání od identity uživatele (uplatní se pro případy cizinců, změn jmen nebo alternativních transkripcí).

Systém bude běžně pracovat s cachovanou informací pro urychlení běhu. Přístup k firmám nebude vyhodnocován při každém dotazu, a proto je potřeba předpočítat identity, které mají mít k té které firmě přístup.

Zobrazení kontrol bude pak pro každou firmu separátní na základě výběru firmy, pro kterou chce uživatel vidět kontroly.

5.7. BPP03 Zplnomocnění, stažení plné moci

Cílem procesu je zajistit zplnomocnění jiné osoby podnikatelem a ukončení takového zplnomocnění.

Práce s plnými mocemi bude probíhat v systému REZA, se kterým bude systém JePEK integrován.

Systém bude využívat tzv. Zákonné plné moci, které budou odpovídat zákonným zástupcům fyzické osoby, která je přihlášena. Zákonné plné moci uchovává systém REZA a jsou v něm automaticky udržovány v aktuální podobě na základě informací ze státních registrů a evidencí.

Dále systém JePEK bude využívat implicitní plné moci vzniklé na základě zápisu do veřejných rejstříků (například prokury) z REZA podle toho, jak budou k dispozici v okamžiku realizace systému.

Vlastní plné moci pro systém JePEK buď zadá do systému REZA (až bude zveřejněn) pro své zástupce elektronicky sám podnikatel, a to přihlášením se státní identitou do systému REZA a vystavením šablony zastoupení pro systém JePEK pro jinou osobu.

Pokud v návaznosti na systém JePEK doručí podnikatel na MPO (vhodné kontaktní místo bude stanoveno v průběhu projektu) osobně, nebo úředně potvrzenou plnou moc na MPO doručí jiná osoba (způsoby budou upřesněny v průběhu projektu), pak pracovník MPO zadá do systému REZA příslušnou plnou moc on-behalf způsobem.

Ukončení platnosti plné moci (pokud není stanoveno předem přímo na plné moci, a tedy proběhne automaticky) bude probíhat obdobně, tedy s použitím systému REZA napřímo, nebo on-behalf způsobem.

Poznámka: případné automatické ukončení na základě externí události (typu úmrtí zastoupené osoby) se provede automaticky v systému REZA na základě propojení základních registrů.

5.8. BPK01 Proces přihlášení reprezentanta kontrolního orgánu

Proces má za cíl přihlásit do systému JePEK reprezentanty kontrolních orgánů, respektive úředníky obecně.

5.8.1. Přihlašování uživatelů - úředníků má typicky následující kroky:

- Autentizace (explicitní autentizace),
- Autorizace.

5.8.2. Autentizace

JePEK přesměruje neautentizované uživatele do CAAIS (https://rest-webauthenticationapplication.caais.gov.cz/login, respektive https://idp.caais.gov.cz/idp/svc/loginExternal/index).

Zde si uživatel vybere způsob přihlášení. Vybere-li si ověření prostřednictvím NIA, je přesměrován do NIA, kde si zvolí identifikační prostředek a jeho prostřednictvím prokáže svoji identitu, následně je přesměrován zpět do CAAIS. Pokud si uživatel vybere v CAAIS jinou autentizační metodu, zadá odpovídající přihlašovací údaje a CAAIS ověří jejich platnost v JIP. Ověřený uživatel je přesměrován zpět do AIS.

> Bližší informace: Popis webových služeb KAAS

(V době zpracování tohoto dokumentu nejsou k dispozici detailní rozhraní CAAIS, ale jen informace, že by měla být zpětně kompatibilní.)

5.8.3. Přihlášení varianty

CAAIS nabízí přihlášení jak variantou Identita občana, neboť každý úředník je zároveň občan, tak přihlášení přímo pomocí CAAIS, tedy jako úředník.

5.8.4. Autorizace

AIS odešle požadavek do autentizační služby CAAIS, která v odpovědi poskytne údaje o uživateli a jeho rolích a oprávněních. Na základě těchto informací systém určí, jaké možnosti bude uživatel mít.

Návrh autorizačních práv úředníků specificky pro JePEK bude:

- Čtení,
- Zakládání a změny kontrol za organizační útvar,
- Zakládání a změny kontrol za celý orgán veřejné moci,
- Role pro adresáty souhrnných notifikací.

Role se mohou ještě upřesnit v rámci detailní analýzy.

Ale systém nebude podporovat detailní členění práv, například dle právního předpisu nebo specifická práva na typy změn (příklad je operace Schválení plánu kontrol). Taková práva jsou přítomna v systémech některých kontrolních orgánů, a uživatelé tedy budou pracovat se systémy svých kontrolních orgánů, které budou na systém JePEK integrovány a změny pak propisovány pomocí integrace mezi systémy.

Struktura práv bude realizována dle principů Role Based Access Control (RBAC), který bude rozprostřen mezi CAAIS poskytující business role a aplikační role, a pak systém JePEK pracující s aplikačními oprávněními. Výchozí oprávnění je neautorizovaný uživatel.

5.8.5. Auditní log

Veškerá přihlášení a odhlášení úředníků do systému budou žurnálována a žurnály/logy budou uchovávány po zadanou dobu (očekáváme nastavení doby v jednotkách roků).

Řešení musí umožnit centrální logování provozních, systémových a bezpečnostních událostí ve formátu SYSLOG dle RFC5424, nebo v jiném formátu čitelném řešením SIEMu Objednatele. Pro logování cloudových komponent bude použito vhodné platformní řešení.

5.8.6. Zavedení uživatelů systému JePEK v CAAIS

Uživatelé budou v rámci projektu zavedeni do systému CAAIS, a to následujícími způsoby:

- **Přímo – pracovníky** MPO pro pracovníky MPO,
- **Delegovanou pravomocí** – pokud kontrolní orgány již používají nebo pro systém JePEK začnou používat systém CAAIS, pak určení pracovníci takových kontrolních orgánů budou spravovat uživatele vlastního úřadu v jejich přístupu a oprávněních pro systém JePEK. Na tyto vybrané uživatele bude delegována pravomoc od pracovníků MPO, kteří budou mít v gesci systém JePEK.
- **Zastoupením**: Pro ty kontrolní orgány, které nepracují se systémem CAAIS a ani s ním nechtějí začít pracovat, pak administrátoři MPO po dohodě s dotyčným kontrolním orgánem provedou zavedení a vybavení rolemi pro pracovníky kontrolního úřadu, kteří mají za kontrolní úřad systém JePEK používat. Tato možnost je pouze po dohodě mezi MPO a kontrolním úřadem a je podmíněna malým počtem pracovníků takového kontrolního úřadu.

5.8.7. Typová oprávnění

V rámci systému JePEK budou použity pouze standardní typy oprávnění – aplikační role. Nebude tedy běžné připravovat specifické role pro jednotlivé typy uživatelů z různých kontrolních úřadů. (Ale vytvoření struktury obchodních rolí, které se ale budou sestávat pouze ze stejných aplikačních rolí systému JePEK, bude možné dle funkčnosti systému CAAIS.)

5.9. BPK02 Dávková koordinace kontrol

Cílem projektu je dávkovým způsobem koordinovat, respektive zapsat kontroly do systému JePEK prostřednictvím importu excelu.

Uplatní se níže uvedené principy verzování, koordinace datumů, přepočtu datumů a podobně – viz příslušné kapitoly níže.

Viz dále BPK04 Koordinace kontroly.

Postup zpracování:

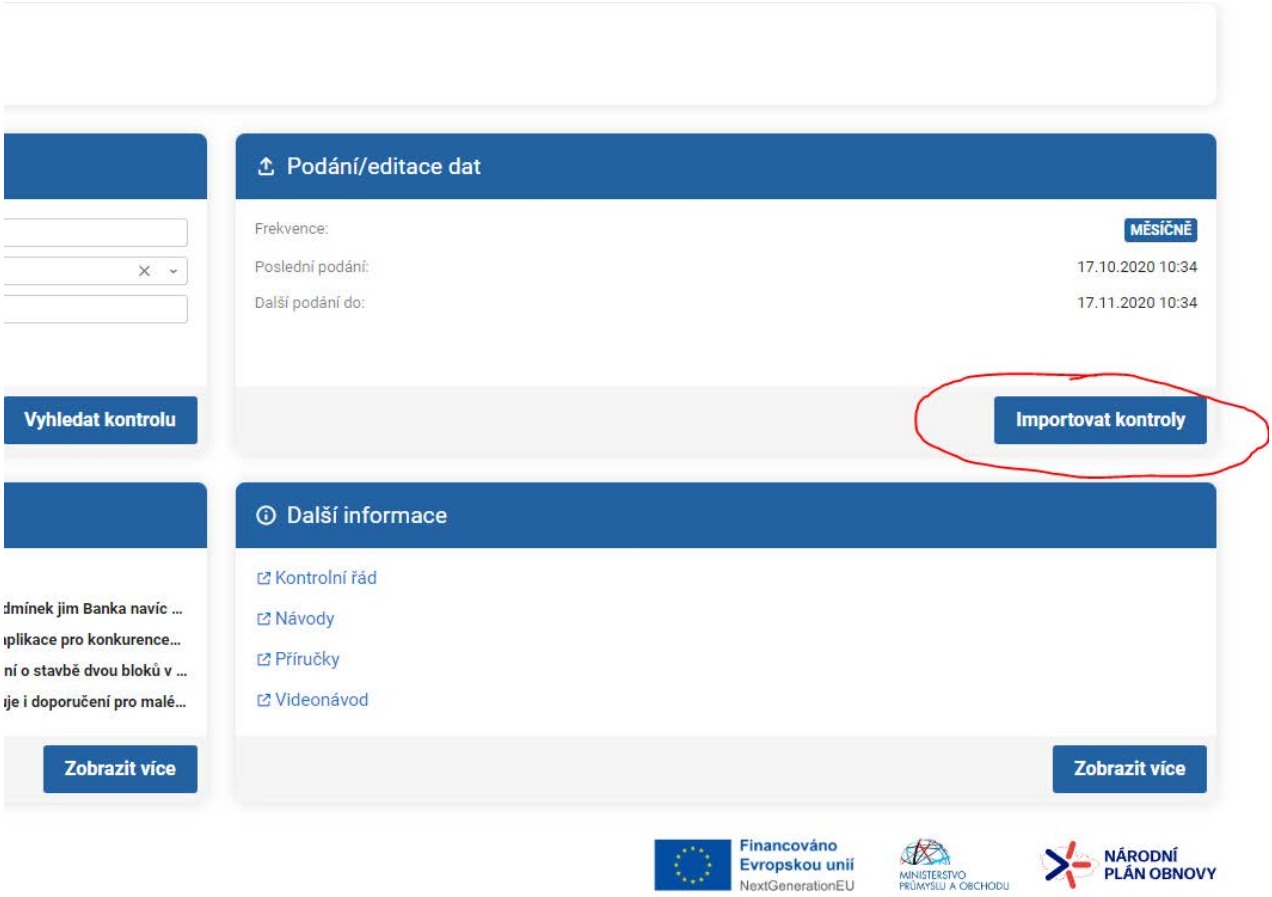
- Nejprve je ověřen soubor na strukturu, kódování a duplicitu zpracování,
- Soubor je technicky uložen jako celek do systému JePEK ve formě auditu,
- Každý věcný řádek z excelu bude zpracován:
  - Ověřena minimální sada informací ke kontrole:
    - identifikací kontroly (některý z identifikačních klíčů kontroly viz dále),
    - alespoň jeden z datumových údajů,
    - identifikací kontrolního orgánu,
    - identifikací kontrolovaného subjektu (nebo alespoň místo kontroly/kontrolované provozovny, pokud zjišťování identity kontrolovaného subjektu je teprve v procesu),
  - Identifikováním, zda se jedná o novou nebo aktualizaci existující kontroly,
  - Identifikováním, zda je potřeba provést koordinaci kontroly,
  - Provedením koordinace kontroly (výpočet a případná hlášení o nekoordinaci),
  - Kontrola je zaznamenána v nové verzi,
- Jsou vráceny informace o celkovém stavu zpracovávaného souboru.

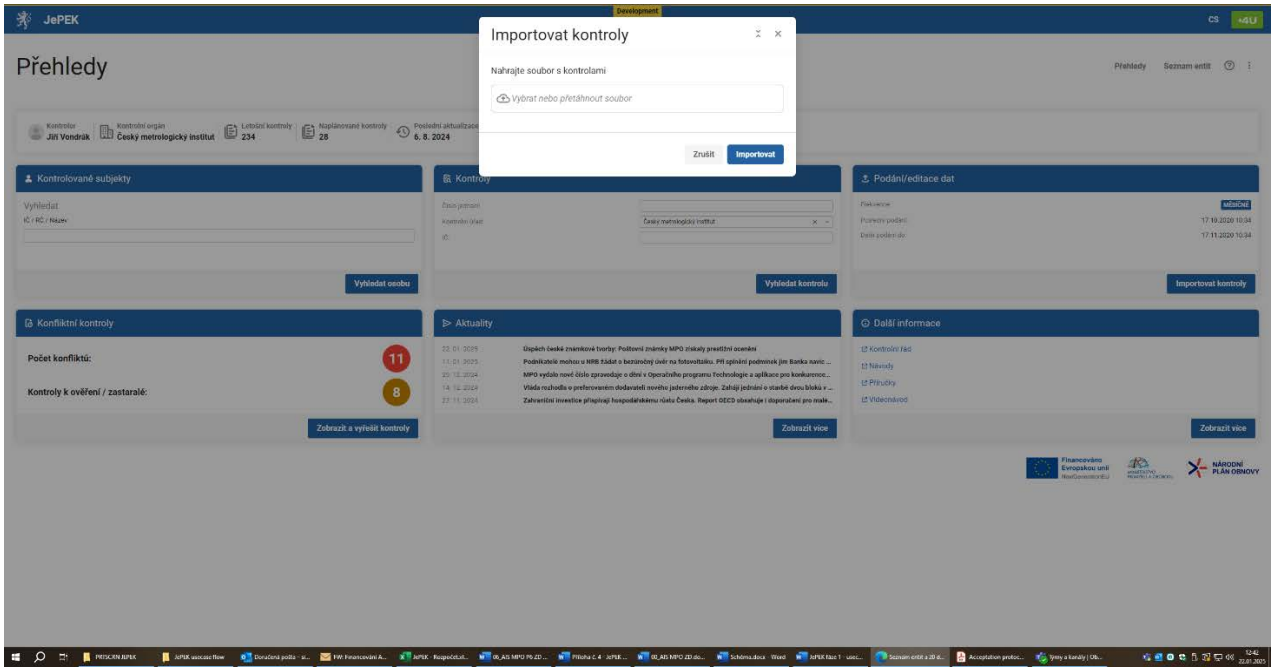
Návrh souboru pro import použitý v Aplikaci JePEK ve fázi 1: JePEK-Import_kontrol.xlsx

Kontrolní orgán bude zadávat pouze takové informace, které odpovídají jeho aktuální metodice. JePEK je designován tak, aby odpovídal široké praxi kontrolních orgánů od takových, které mají detailní evidenci ve svých systémech po takové, které vlastně pracují jen s velmi omezenými údaji.

Jelikož ne každý kontrolní orgán během výkonu kontrolní činnosti využívá či vůbec má dostupný vlastní informační systém, tak se řada kontrolních orgánů uchyluje k využití tabulek ve formátu .xls/.xlsx (excel). Těmto kontrolorům bude umožněno nahrát tabulky v domluveném formátu a v domluvené datové kvalitě přímo do systému JePEK, který nad jejich daty provede kontrolu datové kvality, a případně kontrolora upozorní na chyby v datové kvalitě, a

navede jej na problematickou buňku s žádostí o vyřešení. Při vstupu do systému bude také každá hodnota bezpečnostně ošetřena, aby vkládaná data nebyla rizikem pro informační systém.





5.10. BPK03 Management kontrol

Management kontrol má za cíl typicky zadat novou kontrolu (prostřednictvím GUI) do systému. Je tedy určen pro ty situace, kdy reprezentant kontrolního úřadu chce manuálně zadat novou nebo upravit stávající kontrolu svého kontrolního orgánu. Pracovník business podpory systému pak může upravovat kontroly dle požadavků. Všechny kontroly mají historii změn (pořízených jakýmkoliv způsobem).

5.10.1. Zobrazení kontroly

Uživatel má přístup ke kontrolám dle nastavení jejich viditelnosti z konfigurace typů kontrol (viz kapitola Principy viditelnosti kontrol).

K prohlížení může použít jak přístup přes Kontroly samé, tak přes Kontrolní úřad a zejména pak přes kontroly na Kontrolovaném subjektu. Systém bude umožňovat náhledy na kontroly ve všech těchto kontextech, kdy bude nabízet filtrování specifická k jednotlivým kontextům.

5.10.2. Zobrazení stavu kontroly

Systém JePEK bude rozlišovat zobrazení veřejného a technického stavu kontroly.

- Stav kontroly veřejný, ukazujeme jako Stav kontroly na GUI pro podnikatele i pro KO, odvozujeme z plynutí času a nastavení datumů na kontrole,
- Stav technický, který ukazujeme na GUI jen pro KO, odvozujeme i z hlášení KO, zejména pak od interních stavů kontroly, respektive od koordinace kontroly. Tento stav slouží zejména pro potřeby kontrolních orgánů a spojuje jejich interní stavy kontroly a také stavy datové kvality hlášení o kontrole.

5.10.3. Výpočet veřejného stavu kontroly

Systém JePEK vypočte veřejný stav kontroly dle následujících pravidel:

Stav kontroly veřejný	**Výpočet z datumů na kontrole a jejich porovnání s aktuálním datumem.**
Plánovaná	> (PlanovaneZahajeni (zadané i vypočtené) > dnes a zároveň není zadáno: > zahajení, a pokud je zadáno, pak je > dnes, > zacatekNaMiste, a pokud je zadáno, pak je > dnes, > ukonceniNaMiste, a pokud je zadáno, pak je > dnes, > protokol, a pokud je zadáno, pak je > dnes, > ukonceni, a pokud je zadáno, pak je > dnes.) nebo > (je zadáno zahajeni a zahajení je > dnes a není zadáno > ukonceniNaMiste, a pokud je zadáno, pak je > dnes, > protokol, a pokud je zadáno, pak je > dnes, > ukonceni, a pokud je zadáno, pak je > dnes.) nebo > (je zadáno zacatekNaMiste a zacatekNaMiste > dnes) a není zadáno > ukonceniNaMiste, a pokud je zadáno, pak je > dnes, > protokol, a pokud je zadáno, pak je > dnes, > ukonceni, a pokud je zadáno, pak je > dnes.)
Probíhající	> (Je zadáno zahájení a zahajeni (zadané) <= dnes a zároveň není zadáno > ukonceni, a pokud je zadáno, pak je >= dnes) nebo > (je zadán zacatekNaMiste(zadané) a zacatekNaMiste(zadané) <= dnes a zároveň není zadánoukonceni, a pokud je zadáno, pak je >= dnes)
Pravděpodobně probíhající	> planovaneZahajeni (zadané i vypočtené) <= dnes a zároveň planovaneUkonceni (zadané i vypočtené) >= dnes a zároveň není zadánozahajeni,zacatekNaMiste, a pokud je zadáno, pak je > dnes,ukonceniNaMiste, a pokud je zadáno, pak je > dnes,ukonceni, a pokud je zadáno, pak je > dnes,
Pravděpodobně ukončená	> planovaneUkonceni (zadané i vypočtené) < dnes a zároveň není zadáno ukonceni a zároveň pokud je zadáno zahájení, pak je zahajeni < dnes, a zároveň pokud je zadáno protokol, pak je protokol < dnes, a zároveň pokud je ukonceniNaMiste, pak je ukonceniNaMiste < dnes
Ukončená	> Je zadáno ukončení a ukončení < dnes
Pravděpodobně nezrealizovaná	> planovaneUkonceni (zadané i vypočtené) < dnes - X měsíců (parametrický údaj) a zároveň není zadáno:zahájení, zacatekNaMiste,ukonceniNaMiste,protokol, ukonceni.
Stav nejasný	> Jinak (také mohou být ty datumy zadané nějak nekonzistentně) > Například: Skutečné zahájení je > skutečné ukončení.

5.10.4. Výpočet technického stavu kontroly

Technický stav kontroly je odvozen z hlášení kontrolního úřadu (mapování stavu kontroly KO na unifikované stavy v JePEK).

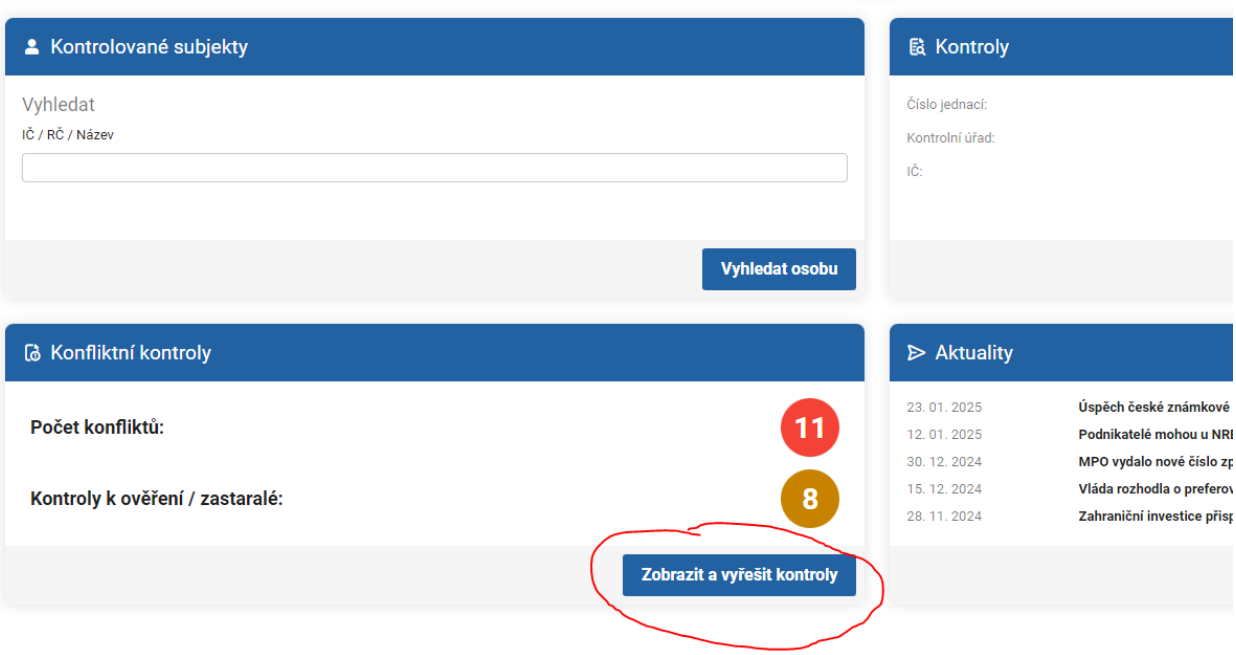
Typy hlášení kontrolního orgánu a vazba na tyto stavy budou v rámci konfigurace vytvořeny pro každý kontrolní orgán dle specifik tohoto kontrolního orgánu.

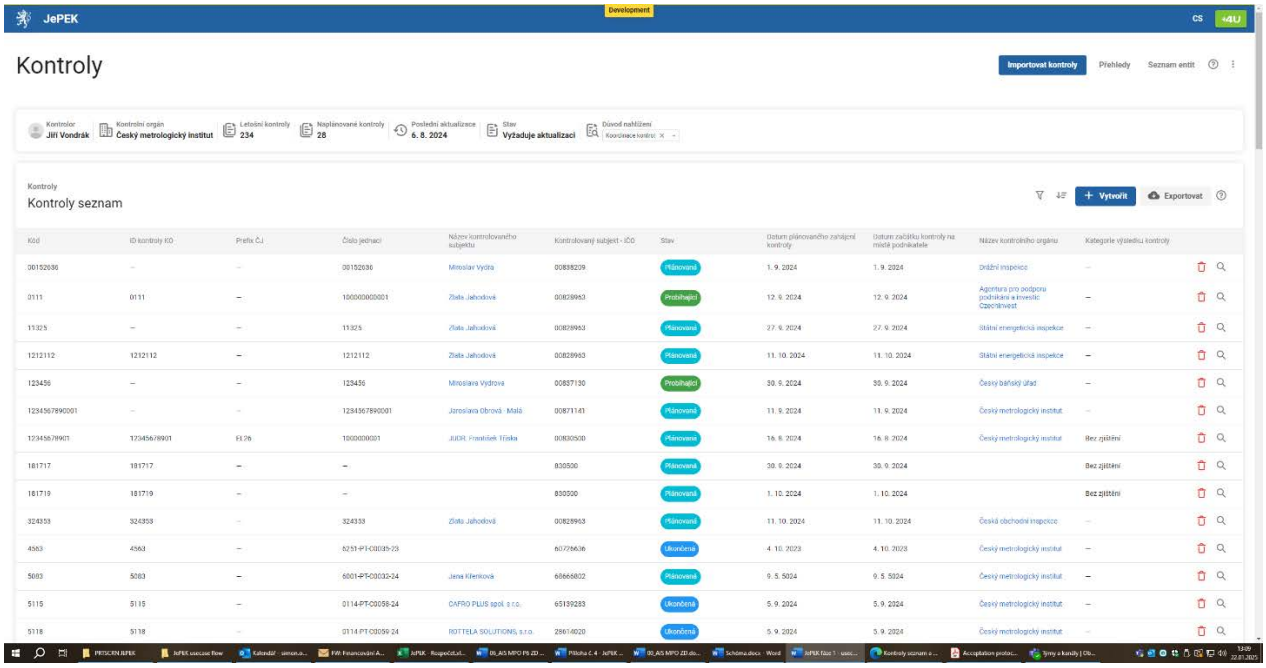
Nebude sledována žádná souslednost stavů, prostě to, co JePEK obdrží, respektive to, co bude zadáno z GUI, systém zobrazí.

JePEK přidává jen technický stav řešení konfliktů, pokud se kontrolní úřad nevyjádří k identifikovanému konfliktu.

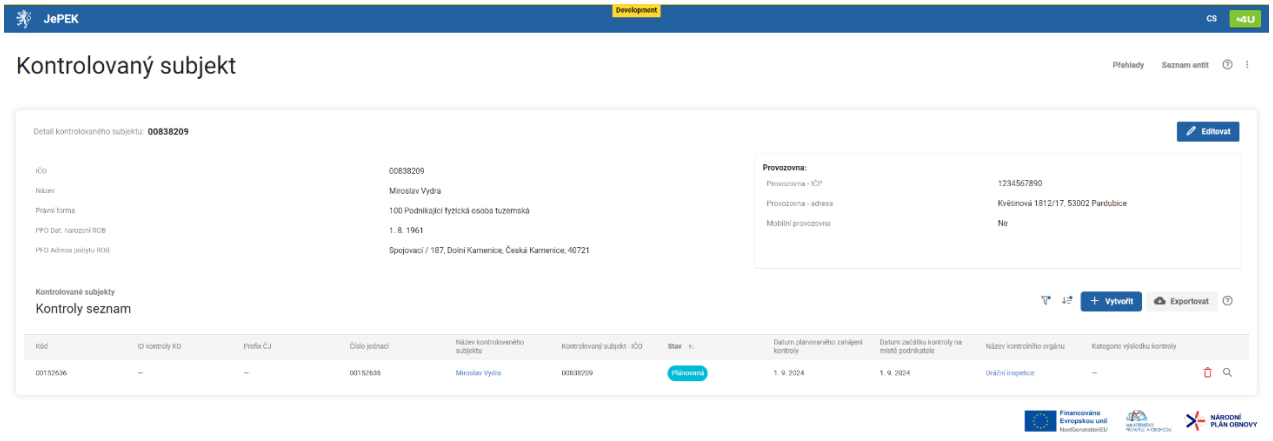
Technický stav	Odvození technického stavu kontroly
Plánovaná nepotvrzená	Odvozeno od stavu hlášení kontrolního orgánu
Potvrzený plán	Odvozeno od stavu hlášení kontrolního orgánu
Pozastavená	Odvozeno od stavu hlášení kontrolního orgánu
V řešení konfliktů	Pokud existují konflikty a nedošlo k zapsání natvrdo přes konflikty
Rozpracovaná	Pokud uživatel zadá Uložit (avšak neuvede termíny, pak je záznam o kontrole rozpracovaný)
Změněná	Odvozeno od stavu hlášení kontrolního orgánu

Kliknutím na ikonu Zobrazit a vyřešit konflikty se zobrazí seznam kontrol, které vykazují konfliktní scénáře, na základě, kterých se může úředník rozhodnout, jak nadále koordinovat kontrolní činnost na těchto specifických kontrolách.

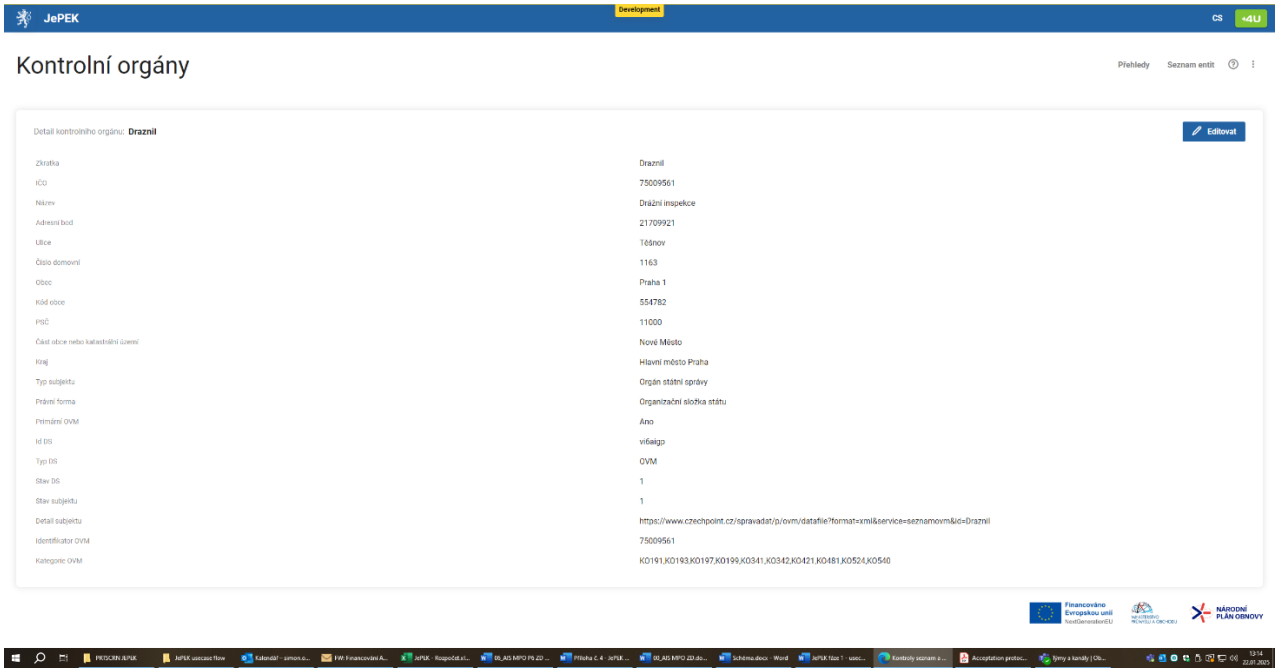




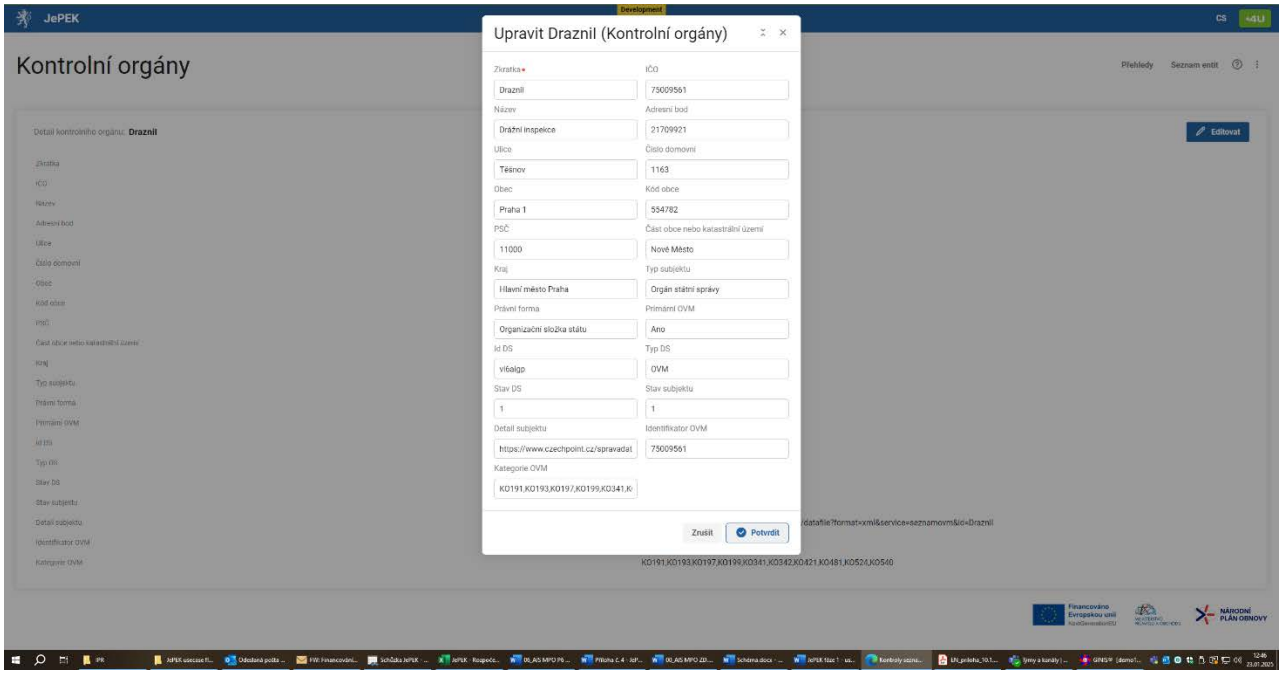
Přechod na obrazovku detail kontrolovaného subjektu kliknutím na jméno kontrolovaného subjektu



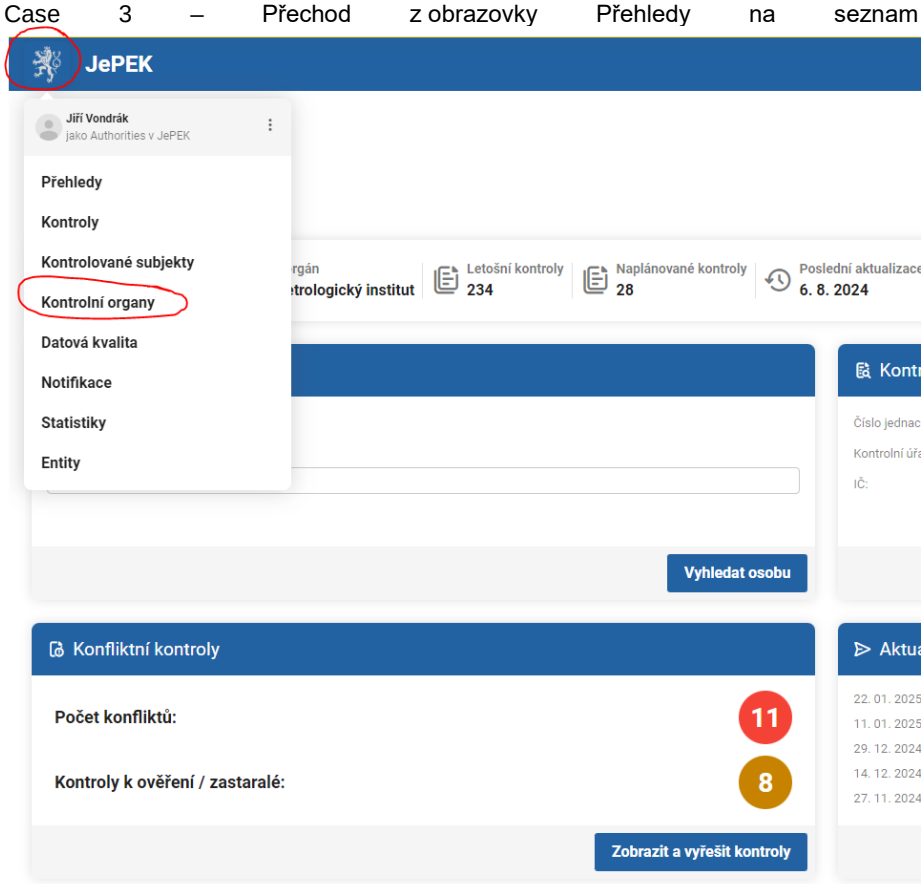
Přechod na detail kontrolního orgánu kliknutím na Název kontrolního orgánu

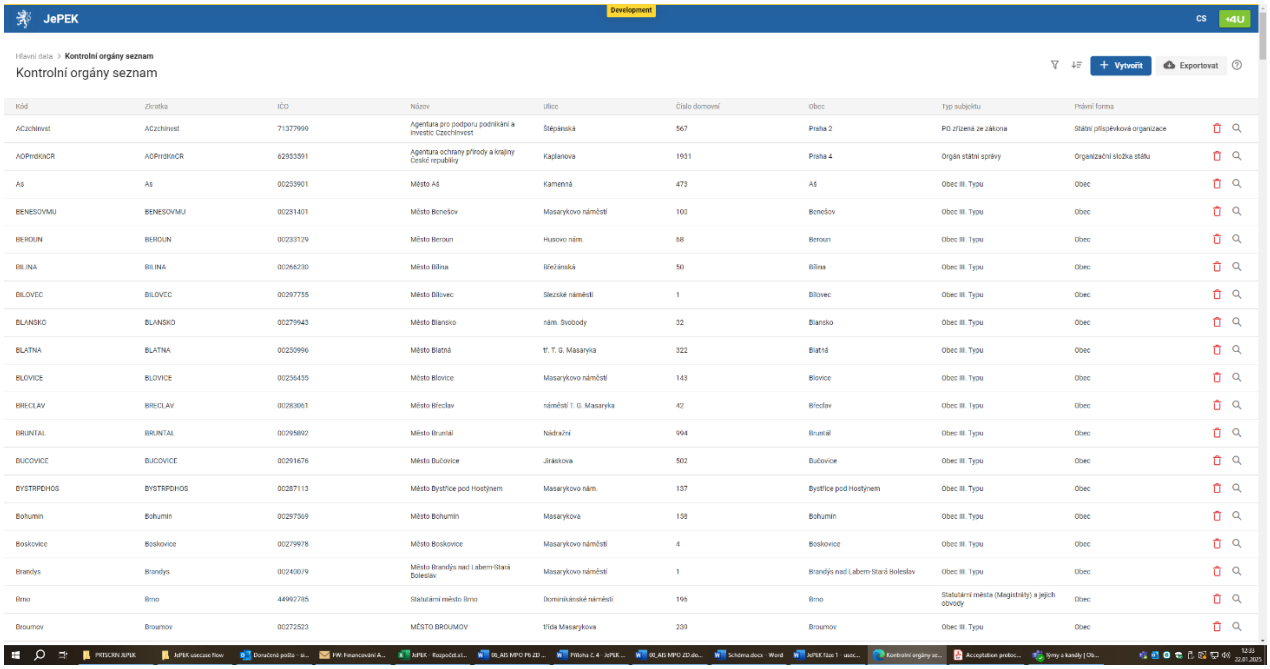


Přechod na editaci Kontrolního orgánu kliknutím na Editovat



Case 3 – Přechod z obrazovky Přehledy na seznam kontrolních orgán





Opět možné dostat se na detail kontrolního orgány pomocí tlačítka lupy vpravo.

5.10.5. Důvody nahlížení na data

Informace o kontrolních zjištěních budou v systému uloženy pro případná nahlížení jiných kontrolních orgánů na základě rozhodnutí Nejvyššího správního soudu ohledně přístupnosti informací o kontrolách (viz rozsudek Krajského soudu v Českých Budějovicích sp. zn. 10Ca 232/2001-40, ze dne 24. 10. 2001, rozsudek Nejvyššího správního soudu sp. zn. 7A 3/2002-46, ze dne 14. 1. 2004). Informace o zjištěních nebudou v základním náhledu tedy automaticky k dispozici, ale budou zobrazeny jen na základě uvedení důvodu, kdy uživateli budou nabídnuty předpřipravené důvody pro nahlížení na výsledky kontrol.

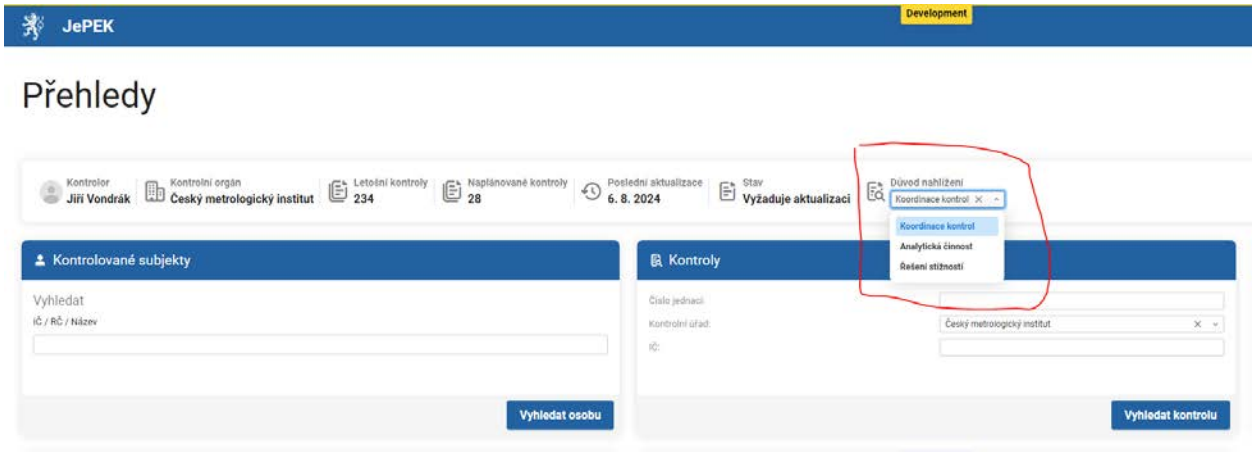
Kontrolnímu orgánu nepřísluší (dle rozhodnutí správního soudu) verifikovat důvody pro nahlížení na výsledky kontrol, proto ani systém JePEK nebude verifikovat tyto důvody. Tímto postupem bude splněn soulad se zákonem a zároveň přístup k výsledkům kontroly.

Poznámka: nahlížení na kontrolní zjištění vychází také z práva na poskytování informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím.

Poznámka: Zároveň nahlížení na kontroly, podobně jako veškeré přístupy v rámci systému JePEK, budou logovány/žurnálovány, aby bylo vždy dohledatelné, kdo, kdy a k čemu přistupoval.

Specifické role (vybrané role pro pracovníky Policie ČR) budou moci prohlížet záznamy a výsledky kontrol bez nutnosti zadat důvod a takové přístupy nebudou logovány v detailu jednotlivého přístupy k záznamům v systému, ale jen na úrovni přihlášení se a odhlášení se nebo vynuceného odhlášení (timeout session) ze systému. Nastavení těchto rolí (pro vyšetřovatele Policie) v systému CAAIS pro JePEK bude podléhat pravidelnému (například jednou za 3 měsíce) fyzickému auditu, který bude zajišťovat Business administrace systému JePEK na MPO ve spolupráci s vedením Policie ČR.

Výběr důvodu nahlížení bude přístupný v záhlaví stránky tak, aby bylo možné jej komfortně, ideálně na jeden klik, vybrat.



5.10.6. Vyhledání podnikatele

Nejtypičtější prohledání kontrol bude pobíhat tak, že vyhledám podnikatele a v jeho kontextu uživatel zobrazí plánované, probíhající i ukončené kontroly.

Vyhledání podnikatele v rámci prohlížení kontrol nebo úprav kontrol bude k dispozici v rámci portletu na Dashboardu (zjednodušeně) a také v menu Kontrolovaných subjektů.

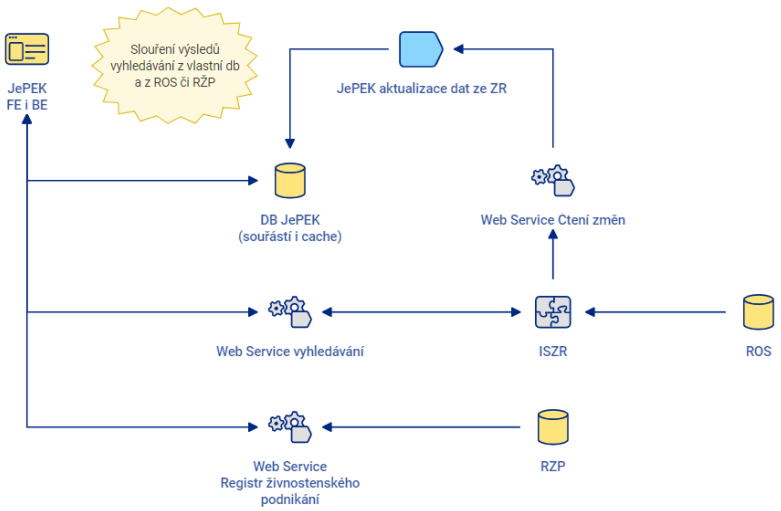
Vlastní vyhledání bude probíhat na částečnou shodu dle možností služeb základních registrů ROS a RŽP.

Systém nejprve vyhledává ve vlastní db v aktuálních verzích firem, následně v historických verzích firem/právnických osob, respektive sloučených firmách (na základě fúze), a pak také v ostatních firmách, které jsou uvedeny v rámci ROS. Uživateli pak systém nabídne vyhledané firmy formou sjednocení všech zdrojů.

Jednotlivé položky množiny vyhledaných firem budou indikovat, jaký vztah mají k vyhledávané frázi, respektive ze kterého zdroje pochází. Systém bude vyhledávat ve zdrojích:

- aktuální cachovaná data ve vlastní db,
- aktuální data po podnikatelích v ROS,
- historická cachovaná data ve vlastní db,
- historická data v ROS.

Pokud budou zadána kritéria pro vyhledávání mimo možnosti ROS a lokální databáze, pak nejprve systém využije Registr živnostenského podnikání a jeho možnosti vyhledávání například v jednotlivých živnostech nebo podle topologické vzdálenosti sídla či provozovny.



V rámci zobrazení výsledku ale eliminuje takové záznamy, které ve výsledku reprezentují jednu firmu v aktuálním zobrazení, tedy pokud je nalezena shoda na aktuálním názvu firmy i historickém názvu firmy a jde o jednu a tutéž firmu, pak se zobrazí jen jeden záznam firmy, a to ve své aktuální podobě. (Případně může být eliminováno i více záznamů.)

5.10.7. Klíče k vyhledání kontroly

Vyhledání kontroly bude probíhat pomocí více alternativně použitelných klíčů, které však nemusí být vždy vyplněny. Alternativními klíči v rámci kontroly jsou:

- Číslo kontroly (interní ID kontrolního úřadu) tak, jak jej drží kontrolní orgán. Toto interní číslo kontroly se uplatní například v případě dlouhodobého plánování, kdy třeba není jisté, že bude kontrola provedena, identifikuje kontrolu v případě kombinace s identifikací kontrolního úřadu a případně příslušným prefixem,
- JePEK číslo kontroly - interní ID systému JePEK,
- Číslo jednací (identifikuje kontrolu v případě kombinace s identifikací kontrolního úřadu a případně příslušným prefixem). Číslo jednací nemusí být vždy k dispozici,
- Dále je možné identifikovat kontrolu číslem protokolu (identifikuje kontrolu v případě kombinace s identifikací kontrolního úřadu a případně příslušným prefixem).

Tyto klíče bude možné použít k identifikaci kontroly v různých stavech, kdy ne vždy má kontrola číslo jednací, a ne vždy je známo číslo JePEK evidence kontroly.

Vyhledávání bude k dispozici v rámci portletu v Dashboardu (zjednodušeně) aplikace a zároveň, detailnější vyhledávání podle více kritérií na částečnou shodu bude k dispozici v rámci menu Kontroly.

Vyhledání kontroly bude možné zajistit i prostřednictvím:

- Výběru kontroly z kontextu kontrolovaného subjektu,
- Výběru kontroly z kontextu kontrolního orgánu.

Vyhledání jak kontrolovaného subjektu, tak i kontrolního orgánu bude možné podle více atributů, a to zejména podřetězce názvu, IČ, adresy sídla nebo adresy pobočky. V případech, kdy vyhledání například kontrolovaného subjektu nepovede právě na jeden kontrolovaný subjekt, pak uživatel nejprve vybere vhodný subjekt z nabídky subjektu odpovídající nastaveným kritériím a zobrazí jeho detail s kontrolami. Následně vybere vhodnou kontrolu například podle typu nebo datumu či kontrolního orgánu.

Vyhledání kontrolovaných subjektů i kontrolních orgánů bude možné ze samostatných přehledů přístupných pod položkami hlavního menu. Navíc vyhledání kontrolovaných osob bude možné z portletu (součást dashboardu/přehledu) pro vyhledání kontrolovaných subjektů. Právě vyhledání kontrol z kontextu kontrolovaného subjektu nalezeného podle IČ bude jedním z nejčastějších scénářů použití systému.

Alternativně pak bude možné kontroly filtrovat podle více kritérií z přehledu kontrol a vyhledání kontrol.

5.10.8. Editace nové verze kontroly

Veškerá editace kontroly bude probíhat formou vytvoření nové verze kontroly s časovou hodnotou platnosti záznamu kontroly. Změny platnosti datumů na kontrole jsou vždy impulsem k jejich přepočtu (pokud nejsou zadány všechny) a též nové koordinace kontroly a také předmětem nového záznamu verze kontroly.

Editace bude umožněna podle nastavení přístupových práv a podle datových práv na tzv. portfolia.

Editace na přístupová práva bude založena na přidělených rolích a z nich vycházejících oprávněních uživatele, kdy například v roli čtenář nebude možné editovat, zatímco v obecné roli inspektor bude možné editovat. Business administrátor systému na MPO a pracovník podpory systému bude moci editovat záznamy všech kontrolních orgánů.

Pro vybrané role bude nastavena editace na tzv. portfolia, což v případě JePEK znamená, že reprezentant kontrolního orgánu, respektive určitého organizačního útvaru kontrolního orgánu, bude moci editovat pouze kontroly zadané odpovídajícím kontrolním orgánem, respektive stejným organizačním útvarem. Při zavedení kontrolního orgánu do systému JePEK bude konfiguračně stanoveno, zda se uplatní možnost editace na celý

kontrolní útvar, nebo zda se uplatní editace pouze na korespondující organizační útvar. Naopak nepředpokládáme možnost přístupu oběma způsoby podle role pro jeden organizační útvar. Při změnách organizačních útvarů nebo změnách způsobu integrace na systém JePEK pro jeden kontrolní útvar bude zajištěna Úprava dat pomocí Business administrace systému na MPO.

Smazání kontroly

Smazání kontroly, respektive plánu kontroly, bude realizováno pouze tak, že bude uložena nová verze příslušné kontroly, kdy stav bude nastaven na Smazaná. Smazání pak znamená „označení za smazanou“, ale nedojde ke skutečnému vymazání kontroly.

Přepočty datumů

Při editaci kontroly dojde k přepočtům datumů. Smyslem přepočtu je doplnit údaje pro takové situace, kdy kontrolní orgán (respektive reprezentant kontrolního orgánu přes GUI) nezadá různé datumy ke kontrole (ať již proto, že s nimi kontrolní orgán nepracuje, nebo z opomenutí, anebo že v okamžiku zadání nejsou údaje známy). Business logika určuje, jak budeme pracovat s datumy, pokud je uživatel nezadá na GUI, nebo nevyplní v excelu anebo systém nezaloží službou či importem. Datumy budou použity pro účely zobrazení a řazení. Principiálně bude systém JePEK vycházet z konfigurace typu kontroly.

5.10.9. Principy datumů

Datumy na kontrole vnímá jinak kontrolní orgán a jinak i podnikatel:

- Z hlediska kontrolního orgánu: zahájení a ukončení kontroly,
- Z hlediska podnikatele: zahájení kontroly na místě, ukončení kontroly na místě.

Dichotomie: Plán a realita

- Plánované datum,
- Skutečné datum.

Pro výpočet dalších informací systému JePEK postačí v podstatě jeden datum na kontrole, pokud víme, co označuje.

Plánem JePEK je spravovat co nejvíce kontrol, i když nebudou datově ideální, a proto kontroly raději přijmeme, než bychom je vraceli kvůli datovým nedostatkům.

5.10.10. Logika výpočtu s datumy

Vše bude systém počítat v pracovních dnech se zohledněním státních svátků.

Pokud mám zadáno Plánované zahájení, pak:

> zahajení: = planovaneZahajeni,
> zacatekNaMiste: = planovaneZahajeni (Pokud je forma kontroly (z konfigurace) "Administrativní/Dokladová" (to znamená nejdu k podnikateli, ale jen si vyžádám nebo jinak získám doklady), pak nepočítám zacatekNaMiste a ukonceniNaMiste),
> ukonceniNaMiste := zacatekNaMiste + Typické trvání kontroly na místě u podnikatele (z konfigurace typu kontroly) – 1,
> protokol (datum protokolu) := ukonceniNaMiste + Typická doba pro vytvoření protokolu (z konfigurace) -1
> ukonceni (datum ukončení kontroly): = protokol (datum protokolu) + Typická doba od protokolu do ukončení kontroly(z konfigurace) -1,
> zverejneniPlanovani := planovaneZahajeni - Zveřejnit plán kontroly pro podnikatele před začátkem(z konfigurace),
> zverejneniKontroly : protokol (datum protokolu) + Zveřejnit kontrolu pro podnikatele s odkladem od datumu protokolu (z konfigurace.)

Pokud máme zadané na kontrole jiné datum, pak výpočty provedeme analogicky dle rovnic uvedených výše s tím, že vyjdeme ze zadaných datumových údajů, kdy největší relevanci mají datumy s nejvyšší hodnotou.

Pozor:

- Pokud by se systém při odečítání někde dostával do nesmyslných datumů (vlivem chybné konfigurace nebo editace, kdy konkrétní kontrola neodpovídá typickým hodnotám), jako například konec kontroly je uváděn s dřívějším datem než její začátek, pak samozřejmě platí, že začátek kontroly je shodný s jejím koncem.
- Pokud již má systém zadané reálné hodnoty, pak již nebude dopočítávat plánované hodnoty (patrně kontrolor provedl kontrolu, aniž ji předtím plánoval a tento plán evidoval v systému).
- Pokud je forma kontroly (z konfigurace) "Administrativní/Dokladová" (to znamená nejdu k podnikateli, ale jen si vyžádám nebo jinak získám doklady), pak nepočítám zacatekNaMiste a ukonceniNaMiste.

Pokud je zadáno více datumů, ale ne všechny, pak se datumy počítají od zadaných „konců intervalů“ a od realizace, nikoliv od plánu.

Všechny datumy, které jsem vypočetl, tak jsou označeny hodnotou "Vypočtená", jinak hodnotou Zadaná. Na GUI systému se vypočtené hodnoty budou zobrazovat vizuálně odlišené (například italikou a o něco světlejší barvou).

5.10.11. Časová osa kontroly při zobrazení a editaci

Na kontrole bude uvedeno více datumových údajů, které zachycují pohled na kontrolní činnosti jak z pohledu podnikatele, tak z pohledu kontrolního orgánu. Zobrazení časové osy: seřadit podle datumových hodnot pod sebou.

Pokud budou mít datumové údaje stejnou hodnotu, pak je na časové ose vypsat podle typů v následujícím pořadí:

- planovaneZahajeni,
- zahajeni,
- zacatekNaMiste,
- ukonceniNaMiste,
- protokol,
- planovaneUkonceni,
- ukonceni,
- zverejneniPlanovani,
- zverejneniKontroly.

Pro Editaci bude použito stacionární zobrazení jednotlivých možných datumů.

5.10.12. Zobrazení poznámek na kontrole

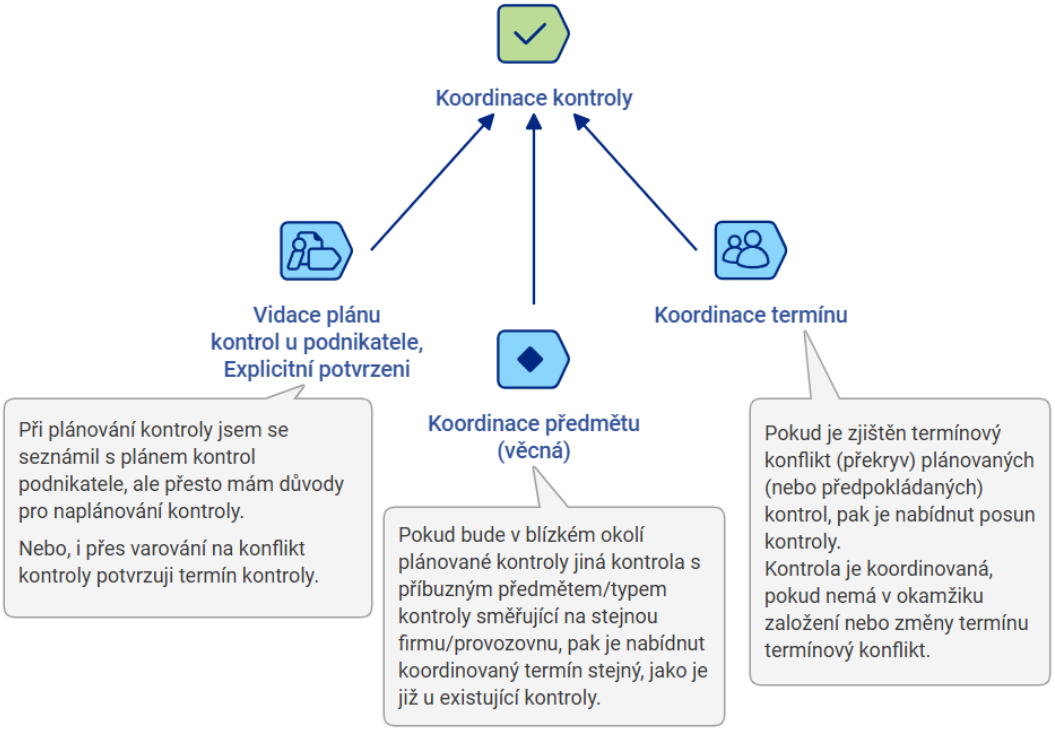
Každá kontrola může obsahovat nula či více poznámek. Tyto poznámky se zobrazují vždy na aktuální verzi kontroly všechny, tedy včetně sjednocení poznámek vázaných k historickým verzím kontroly.

5.10.13. Zobrazení historických verzí kontroly

V rámci kontroly je možné si zobrazit i historické verze kontroly, a to po jednotlivých datumech, kdy došlo ke změně kontroly. Historická verze zobrazuje stav a hodnoty kontroly tak, jak odpovídaly poslednímu okamžiku před další změnou verze kontroly. Poznámky na kontrole se zobrazují relevantně, tj. ty, které byly známé před změnou verze kontroly (včetně informace, že následně došlo k aktualizaci kontroly).

5.11. BPK04 Koordinace kontroly

Cílem procesu je umožnit uživateli, ať již přistupuje k systému jakýmkoliv způsobem, aby snadno obdržel informaci o tom, zda je kontrola bez termínových i věcných konfliktů s jinými kontrolami, případně navrhnout vhodné termíny pro realizaci kontrol.



Kontrola je koordinovaná, pokud nemá termínový (a místní) konflikt u konkrétní firmy.

Dále je kontrola koordinovaná v následujících případech:

a) Je zapsána v překryvu termínů u podnikatele (termínový konflikt a zároveň místní konflikt), pokud se reprezentant kontrolního orgánu již ptal na konkrétní časové období u podnikatele v minulosti (konfiguračně dáno, jak velké). Tedy patrně zjišťoval, zda u podnikatele jsou plánovány jiné kontroly, a pokud se pak rozhodl zapsat plánovanou kontrolu i přes konflikty znamená, že k tomu měl nejspíše důvod.
b) Pokud reprezentant v rámci webové služby nebo přes GUI potvrdí, že ví o konfliktech, a přesto nepřeplánuje kontrolu.

Smysl vyhodnocení stavu koordinace kontroly je, že pokud už u kontrolované osoby jsou v překryvu termínů nějaké jiné kontroly, pak jde o jednotlivé konflikty k řešení.

Řešení konfliktu je buď překryv kontrol (tj. přijďte spolu – ve stejný datum a čas) v případě, že kontroly jsou dle konfigurace příbuzné (tj. například vyžadují součinnost od stejné odbornosti například bezpečnostního technika nebo účetní), nebo naopak posun kontroly, tj. přijďte jindy, v případě, že předmět kontroly je nepříbuzný.

V případě, že konflikt je v datumech, ale v zásadě jde o příbuzný typ kontroly, pak se vlastně o konflikt kontrol nejedná (protože řešení je již původní návrh).

Výpočet kontroly vhodného datumu pro koordinaci kontroly je uveden v příloze. Tento se následně použije v rámci práci na GUI i v případě vzdálené dávkové i vzdálené koordinace.

Vidace plánu kontroly bude mít odlišná pravidla po plánování kontrol a zpětný zápis historické kontroly:

Plánování kontrol: pro vidaci plánu kontroly (tedy pracovník se zamyslel nad možnostmi vyjít podnikateli vstříc, ale nebylo to v jeho možnostech, pak předpokládáme krátký časový úsek mezi naplánováním kontroly a předchozí vidaci plánu kontroly. Bude použit jeden konfigurovaný časový úsek pro použití kanálu přímé editace (v řádu minut), jeden konfigurovaný časový úsek pro plánování kontrol formou excelu (v hodinách či desítkách hodin) a jeden časový úsek pro integraci formou integrace informačních systémů.

Zápis provedených kontrol: v případě, že kontrolní orgán pracuje pouze se zápisem ukončených kontrol, pak logicky by mělo dojít k vyhodnocení situace, kdy si pracovník kontrolního orgánu prohlížel před započetím kontroly, ačkoliv

zapisuje až po ukončení kontroly. V takovém případě se časové intervaly na prohlížení kontroly nebudou vztahovat k zápisu plánu kontroly ale k zapisovanému skutečném počátku kontroly.

5.12. BPK05 Vzdálená koordinace a management kontrol

Předmětem vzdálené koordinace a managementu kontrol je komunikace pomocí webových služeb, zakládání, editace a synchronizace kontrol mezi systémy kontrolních orgánů a systémem JePEK.

Kontrolní orgán bude postupovat v několika krocích:

1. Seznámení se s plánem kontrol na kontrolovaném subjektu a jeho provozovně (nepovinný krok),
2. Naplánování (nepovinné z hlediska JePEK, povinnost a míru plánování si stanovuje každý kontrolní orgán samostatně),
3. Aktualizace kontroly (nepovinný krok z hlediska JePEK),
4. Aktualizace či propis uskutečněné kontroly (povinný krok) včetně ošetření vstupních dat před zápisem do IS.

5.12.1. Naplánování kontroly, respektive zápis kontroly

Pokud se kontrolní orgán rozhodne kontrolovat podnikatele a používá vlastní informační systém, který je integrovaný se systémem JePEK, pak kontrolní orgán využívá vlastní pravidla plánování, tedy kdy, koho a na co bude kontrolovat. Zároveň identifikuje kontrolu vlastním identifikátorem.

Následně zapíše do systému JePEK kontrolu, a pokud je tato kontrola bez termínové kolize a věcné kolize včetně parametricky zadaných intervalů mezi kontrolami, pak je kontrola zapsána do systému. V opačném případě systém upozorní na kolizi a navrhne až čtyři možné termíny. Viz kapitola Algoritmus návrhu termínů koordinace kontrol.

Příslušnou informaci obdrží integrovaný systém kontrolního orgánu a zpracuje ji podle interní logiky. (Ideálně aby tuto informaci předal uživateli ke změně termínu, respektive automaticky zohlednil při automatickém rozvržení termínů pro plánování). Pokud integrovaný systém kontrolního orgánu zapisuje již ukončenou kontrolu, pak systém JePEK již jen kontrolu zapíše bez koordinace, protože tato v případě ukončené kontroly již nedává smysl. Konflikty na kontrole a koordinovanost kontroly je ale systémem JePEK spočítána, aby mohla být použita pro statistické účely vyhodnocení kontrol.

Případ odpovídá zelenému obdélníku na přiložené ilustraci.

5.12.2. Zápis kontroly i přes konflikty

Pokud uživatel integrovaného systému nebo algoritmy zpracování v rámci integrovaného systému vyhodnotí, že je nutno naplánovat kontrolu do uvedeného období, pak nastaví hodnotu flagu zápis přes konflikty (force). Následně systém zapíše příslušnou verzi kontroly (včetně informace o vynuceném zápisu přes konflikty) do systému, což bude statisticky využito při hodnocení práce s kontrolami a koordinací kontrol.

V případě zápisu ukončené kontroly nebo vynuceného zápisu přes konflikty na překrývající se intervaly kontrol od stejného kontrolního orgánu a stejného předmětu kontroly bude systém generovat zjištění datové kvality.

Případ odpovídá červenému obdélníku v následující ilustraci.

5.12.3. Aktualizace kontroly

Kontrolní orgán dle svého uvážení může provést aktualizaci kontroly. Aktualizace kontroly zohledňuje veškerá pravidla verzování kontrol a autorství verzí kontrol. Aktualizaci kontroly lze provádět v jakémkoliv stavu kontroly včetně návratů mezi stavy. Díky tomu, že integrovaný systém má vlastní pravidla přidělování identifikace kontroly i příslušných čísel jednacích, bude systém JePEK podporovat více variant identifikace kontrol pro jejich aktualizaci.

5.12.4. Aktualizace pod vlastní identifikací kontroly

Pokud integrovaný systém kontrolního orgánu pracuje s vlastní číselnou řadou nativně, bude moci použít vlastní identifikaci kontrol k provedení jejich aktualizace.

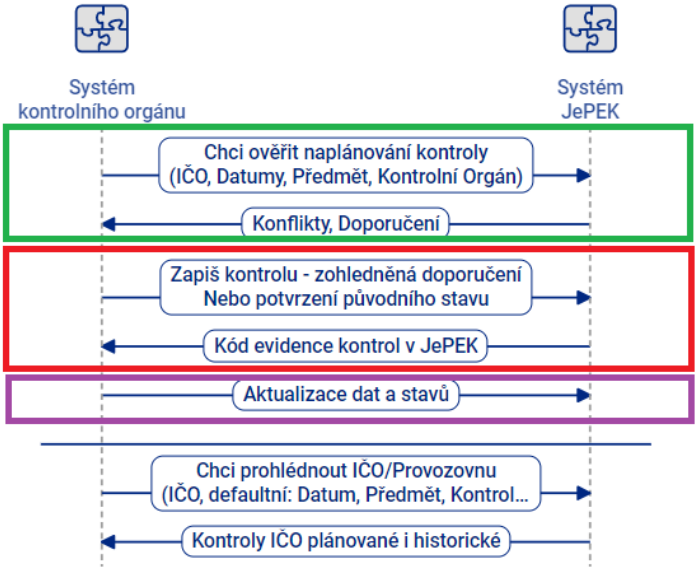
Pokud integrovaný systém kontrolního orgánu přiděluje čísla jednací ke kontrolám (nebo je nějak odvozuje z jiných identifikací), integrovaný systém může alternativně použít k identifikaci i číslo jednací.

5.12.4.1. Aktualizace pod JePEK identifikací kontroly

Pro identifikaci kontroly pro aktualizaci je nutno použít alespoň jeden z nabízených prostředků identifikace kontrol. Pokud je použito více, pak systém JePEK použije identifikaci dle priority identifikačních atributů a zaloguje varování případné neodpovídající/zmatečné identifikace.

Pokud nebude kontrola identifikována, pak ji JePEK bude považovat za novou kontrolu. V případě opakovaného zadání bez identifikace na překrývající se datumové intervaly od stejného kontrolního orgánu, budou takové případy zachyceny pravidly datové kvality viz kapitola Zjištění datové kvality.

Aktualizace je předmětem fialového obdélníku v přiložené ilustraci.



5.12.4.2. Prohlížení kontrolovaných subjektů - audit

Záznamy o prohlížení jsou uchovávány pro potřeby auditu, respektive logy pro analýzy chyb.

5.12.4.3. Údaje o prohlížení kontrolovaných subjektů jako podklad pro koordinaci

Údaje o prohlížení bude využívat samotná aplikace pro výpočet koordinovanosti kontroly. Pokud bude informační systém v rámci kontrolního orgánu využívat možnost náhledu na kontrolované osoby, pak tím bude indikovat, že došlo „k zájmu o kontrolovanou osobu, příslušné časové období v relevantně poslední době“. Pokud došlo k dotazu, a tedy pravděpodobně k vidaci pracovníkem kontrolního orgánu, a pracovník i přesto kontrolu naplánoval, tak systém JePEK bude takovou kontrolu považovat za koordinovanou. Nebude tedy již požadovat nové potvrzení ani navrhovat alternativní termíny. Relevantní časový interval, v rámci kterého je považována vidace pro koordinaci, bude parametrem systému.

Pro koordinaci nebude zohledňováno případné organizační členění kontrolního orgánu, ale pouze konkrétním pracovníkem.

5.13. BPS01 Manuální řešení datové kvality

Proces má za úkol umožnit úpravy dat kontrol, na které jsou identifikovány nálezy datové kvality, tedy záznamy kontrol, které nesplňují v nějakém aspektu dostatečnou kvalitu dat v systému.

Pokud dojde k opravě datové kvality formou aktualizace verze kontroly on-line integrací nebo na základě nového podání excelového souboru, pak jsou pro aktualizovanou verzi kontroly přepočítána zjištění datové kvality a

případně jsou historické záznamy označené za vyřešené, a tedy se nebudou on-line zobrazovat, avšak v emailových notifikacích stále budou a na základě deeplinku budou odkazovat do systému.

Pokud uživatel pracuje z GUI, pak z přehledu nebo z detailu nálezu datové kvality, kde je odkaz na kontrolu a vysvětleno, co je na kontrole chybně nebo podezřele, uživatel může upravit data na kontrole. Každá oprava je standardně historizována. Nález datové kvality je po uložení nové verze kontroly přepočítán a korektně nastaven jeho stav.

Pokud uživatel nesouhlasí s nálezem jen v konkrétním případě, pak na elementárním záznamu zjištění datové kvality uživatel označí, že se v tomto konkrétním případě nejedná o problém. Pokud naopak má uživatel názor, že zjištění je chybné, pak mimo systém může kontaktovat Business support systému JePEK na MPO t, aby došlo ke zmírnění pravidla zjišťující varování nebo nálezů datové kvality nebo změně konfigurace.

5.14. BPS02 Procesování v zastoupení

Při provádění změn v zastoupení za reprezentanta kontrolního úřadu, a to nikoliv v podobě plné moci REZA, ale v podobě administrátorského zásahu, pracovník nezastupuje jinou fyzickou osobu (stále pracuje sám za sebe), ale jako fyzická osoba činí kroky za jiný kontrolní úřad. Dopady zastoupení jsou do výběru zastoupené osoby, dopady do logování (kdy takové logovací záznamy budou obsahovat jak informace o zastupujícím, tak informace o zastoupeném uživateli systému).

Pracovníci Business supportu na MPO mají možnost vidět všechny nálezy datové kvality přehledově přes všechny kontrolní orgány a také všechny kontroly bez ohledu na nastavení viditelnosti kontrol. Pracovník pak může na základě informace a domluvy se zástupcem kontrolního orgánu upravit/opravit na kontrole, kdy proces by měl sloužit zejména k situacím, kdy není k dispozici oprávněný pracovník kontrolního úřadu, který má evidenci v systému JePEK na starosti, a je potřeba upravit urgentně data.

Procesování v zastoupení bude indikováno jen pro specifickou roli a na specifických procesech a případech užití. Procesování v zastoupení bude relevantní jen pro procesy Editace kontroly a Dávková editace kontroly. V procesování v zastoupení je potřeba toto vybrat v rámci systému explicitně, že v tuto chvíli nejedná přihlášený uživatel za svůj úřad, ale v zastoupení za ten kontrolní úřad, který původně kontrolu založil nebo za vybraný kontrolní úřad, pokud nové kontroly zakládá. Výběr zastoupení je logováno samo o sobě a zároveň je logováno u každé jednotlivé transakce v systému. Změny kontroly v zastoupení jsou relevantně patrné při zobrazení kontroly.

Naopak procesování v zastoupení se neuplatní pro procesy případy užití jako prohlížení a uložení podkladů pro koordinaci termínů.

5.15. BPS03 Školení a přeškolování

5.15.1. Školení

V rámci systému JePEK bude systémová podpora pro školení uživatelů a zejména pak přeškolování a doškolování.

Na základě zkušeností z jiných podobných systémů předpokládáme, že bude potřeba provést přeškolení/doškolení pracovníků MPO i zmocněnců a reprezentantů kontrolních orgánů při relevantním realeasu, v návaznosti na komunikaci s Poskytovatelem. Školení budou probíhat v neprodukčním prostředí, na anonymizovaných či fiktivních datech.

5.16. BPS04 Řešení neautomatizovaných úloh

Specifické úlohy budou řešeny pomocí předpřipravených, ale běžnému uživateli nepřístupných, funkčností. Budou přístupny jen administrátorům. Takové funkčnosti systému budou určeny jen pro specifické situace a mimořádné situace. Půjde o následující operace:

- Datová migrace – bulk load: takové budou použity třeba pro úvodní datovou migraci ze systémů MF a MMR (FKVS, MS2021Plus) případně při zavádění dalších kontrolních orgánů do systému JePEK migrací jejich kontrol třeba ze starších verzí systémů, které neodpovídají aktuálnímu způsobu domluvené integrace se systémem příslušného kontrolního úřadu.

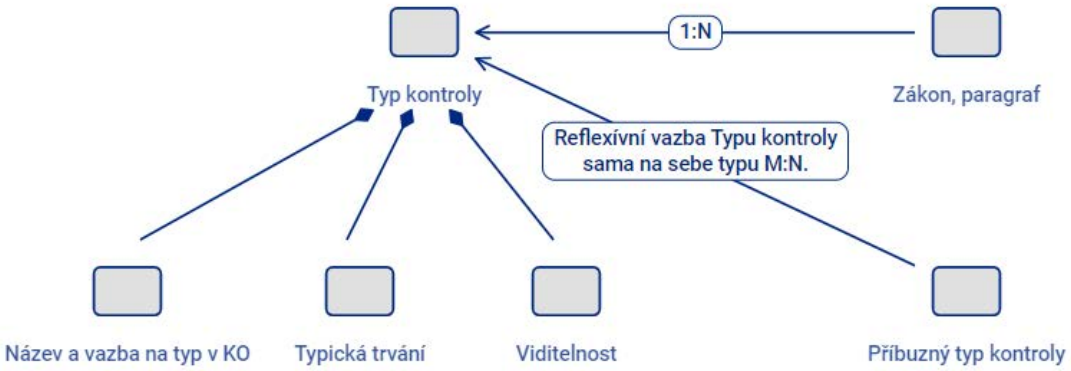
> Opravy verzí systému například možnost změnit kontrolní úřad: takové budou použity například pro situace sloučení kontrol nebo převedení „vlastnictví“ kontroly.
> Převody kontrol mezi organizačními útvary kontrolního orgánů.
> Opravy (či výmaz) kontrol propsaných přes propojení na systémy MS2021+ a FKVS.
> ... neautomatizované úlohy budou přibývat na základě zkušeností z provozu systému.

V případě, že vybrané funkčnosti nebudou přímo zpřístupněny na GUI, budou existovat skripty a návody, jak provést operaci pomocí skriptu administrátorským způsobem.

5.17. BPS05 Správa business konfigurací

Cílem procesu je zajistit business konfigurace, kdy jde zejména o konfiguraci typů kontrol a konfiguraci předvoleb kontrolního orgánu.

5.17.1. Konfigurace kontroly



Typ kontroly bude sdružovat informace o:

> Názvu a typu kontroly a vazbě na kontrolní úřady, které mohou takovou kontrolu provádět,
> Typickém trvání kontroly pro další výpočty typicky datové kvality,
> Viditelnosti kontroly,
> Příbuzných typech kontrol,
> Zákonném ukotvení kontrol.

5.17.2. Označení předmětu kontroly

Pro označení předmětu kontroly bude v rámci projektu připraven konfigurační číselník či sada číselníků, který bude obsahovat několik desítek položek ke konfiguraci předmětu kontroly ve vztahu k chování kontrol.

Předmět kontroly bude spojovat informace o:

- Zákonném důvodu kontroly (vazba na paragraf zákona),
  - Název kontroly
  - Zkrácený název
  - Pravidelnost kontroly (tedy zda musí být provedena v nějakém časovém období)
  - Vynucenost kontroly (zda je konkrétní provedení kontroly přímou povinností a součástí kontraktu/licence/dotace)
  - Povinně koordinovaná kontrola
  - Integrovaná kontrola
- Kategorizaci kontroly,
  - Místní
  - Dokladová
  - Jiná

- Vazbách Typy kontrol (v případě rozvoje právního prostředí, které jsou předchozí a navazující typy kontrol):
    - na předchozí
    - následující typy kontrol
- Vazbách na kontrolní orgány, které typ kontroly mohou provádět,
- Vazbách na kontroly, které mají příbuzný účel kontroly (a tedy mají být plánovány ve stejný den jako jiné kontroly kontrolních orgánů),
- Kategorizaci dopředné viditelnosti kontroly (zda je viditelná všem včetně kontrolovaného subjektu, viditelná kontrolním orgánům, viditelná jen pro specifickou podmnožinu kontrolních orgánů, jen pro specifické subjekty (policie, celní správa, ...), jen pro samotný kontrolní orgán, jen pro hlásící organizační jednotku v rámci kontrolního orgánu (kdy kontrolní orgán utajuje kontroly i před jinými kontrolory v rámci sebe sama),
- Vazbě Dopředná viditelnost pro kontrolní orgány (tedy které KO mohou vidět kontrolu dopředu) - specifická podmnožina KO pro čtení typu kontroly,
- Kategorizaci zpětné viditelnosti kontroly,
- Typických hodnotách provedení kontroly (použije se v případě neúplnosti dat od kontrolních orgánů, kdy typicky data nejsou ve strojově zpracovatelné podobě)
    - Typické trvání kontroly
    - Typická doba kontroly na místě u kontrolovaného
    - Typický interval mezi provedením “kontroly na místě, kdy je vyžadována součinnost kontrolovaného” a datumem protokolu
- Vazbě na zákony a paragrafy
    - Identifikace právního předpisu,
    - Název právního předpisu
    - Odkaz na právní předpis (MPO: businessinfo.cz, e-sbirka.cz)
    - Datumy novelizace

5.17.3. Konfigurace kontrolního úřadu

Konfigurace kontrolního úřadu bude spočívat zejména v nastaveních:

- Povinnosti dodávat data: frekvence, tolerance a povolené způsoby,
- Zajištění uživatelů a domluva o jejich správě, buď delegovaná na administrátora/zmocněnce kontrolního úřadu nebo provedená pracovníky MPO (v CAAIS),
- Zajištění zmocněnce, který bude dostávat upozornění na datovou kvalitu,
- Konfigurace organizační struktury kontrolního úřadu podřízených jednotek tak, aby to bylo možné použít pro konfiguraci viditelnosti kontrol.

5.17.4. Konfigurace číselníků kontrolního úřadu

Interní stavy pro práci interního systému v rámci kontrolního úřadu je potřeba transformovat do unifikovaného pohledu v rámci JePEK nebo alespoň počítat s jejich zpracováním a případně zobrazením na GUI.

Typickými číselníky budou:

- Kategorizace zjištění na kontrole,
- Interní stavy kontroly dle kontrolního úřadu,
- Činnosti, které vyžadují nahlížení na kontroly,
- Prefixy kontrolního úřadu – rozlišení kontrolních úřadů zkratkou pro (pokud nebudou pevně svázány s typem kontroly).

5.17.5. Ostatní technické konfigurace

Další technickou konfigurací je zavedení technických uživatelů v případě integrace systémů, kdy integrace systému kontrolního úřadu a systému JePEK je postavena na komunikaci pomocí certifikátů, kdy k prvnímu vyzvednutí či opakovanému vyzvednutí/obnově certifikátu je potřeba technický uživatel s příslušnými credentials.

Po vyjasnění, zda bude kontrolní úřad napojen prostřednictvím vystavených služeb v CMS2 nebo bude připojen na základě jen vystavených služeb JePEK volně do Internetu budou připravena další nezbytná nastavení pro integraci.

5.18. BPM01 Statistická zpracování

Cílem procesu je zajistit statistická zpracování dat, která budou systémem JePEK spravována a schraňována. Systém JePEK bude nabízet jen omezené statistické informace (například počty u kontrolních orgánů nebo u kontrolovaných osob). Vlastní zpracování bude probíhat ve vhodném Reportingovém systému (jako platformové služby), pro který bude systém JePEK exportovat data v denních EoD dávkách.

Uživatel bude mít k dispozici datové struktury JePEK přístupné v reportingovém systému, ideálně, který již dnes MPO používá.

Systém bude provádět denní extrakty do speciální db, která bude napojena na platformovou službu pro reportingový systém, ke které budou nakofigurovány stejné přístupové údaje, tedy CAAIS role, aby nebylo nutné provádět jiné zavedení uživatelů.

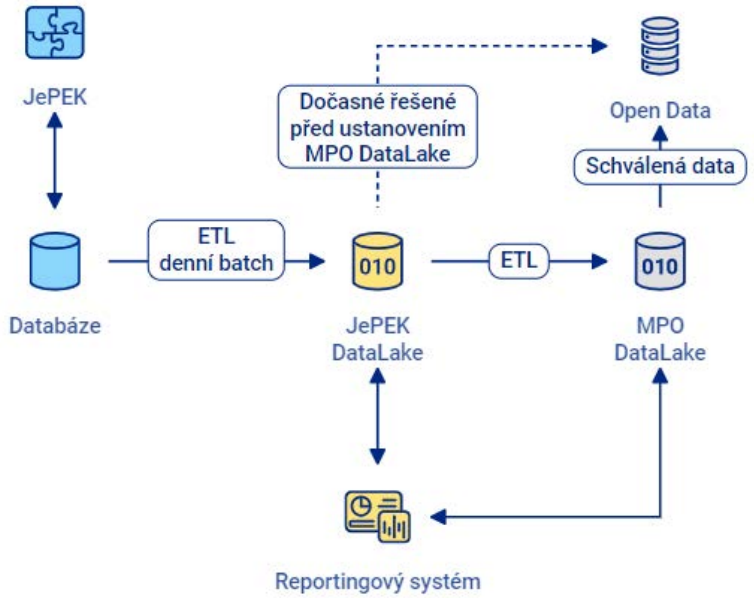
Vlastní zpracování v reportingovém systému bude obsahovat:

a) Sledování business použití systému JePEK – Business kokpit – viz procesy BPM02 nebo BPS03,
b) Statistické zpracování údajů o kontrolách a použití systému JePEK – Analytické studio,
c) Přípravu datové kostky pro zveřejnění v rámci OpenData.

Business kokpit znamená připravenou sadu nástrojů: portálu, datové reporty, datové portlety nebo snipety, a to vše v technologii reportingového systému. Uživatel tyto předpřipravené elementy používá pro předem známé účely zpracování.

Proces statistického zpracování v rámci Analytického studia bude probíhat manuálně a ad-hoc dle potřeby statistických výstupů. Termín Analytické studio v tomto případě označuje část funkčností Reportingového systému, kde uživatel pracuje s daty ad-hoc a jako takové obsahuje funkce pro selekci, spojování a filtrování dat, možnost provádět dílčí výpočty a také obsahuje funkce pro grafickou vizualizaci data a zpřístupňování výstupů.

Příprava dat do datové kostky bude automatizována na základě zpracování datových extraktů z databáze systému JePEK, kdy data budou přenesena a zpracována v rámci datového zdroje pro reportingový nástroj.



5.19. BPM02 Provozní procesy

Cílem projektu je zajistit denní business provoz, vyhodnotit informace o provozu a případně zjednat nápravu v případě provozních problémů.

Business support pro MPO bude realizovat procesy a úpravy denního sledování provozu systému v aktuálním, respektive historickém dni pomocí nástroje pro business administraci, a to zejména:

- Doběhlé a nedoběhlé denní joby:
  - Prostřednictvím konsole jobů s možností je pozastavit, spustit a informacemi o historických běžích jobu, spolu se základními informacemi o zpracování (počty zpracovaných záznamů),
- Kontrolu logovacích souborů:
  - Alternativně je možné nasadit vybraný monitorovací nástroj,
  - Kontrola technických prostředků,
- Kontrolu notifikací,
- Provozní kontrolu na základě business kokpitu v rámci monitorovacího a reportingového nástroje:
  - Sumarizace dat (počty přístupů, počty uživatelů),
  - Podklady pro provozní kontroly budou zpracovány v reportingovém systému jako vhodný dashboard,
  - V případě, že kdy nebudou data odpovídat očekávaným hodnotám, obsluha začne zjišťovat, v čem může být problém.

Obsluha zjistí stav zpracování a podle výsledku provede případně určité provozní služby. Kdy provozní službou jsou známé a definované úkony typicky technického charakteru. Pokud ale výsledek indikuje neznámý problém a zároveň tento problém nemá čistě businessové řešení, pak se uživatel obrátí na IT podporu.

Rozpad Usecase:

Konsole backendového zpracování				
	BUC	S		Specifická aplikace konzole backendového zpracování
	BUC	S		Administrátorské přihlášení do konsole (alternativa bez NIA)

	BUC	L		Menu: Logy a vyhledání, Joby, Konfigurace, Číselníky, Aplikace (info, verze, odhlášení/přihlášení),
	SUC	L		Technické logování přístupů (detaily subjektů, přihlášení, odhlášení)
	BUC	L		Vyhledávání v log souborech
	BUC	L		Konsole na sledování dávkových úloh (co proběhlo a s jakým následkem bylo zpracováno, co by mělo ještě proběhnpout, možnost spustit znovu)
	BUC	L		Přehled jobů - možnost pozastavit a zase znovu spustit
	BUC	L		Znovuprovedení jobů
	BUC	L		Scheduler jobů
	BUC	M		Spustit na požádání
	BUC	M		Přehled odešlých notifikací
	BUC	M		Přehled evidovaných číselníků
	BUC	M		Vylistování obsahu číselníku
	BUC	M		Vyhledávání v obsahu číselníku
	BUC	M		Nastavení nové platnosti položky číselníku
	BUC	M		Editace aktuální položky číselníku
	BUC	L		Správa stromu konfiguračních parametrů obecných
	BUC	M		Správa konfiguračních parametrů kontrolního úřadu (defaultní hodnoty, doby dodávání a podobně)
	BUC	M		On behalf zpracování nahrávaných excelů a příslušné protokoly chyb
	BUC	M		Zobrazení nesouladů mezi konfigurací a předanými kontrolními hlášeními ("Nahlásili za někoho jiného nebo neuvedli")
	BUC	S		Výběr pro Hromadnou změnu (filtr na rozmezí data a času od-do, hlásící uživatel nebo kontrolní orgán)
	BUC	M		Akce změna stavu hlášení kontrol
	BUC	M		Akce změna atributu (KO, závažnost aj) s evidencí historie

5.20. BPM03 Přihlášení čipovou kartou úřadu

Kromě přihlášení pomocí státních prostředků do CAAIS se budou uživatelé (zaměstnanci MPO) přihlašovat pomocí kartičky používané pro přístup do budovy a s certifikátem pro přihlašování se do počítačů v rámci sítě úřadu. Tato karta obsahuje také certifikát, splňující požadavky na přihlašování certifikátem v CAAIS. Aby bylo možné použít přihlašování pomocí certifikátu na této kartě, je potřeba si tento certifikát nejprve zaregistrovat do CAAIS.

5.20.1. Registrace certifikátu

Postup registrace certifikátu do systému CAAIS (zatím popsáno pro starší verzi, ale v nové by mělo být obdobně) https://www.dia.gov.cz/wp-content/uploads/2024/01/CzechPOINT_zmena_hesla_a_certifikatu.pdf.

5.20.2. Přihlášení uživatele MPO certifikátem do JePEK přes CAAIS

Pracovník MPO se do systému JePEK přihlásí, a to (pro produkční prostředí) výhradně pomocí JIP/KAAS případně CAAIS.

Postup přihlášení se pomocí certifikátu do CAAIS (zatím popsáno pro starší verzi, ale v nové by mělo být obdobně) https://www.dia.gov.cz/wp-content/uploads/2024/01/JIP_prihlaseni_Certifikatem.pdf.

Stejné řešení mohou použít rovněž **zaměstnanci jiných úřadů**, kteří se také potřebují přihlásit do vlastních počítačových sítí a mohou využít certifikátu z kartičky nebo jiného nosiče, pokud tento certifikát splňuje příslušné náležitosti.

Jde-li o použití JIP/KAAS jako starší verze systému CAAIS, tak vzhledem ke (deklarované) zpětné kompatibilitě systému je vhodné již používat novou verzi, která by neměla činit problémy s případným přihlášením do starých aplikací.

5.21. BPD01 Procesy dávkových úloh

Pro více účelů je potřeba zajistit dávkovou komunikaci mezi systémem JePEK a s ním dávkově integrovanými systémy. Dále systém bude pravidelně spouštět vybrané úlohy v rámci EoD zpracování.

Součástí řešení JePEK bude subsystém pro definici a spouštění jobů, sledování výsledků jejich běhů a chybových hlášení. V případě problémů bude možné běhy restartovat a případně znovu spouštět.

Dávková integrace:

- Načtení a zpracování souboru z FKVS,
- Načtení a zpracování synchronizačního souboru z ISKP2021+,
- Stažení číselníků z CzechPoint,
- Stažení číselníků z ISZR,
- Datový extrakt pro zpracování v DataLake a reportingovém systému.

Joby, které bude systém spouštět v pravidelných intervalech:

- Výpočty datové kvality,
- Příprava notifikací a odeslání emailů s notifikacemi,
- Načtení a zpracování aktualizačních streamů základních registrů.

Veškerá data budou na vstupu před zápisem do IS a při výstupu bezpečnostně ošetřena.

5.22. BPD02 Výpočty datové kvality

Systém bude pracovat s ukazateli datové kvality v následujících kategoriích případných odchylek od předpokládané či stanovené datové kvality:

- Zastarávání,
- Neodpovídá konfiguraci,
- Nesoulad mezi podáními a domluvenou frekvencí.

5.22.1. Zjištění datové kvality

V rámci pravidelných zpracování budou zjišťována definovaná podezření či nálezy datové nekonzistence nebo chybějících nebo nesprávných údajů - souhrnně nálezy datové kvality.

Jejich cílem je informovat jak Business podporu systému JePEK na MPO o aktuálním stavu a také vybranou roli na straně kontrolního orgánu o nálezech datové kvality tak, aby mohli provést jak nápravu, tak nápravné opatření k tomu, aby podobná zjištění již nevznikala. Zda bude provedena v konkrétním případě jen náprava (náhodný, ojedinělý výskyt nálezu datové kvality), nebo zda bude provedeno i nápravné opatření rozhodne na základě domluvy s MPO zmocněná osoba kontrolního orgánu.

Technicky bude naplněno, aby zjišťující pravidla byla v souladu s kompetencí business administrace do stanovené míry nastavitelná/ovlivnitelná přímo business administrátory MPO bez zásahu Poskytovatele systému JePEK.

Zjištění datové kvality budou kvalifikována z hlediska závažnosti.

5.22.2. Zobrazení zjištění datové kvality na GUI

Zjištění datové kvality budou v systému zobrazena v souhrnné i jednotlivé podobě pro:

- Reprezentanty kontrolního orgánu, kteří budou moci opravit případné zjištění.

- Uživatele v rámci Business supportu MPO systému JePEK pro případnou opravu nebo jednání se zmocněnci kontrolních orgánů.

Zjištění datové kvality budou pravidelně systémem automaticky rozposílána v souhrnných emailech (souhrn zjištění datové kvality pro příslušný kontrolní orgán a/nebo uzel organizační struktury kontrolního úřadu) na reprezentanty jednotlivých kontrolních orgánů určených rolí v systému a v případě použití organizační struktury určených i konfigurací v systému.

5.22.3. Pravidla datové kvality

Pravidla budou zaměřena na následující oblasti:

Zastarávání dat:

> Nenaplněné plánované kontroly po jisté grace periodě.
> Neaktualizovaná ukončení započatých kontrol.
> Kontroly bez doplněných údajů (například ukončená bez protokolu).

Chybné údaje:

> Datumové diskrepance (například záporná nebo nulová trvání, ukončení před datem protokolu a podobně),
> Nedodržování zákonných lhůt nebo naopak příliš dlouhé termíny.

Frekvence podání či aktualizací dat:

> Kontrola včasnosti podání,
> Kontrola správnosti podání (procento chyb v podání).

Obecné kontroly

> Sledování celkového objemu kontrol ve srovnání s minulým obdobím (měsíc, kvartál, rok) na signifikantní rozdíly,
> Termínové konflikty na stejný kontrolní úřad, což indikuje nesprávnou identifikaci kontrol,
> Významné změny stavů a kompletnosti doplnění, což indikuje manipulace s kontrolou.

Konkrétní příklady zjištění datové kvality budou zpřesněny v průběhu další fáze projektu.

5.22.4. Omezené řešení historie datové kvality

Kontroly datové kvality budou relevantní jen pro historicky parametricky daná období tak, aby případně nedocházelo k přehlcení pracovníků množstvím historicky ne zcela datově kvalitních kontrol. Vybraná pravidla datové kvality mohou mít platnost, která umožní stanovit určitou grace periodu pro zavedení nového pravidla.

5.22.5. Napravení zjištění datové kvality

V rámci pravidelných (typicky denních) intervalů bude zjišťováno, zda jednotlivá zjištění datové kvality na konkrétních kontrolách přetrvávají nebo nikoliv.

Pokud bude zjištěno, že kontrola trpící nějakou datovou nekvalitou, tedy zjištěním na základě kontroly datové kvality, již touto nekvalitou netrpí (například po editaci), pak je zapsána na kontrolu typizovaná poznámka, že zjištění datové kvality bylo vyřešeno.

5.23. BPD03 Výpočty a odesílání souhrnných notifikací

Úkolem procesu je identifikovat předpokládané notifikace a tyto notifikace poslat oprávněným uživatelům.

5.23.1. Konfigurace notifikací

V rámci konfigurace systému bude stanovena závažnost jednotlivých zjištění datové kvality a příslušná grace perioda. Dále v rámci konfigurace systému bude nastaveno, která zjištění datové kvality mají být součástí notifikací.

Celá konfigurace bude verzována tak, aby bylo zřejmé, kdy došlo k jakým změnám, a co bylo kdy předmětem notifikací.

5.23.2. Výpočty elementárních notifikací

Součástí řešení bude opakovaný výpočet (job), který bude pravidelně spouštěn typicky každou noc a bude navazovat na výpočty datové kvality.

Pro účely notifikací pak budou nejprve zjištěna všechna relevantní zjištění datové kvality, které jsou předmětem notifikací dle konfigurace notifikačního pravidla.

5.23.3. Tvorba souhrnných notifikací

Souhrnná notifikace se bude sestávat z hlavičky sumarizující počty a kategorie notifikací.

Kategorie budou minimálně:

- Datová kvalita:
  - Zastarávající,
  - Neúplné,
  - Chybné.
- Zprávy obsluhy pro uživatele.

Notifikace budou dále kategorizovány a uváděno, zda jsou Nové, Opakované. Kategorie Nové znamená nové od posledního běhu jobu připravujícího notifikace, tedy že stejná notifikace nad stejnou kontrolou nebyla v minulosti odeslána, respektive připravena k odeslání.

Bude-li pro kontrolní úřad potřeba odeslat více než 500 (konfigurační parametr) notifikací na základě datové kvality, pak je odesláno pouze 500 elementárních notifikací a spolu s nimi upozornění, že počet aktuálních zjištění vyžadujících zásah uživatele je větší a bude prezentován jejich celkový počet.

Jednotlivé notifikace budou posílány na kontrolní orgán podle frekvence aktualizace dat, a to buď týdně (pro týdenní nebo kratší interval), nebo měsíčně a případně i v delším intervalu.

5.23.4. Určení adresátů notifikací

Adresáti notifikací budou identifikovány rolí Zmocněnec kontrolního úřadu. Osoba s touto rolí bude dostávat pravidelné notifikace.

Systém ze systému CAAIS získá seznam uživatelů pro agendu JePEK pomocí GetUserListRole, která slouží k získání seznamu uživatelů jednoho subjektu, kteří mají přidělenu určitou přístupovou roli do agendového informačního systému. Následně rozdělí uživatele dle subjektů - Kontrolních orgánů. Bude platit, že všichni uživatelé pro kontrolní orgán s příslušnou rolí obdrží kompletní sadu notifikací příslušného kontrolního orgánu. Tento seznam bude v systému JePEK cachován.

Postup použití GetUserListRole:

1. Dojde k události, která vyžaduje, aby AIS zavolal webovou službu GetUserListRole.
2. JePEK musí informovat lokálního administrátora příslušného subjektu, že od něj vyžaduje autorizaci příslušné akce přihlášením. JePEK musí lokálnímu administrátorovi zobrazit důvod autorizace příslušné akce.
3. JePEK přesměruje lokálního administrátora do autentizační webové služby CAAIS, kde lokální administrátor zadá své přihlašovací údaje a po jejich úspěšném ověření je přesměrován zpět do AIS. AIS po zavolání metody authConfirmation obdrží v odpovědi od autentizační webové služby CAAIS údaje o lokálním administrátorovi včetně údaje „TimeLimitedId“ (viz dokument s technickým popisem autentizační webové služby. KAAS). JePEK použije údaj „TimeLimitedId“ k autentizaci do webové služby GetUserListRole.

4. JePEK zašle požadavek webové službě GetUserListRole. Požadavek obsahuje zkratku přístupové role a odůvodnění, proč je požadavek pokládán. Důvod zpracování požadavku na pozadí musí lokální administrátor znát a akci musí také explicitně potvrdit JePEK.
5. JePEK obdrží od webové služby GetUserListRole odpověď, která obsahuje seznam uživatelů s přidělenou danou přístupovou rolí a patřících do stejného subjektu jako lokální administrátor.
6. JePEK zpracuje přijatou odpověď, uloží si ji.

JePEK se bude autentizovat pomocí basic autentizace podle RFC 2617, kdy parametr „userid“ obsahuje prázdný řetězec a parametr „password“ obsahuje hodnotu tokenu „TimeLimitedId“, který JePEK obdržel v odpovědi od autentizační webové služby KAAS na základě úspěšného ověření uživatele.

JePEK se autentizuje pomocí komerčního serverového certifikátu, který vydala certifikační autorita I.CA, PostSignum, eIdentity nebo Národní certifikační autorita. Zejména v případě I.CA musí vydaný certifikát obsahovat v rozšíření certifikátu „extendedKeyUsage“ atribut „Client Authentication“ (id-kp-clientAuth, OID 1.3.6.1.5.5.7.3.2). Tento autentizační certifikát musí být zaregistrován v nastavení AIS, což se provede pomocí administrační aplikace Správa dat (https://www.czechpoint.cz/spravadat/).

Pokud bude v konfiguraci kontrolního úřadu posílat souhrnné notifikace i na uzly organizační struktury, pak identifikace reprezentanta bude konfigurována na úroveň organizační struktury přímo v systému JePEK. Odesílání souhrnného emailu na reprezentanta celého kontrolního úřadu nebo na reprezentanta uzlu organizační struktury (například místního pracoviště) bude možné kombinovat.

5.23.5. Registrace a odesílání notifikací

Připravené seskupené notifikace jsou odeslány prostřednictvím webové služby pro odesílání emailů do emailových schránek adresátů, které byly obdrženy přímo ze systému CAAIS v rámci poslední aktualizace.

O odeslaných emailech je vytvořen logovací záznam.

5.23.6. Deeplinky notifikací

Součástí každé elementární notifikace je indikátor, zda se jedná o novou, nebo opakovanou notifikaci. Součástí elementární notifikace je i deeplink, který obsahuje odkaz přímo na příslušnou kontrolu v systému JePEK (po případném přihlášení), aby ji uživatel rovnou mohl editovat, doplnit či opravit.

5.24. BPD04 Zpracování změn registračních údajů

Systém bude v rámci CMS2 napojen na ISZR, a to zejména ROB a ROS. Systém bude zpracovávat informace o změnách v systému ROS, neboť tyto změny musí zaznamenat do aktuálních i historických kontrol. Smyslem je podchycení skutečnosti, že se určitá firma transformovala, přejmenovala nebo se přestěhovala – je nutné zachytit její historii. Historie bude zachycena formou historizace cachovaného záznamu firmy, která byla kontrolována – kontrolované osoby, kdy na kontrolu bude zapsána poznámka o aktualizaci kontroly.

5.25. Základní vysvětlení k aktualizaci

V základních registrech jsou vedeny základní údaje, které jsou zároveň obsaženy v mnoha AIS. Např. u základního registru obyvatel (dále jen „ROB“), resp. základního registru osob (dále jen „ROS“), se jedná zejména o jméno, název (obchodní firmu), datum narození, identifikační číslo osoby.

Správnost tzv. referenčních údajů v základních registrech je naproti tomu výslovně garantována, a to prostřednictvím § 4 odst. 4 zákona o základních registrech. Zásady ochrany dobré víry ve správnost referenčních údajů jsou dále ochráněny prostřednictvím § 4 odst. 6 a 7 zákona o základních registrech. Správnost referenčních údajů tak není třeba ověřovat a není dáno oprávnění požadovat po osobách doložení těchto údajů, jak je výslovně stanoveno § 5 zákona o základních registrech.

(Naopak, systém JePEK podobnou garanci, podobně jako většina ostatních systémů státní správy, neobsahuje.)

Pokud je některý z údajů v základních registrech změněn a správci AIS tyto údaje vedou ve svých AIS, přičemž mají oprávněni čerpat tyto údaje ze základních registrů, jsou automaticky informováni (notifikováni) o tom, že došlo

ke změně těchto údajů. Např. v případě osoby, u níž dojde ke změně adresy místa trvalého pobytu a která je vlastníkem nemovité věci zapsané v katastru nemovitostí a zároveň společníkem ve společnosti s ručením omezeným, budou správci příslušných AIS, jak v katastru nemovitostí, tak i v obchodním rejstříku automaticky notifikováni. Uvedený mechanismus funguje i mezi základními registry navzájem, v uvedeném případě dojde též k notifikaci do základního registru osob a do základního registru územní identifikace, adres a nemovitostí (dále jen „RÚIAN“).

Nejvhodnějším provedením popsaného propojení je tzv. referenční vazba, kdy je údaj veden v AIS (nebo v jiném ZR) technicky, nikoliv jako doslovný zápis údaje, nýbrž jako odkaz, který zobrazuje údaj vedený v příslušném zdrojovém základním registru. K jeho změně tak dochází zcela automaticky. Nicméně takový přístup není z provozních důvodů aplikace možný (zobrazení v browsech, statistické zpracování), a proto aplikace JePEK bude udržovat informace dle platného postupu ze základních registrů z ROS a následně je bude na základě poskytované notifikační služby změn aktualizovat.

5.25.1. Pravidelné čtení změn

Systém JePEK bude obsahovat job pro načtení změn. V rámci tohoto jobu bude systém pro účely aktualizace cachovaných dat využívat službu

rosCtiZmeny - https://www.szrcr.cz/images/dokumenty/v%C3%BDvoj%C3%A1%C5%99i/detailn%C3%AD_popisy_eGon_slu%C5%BEeb/SZR_popis_eGON_sluz%CC%8Ceb_E28_rosCtiZmeny_1_01_v7_r0_002.pdf

jedná se o notifikační službu. Výstupem je seznam IČO, včetně všech záznamů, u nichž došlo během uživatelem zadaného časového intervalu ke změně v referenčních údajích osoby. Informuje o změnách referenčních dat, které v ROS proběhly během uživatelem stanoveného období, kdy období bude nastaveno od posledního běhu jobu, tedy za poslední den.

Službu bude nutné volat opakovaně, protože služba bude vracet pouze limitovaný počet záznamů, tedy pokud bude počet změn v daný den větší než limit služby.

5.25.2. Čtení jednotlivé změny

Každý změněný záznam z minulého kroku bude systémem JePEK zpracován následujícím způsobem. Nejprve systém načte informace z ROS/ROB pomocí služeb, následně zhodnotí, zda jde skutečně o změnu, která je relevantní pro provedení zaznamenání a zaverzování do systému JePEK.

Ke čtení jednotlivé změny systém JepEK následně použije služby:

- rosCtiICO – služba poskytuje údaje pro zadané IČO. Výstupem jsou všechny referenční údaje, které se o dané osobě v ROS vedou. Mohou jí tedy používat agendy, které mají v RPP oprávnění pro čtení všech údajů ROS.
- rosCtiAIFO – služba čte údaje podnikající fyzické osoby, kde podnikatel je identifikován odkazem do ROB předaným jako vstupní parametr služby. Výstupem jsou vždy všechny referenční údaje osoby. Může ji použít tedy jen agenda, která má oprávnění ke čtení všech údajů ROS.
  Tato služba bude použita jen jako doplňková v situaci podnikající fyzické osoby a její údaje nebudou použity pro například v přepočtu dat pro přístup podnikatelů.

5.25.3. Zaverzování změny do cachovaných dat

Pokud se v cachovaných datech v rámci systému data kontrolované osoby liší od nově získaných dat z ROS, systém JePEK provede aktualizaci formou vytvoření nové verze záznamu kontrolované osoby. Naopak, pokud změna je v jiných atributech, než jsou persistována v systému JePEK, taková změna je vyhodnocena jako JePEK nevýznamná a není předmětem dalšího zpracování v rámci systému.

Zaverzování proběhne tak, že systém JePEK vytvoří novou verzi záznamu kontrolované osoby, změní platnosti historické verze záznamu a zajistí provázání verzí mezi sebou. Aktuální zobrazení historické, probíhající i plánované kontroly pak zobrazují nejnovější verzi záznamu, vyhledávání pracuje s nejnovějším záznamem a také s historickými verzemi záznamu (Tedy pokud se kontrolovaná firma jmenovala Alfa do loňského roku a letos už se jmenuje Beta, pak při vyhledání kontrol firmy Alfa je historický záznam o kontrole na firmu původně Alfa-nyní Beta-

nalezen a zobrazen uživateli). Při další aktualizaci kontroly bude změna znovu zaverzována, a tedy vytvořena nová verze. Při zobrazení explicitně historické verze záznamu systém zobrazí příslušnou historickou verzi záznamu o kontrole.

Po zaverzování pak systém zapíše na kontrolu poznámku o aktualizaci kontrolovaného subjektu a zapíše také záznam do aplikačního logu.

5.26. BPD05 Synchronizace s MS2021+

Synchronizace se systémem bude probíhat formou dávkového exportu ze systému MS2021+ a jeho automatizovaným předáním do systému JePEK. Předpokladem je zabezpečený dávkový přenos souborů nebo zápisem prostřednictvím rozhraní pro aktualizaci. Forma bude upřesněna na základě jednání v průběhu projektu.

Synchronizované kontroly ze systému MS2021+, pokud jejich poslední aktualizace bude provedena právě dávkovou synchronizací (a nikoliv například následnou ruční editací), nebudou předmětem zkoumání datové kvality a ani notifikací respektive validací, kdy nebudou předávány zpět chybové hlášky, neboť pro tyto kontroly je autoritativním systémem MS2021+.

Vstupní data před zápisem do IS budou však pro jistotu bezpečnostně ošetřena.

5.27. BPD06 Synchronizace s FKVS

Synchronizace se systémem bude probíhat formou dávkového exportu ze systému FKVS a jeho automatizovaným předáním do systéme JePEK. Předpokladem je zabezpečený dávkový přenos souborů.

Synchronizované kontroly ze systému FKVS, pokud jejich poslední aktualizace bude provedena právě dávkovou synchronizací (a nikoliv například následnou ruční editací), nebudou předmětem zkoumání datové kvality a ani notifikací, respektive validací, kdy nebudou předávány zpět chybové hlášky, neboť pro tyto kontroly je autoritativním systémem FKVS.

Vstupní data před zápisem do IS budou však pro jistotu bezpečnostně ošetřena

5.28. BPD07 Stažení externích číselníků

Obecně je Kontrolní orgán právnickou osobou, a tedy veden v registru osob. Jako s takovým údajem je potřeba nakládat dle pravidel evidence údajů o subjektech viz https://archi.gov.cz/nap:evidence_udaju_o_subjektech.

Zároveň je Kontrolní orgán orgánem veřejné moci a jako takový udržován v seznamu orgánů veřejné moci publikovaného dle dokumentace v https://www.czechpoint.cz/data/files/SOVM_datove_soubory.pdf publikován na adrese: https://www.czechpoint.cz/spravadat/ovm/datafile.do?format=xml&service=seznamovm, respektive na adrese: https://www.czechpoint.cz/spravadat/ovm/datafile.do?format=xsd&service=seznamovm. Seznam orgánů veřejné moci dále využívá další číselníky, a to:

- Číselník krajů,
- Číselník typů e-mailových adres,
- Číselník typů webových stránek,
- Číselník kódů stavů datových stránek,
- Číselník typů datových schránek,
- Číselník podtypů datových schránek.

Soubor s detailními informacemi o OVM je dostupný na této adrese: https://www.czechpoint.cz/spravadat/ovm/datafile.do? format=xml&service=seznamovm&id=ZKRATKA Místo „ZKRATKA“ je zapotřebí uvést zkratku subjektu, kterou lze dohledat v indexovém souboru jako element „Zkratka“.

Kdy jednoznačně data o orgánu veřejné moci z číselníku Checkpoint jsou detailnější a pro JePEK použitelnější než data v ROS. Ale jsou aktualizována se zpožděním (bez známé garance) a aktualizace zveřejňována jen jednou za 24 hodin.

V tomto datovém souboru je uložen seznam následujících OVM, mezi které patří:

- Krajské úřady,
- Ministerstva,
- Obce I. Typu,
- Obce II. Typu,
- Obce III. Typu,
- Statutární města (magistráty) a jejich obvody,
- Orgány státní správy,
- Ostatní orgány veřejné moci.

V souboru se nacházejí základní údaje o OVM a odkaz pro stažení datového souboru s detailními informacemi o daném OVM.

Číselník typů OVM bude stahován na základě zveřejněných open dat a k dispozici jsou https://data.gov.cz/datov%C3%A1-sada?iri=https%3A%2F%2Fdata.gov.cz%2Fzdroj%2Fdatov%C3%A9-sady%2F17651921%2F7b645f4f6ec980bcbe68343a59a69d28

Součástí možnosti stahovat a používat takový číselník je registrace systému JePEK jako odběratelského aplikace/systému číselníku v rámci OpenData. Tuto registraci zajistí MPO v rámci pokračování projektu.

Dále bude systém cachovat číselníky používané v rámci základních registrů, a to pomocí služeb:

- iszrCtiSeznamCiselniku pro načtení seznamu číselníků - https://www.szrcr.cz/images/dokumenty/v%C3%BDvoj%C3%A1%C5%99i/detailn%C3%AD_popisy_eGon_slu%C5%BEeb/E97_iszrCtiSeznamCiselniku.pdf,
- aisvCtiCiselnikUdaju pro načtení obsahu obsahu číselníku - https://www.szrcr.cz/images/dokumenty/v%C3%BDvoj%C3%A1%C5%99i/detailn%C3%AD_popisy_eGon_slu%C5%BEeb/SZR_popis_eGON_sluzeb_E321_aisvCtiCiselnikUdaju.pdf.

V rámci těchto služeb bude systém načítat číselníky potřebné pro načtení dat z ROS, ROB či RUIAN. Jde například o následující číselníky:

- Číselník_právních_forem_ROS,
- Číselník právních vztahů,
- Číselník_typů_datových_schránek.

Systém bude v rámci jobu stahovat číselníky a také logovat tuto činnost tak, aby bylo možné v rámci Administrační konsole kontrolovat, kdy došlo ke stažení číselníků a jaká data byla aktualizována.

Rozpad Usecase:

Backend zpracování				
	SUC	L		Dořešení časového omezení souhlasů se zpracováním osobních údajů (převzaté informace z NIA pro uživatele)
	SUC	M		Zpracování aktualizace subjektů - obecně, notifikační služba základních registrů - základní změny
	SUC	XL		Zpracování následnictví: Fůze, Splity na základě informace z ROS
	SUC	L		Zpracování přerušení podnikání, obnovení podnikání na základě informace z Živnostenského podnikání (nebo ROS)
	SUC	L		Zpracování změn statutárních orgánů
	SUC	L		Zpracování změn kontaktů FO (na základě FOP)

	SUC	S		Joby pro stažení číselníků a identifikace a verzování změn v číselnících
	SUC	M		Joby pro komunikace s FKVZ, MS2021+
	SUC	S		Joby pro interní přepočty
	SUC	M		Joby při ETL
	SUC	S		Joby pro notifikace kontrolních orgánů
	SUC	S		Joby pro notifikace zástupců podnikatelů
	SUC	L		Joby pro notifikační služby ROS
	SUC	L		Joby pro notifikační služby ROB

5.29. Dopady projektu do MPO

Organizační dopady na MPO:

- Pověření pracovníků pro péči o systém včetně zajištění jejich kapacity pro provádění Business administrace systému,
- Zajištění návaznosti na infolinku/helpdesk pro pracovníky MPO,
- Zajištění návaznosti na infolinku/helpdesk pro podnikatele využívající jiné veřejné informační systémy MPO (portál podnikatele, DIP, BusinessInfo …).

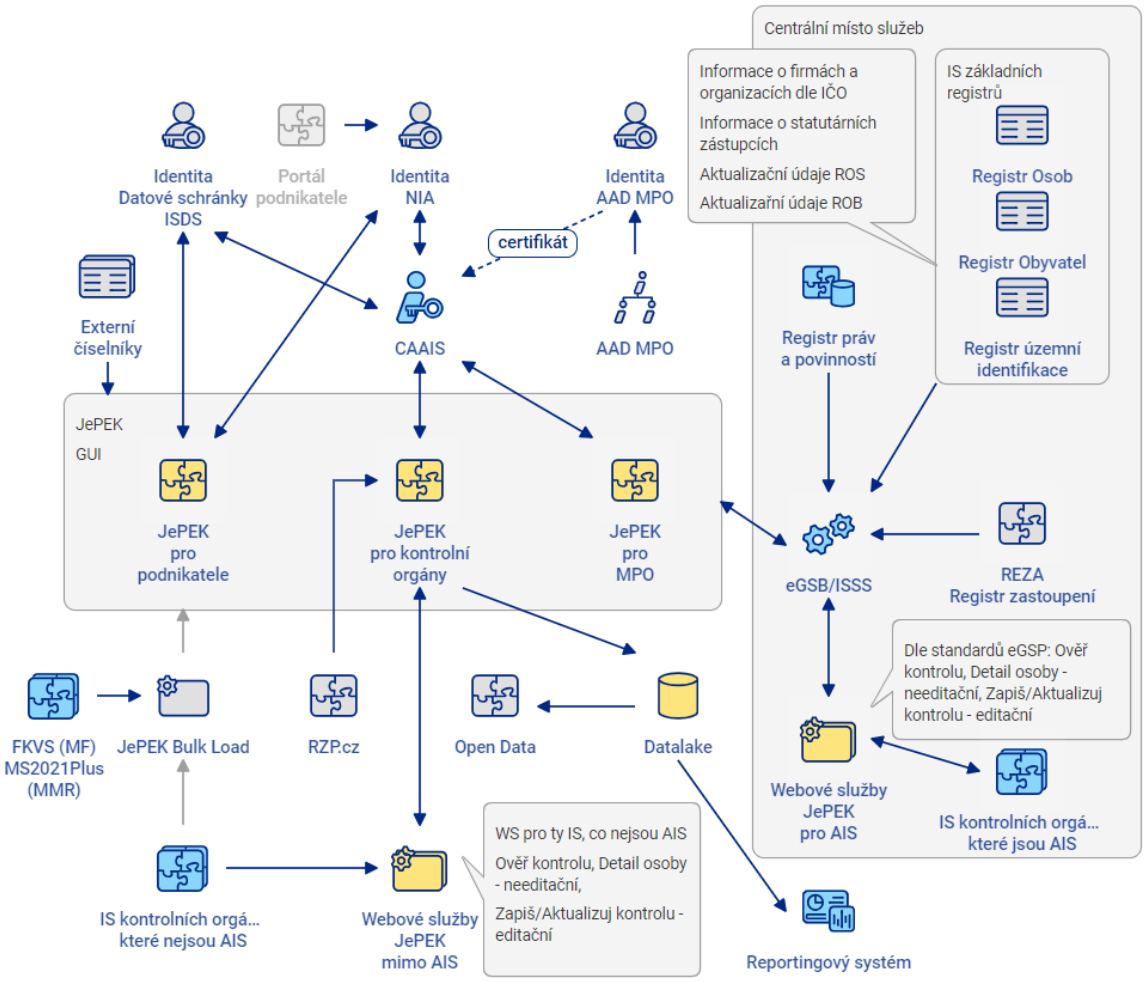
6. APLIKAČNÍ ARCHITEKTURA

Následující kapitoly obsahují způsoby využití informačních systémů a integrace na tyto systémy. Kapitoly zejména sumarizují dopady do těchto systémů a integraci s těmito systémy na úrovni datových toků.

6.1. Aplikační architektura

Systém JePEK bude rozdělen dle základního integračního schématu na mikroslužby (viz níže) a bude integrován jak na centrální místo služeb a státní registry, tak na infrastrukturní komponenty v rámci MPO.

!pozor na ZR se komunikuje přes ISZR a nikoliv přes ISSS.



6.2. CAAIS (JIP KAAS)

CAAIS je centrální autentizační a autorizační informační systém.

CAAIS je vytvořen v designu respektujícím jednotné prostředí gov.cz a přináší pokročilé služby, které usnadní uživatelům přihlašování do agendových informačních systémů jako je JePEK.

Autentizační a autorizační služby v CAAIS jsou na principu tzv. federačního hubu, který umožňuje připojení dalších poskytovatelů identit, kdy ale napojení na jiného poskytovatele není předmětem implementace další verze systému JePEK.

Systém CAAIS v průběhu projektu postupně nahradí systém tzv. JIP/KAAS, se kterým je zpětně kompatibilní.

Systém JePEK bude potřebovat následující nastavení pro kooperaci se systémem CAAIS:

- Zavedení (nebo sdělení) lokálního administrátora za MPO,
- Zavedení (nebo sdělení) lokálního administrátora za kontrolní orgán, se kterým se nedomluví na tom, že administraci uživatelů bude zajišťovat za tento kontrolní orgán,
- Zavedení systému JePEK (případně převzetí informací ze systému RPP) do systému CAAIS,
- Převzetí činnostních rolí ze systému RPP.

6.3. Identita NIA

6.3.1. Identita pro pracovníky orgánů veřejné moci

O tom, zda se zaměstnanci orgánu veřejné moci mohou přihlašovat prostřednictvím NIA obecně k více informačním systémům, rozhoduje každý orgán veřejné moci sám. (Ale ne všechny informační systémy veřejné správy tuto možnost podporují.)

Systém JePEK bude podporovat převzetí identity ze systému CAAIS, a tím i možnost přihlášení uživatelům prostřednictvím NIA.

Zároveň dále bude moci kontrolní orgán nastavit práva jen pro některé zaměstnance, a tím efektivně umožnit práci v systému JePEK jen pro vybrané zaměstnance (například metodiky nebo vedoucí pracovníky).

Údaje, které JePEK získá, se nijak neliší od údajů, které získává při přihlášení pomocí účtu JIP, respektive CAAIS. Detailní seznam poskytovaných údajů lze nalézt v technické dokumentaci ke službám CAAIS či JIP/KAAS. Z osobních údajů se jedná o jméno a příjmení.

Pokud má konkrétní fyzická osoba účty u více orgánů veřejné moci, tedy kontrolních orgánů, je po přihlášení pomocí NIA vyzvána, aby si zvolila právě jeden z nich. JePEK se případně o existenci ostatních účtů nedozví.

6.3.2. Identita pro podnikatele

Identita NIA bude napřímo pro systém JePEK poskytovatel identity uživatele-podnikatele, a to na základě větší sady identitních prostředků (Mobilní klíč eGovermentu, NIA ID, BankID a další).

6.4. RŽP

Registr živnostenského podnikání nabízí možnost vyhledání subjektu podle předmětu zájmu, a tak pomůže kontrolnímu orgánu v plánování kontrol a vyhledávání podnikatelů podle více kritérií.

Systém JePEK bude napojen na službu popsanou v https://www.rzp.cz/verejne-udaje/cs/o-sluzbe.

6.5. ISDS

ISDS (Integrovaný systém datových schránek) bude k dispozici jako poskytovatel identity pro podnikatele vedle NIA státních identitních prostředků.

ISDS nabízí řadu služeb, které umožňují bezpečnou identifikaci uživatelů a jejich autorizaci pro přístup k různým systémům a službám. Pokud externí aplikace potřebuje převzít identitu uživatele ze systému datových schránek, využívá se především mechanismu autentizace.

Základní principy autentizace v ISDS:

- Jednotné přihlášení (Single Sign-On, SSO): Uživatel se přihlásí jednou do ISDS a následně může přistupovat k různým spojeným aplikacím bez opakovaného zadávání přihlašovacích údajů.

- Otevřené standardy: ISDS podporuje otevřené standardy pro autentizaci, jako je například SAML 2.0, což umožňuje snadnější integraci s různými systémy.
- Různé úrovně zabezpečení: ISDS nabízí různé úrovně zabezpečení pro autentizaci, což umožňuje přizpůsobit se různým požadavkům na bezpečnost.

Služby ISDS pro převzetí identity uživatele:

- SAML 2.0 Identity Provider (IdP): ISDS působí jako poskytovatel identity (IdP) a vydává bezpečnostní tokeny (SAML assertion), které obsahují informace o autentizovaném uživateli. Externí aplikace (Service Provider, SP) pak tyto tokeny ověřuje a získává tak informace o uživateli.
- REST API: ISDS poskytuje REST API rozhraní, které umožňuje programové přístupy k různým funkcionalitám systému, včetně autentizace. Externí aplikace může využívat toto API pro získání informací o uživateli nebo pro správu uživatelských účtů.
- OAuth 2.0: ISDS může podporovat také protokol OAuth 2.0 pro delegaci přístupu. Tento protokol umožňuje uživateli udělit externí aplikaci oprávnění k přístupu k jeho datům v ISDS.

Příklad: Systém JePEK bude využívat systém Oauth 2.0 v režimu Authorization Code Grant: Uživatel je přesměrován na autorizační server ISDS, kde udělí oprávnění k přístupu k jeho datům. Následně je aplikace přesměrována zpět s autorizačním kódem, který může vyměnit za access token.

Konfigurace na straně ISDS

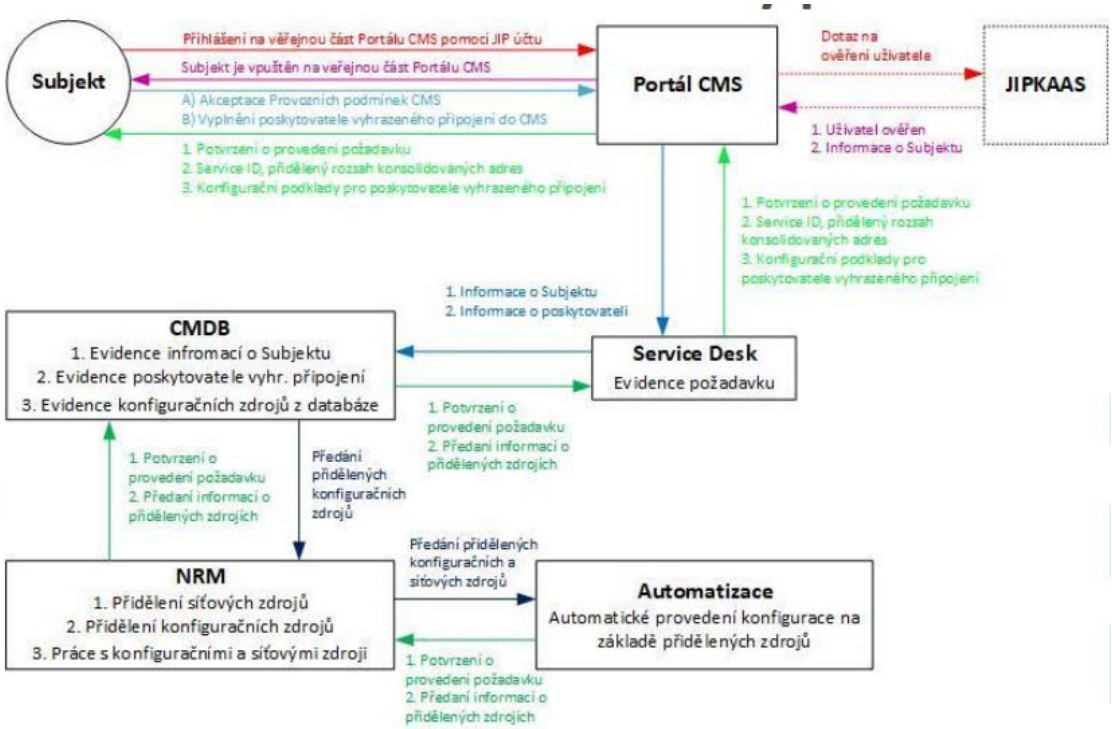
- Registrace aplikace: Každá externí aplikace, která chce využívat služeb ISDS, musí být v systému zaregistrována. Při registraci se obvykle zadávají informace jako název aplikace, popis, URL pro přesměrování po úspěšné autorizaci (redirect URI) a další relevantní údaje.
- Definice scope: Je nutné definovat, jaká oprávnění může aplikace požadovat. Scope určuje, k jakým informacím o uživateli bude mít aplikace přístup (např. jméno, příjmení, e-mailová adresa).
- Konfigurace grant typů: Vybere se vhodný grant typ (např. authorization code, implicit, client credentials) v závislosti na typu aplikace a požadovaném pracovním toku.
- Nastavení klíčů a tajemství: Aplikaci jsou přiděleny klientské ID a klientské tajemství, které slouží k identifikaci aplikace při komunikaci s ISDS.

6.6. CMS

CMS je systém, jehož primárním účelem je zprostředkovávat bezpečné, řízené a evidované propojení informačních systémů subjektů OVS a OVM ke službám (aplikacím), které poskytují informační systémy jiných subjektů OVS a OVM – přístup ke službám eGovernmentu.

Poznámka, pro infrastrukturní část se někdy používá termín KIVS-komunikační infrastruktura veřejné správy.

CMS je centrální funkční celek skládající se ze dvou částí: bezpečnostních prvků CMS samotného a vyhrazeného připojení poskytovaného jak komerčními, tak nekomerčními poskytovateli připojení. CMS spolu se sítí tvořenou vyhrazenými přípojkami tvoří oddělenou, bezpečnou a na síti Internet nezávislou infrastrukturu. To znamená, že je tato infrastruktura nejen odolná proti kybernetickým hrozbám, ale také v případě výpadku sítě Internet udrží komunikaci OVS a OVM na služby eGovernmentu.



V rámci napojení systému JePEK na státní registry musí být systém JePEK zařazen do CMS (verze 2 respektive 2.5 tak, jak bude k dispozici v okamžiku realizace projektu).

Napojení bude mít dvě roviny: logická a fyzická.

- Logická rovina: Zavedení systému JePEK jako takového bude součástí ohlášení v rámci RPP. Pokud bude ohlášení systému přijato, pak bude zaveden do security části CMS, systému RPP a jako ISVS.
- Fyzická rovina – stav napojení JePEK na CMS2 po infrastrukturní rovině: (na základě dohody s odborem informatiky) JePEK bude provozován v cloudu a napojení na CMS2 bude provedeno formou virtuální privátní sítě. MPO zprostředkuje žádosti pro připojení do CMS2.

Kroky zpřístupnění:

1. Ověření registrace správce JePEK v RPP,
2. Definice lokálních administrátorů v CAAIS,
3. Akceptace provozních podmínek a zřízení přístupu správce JePEK do CMS,
4. Definice uživatelů pro využívání prostředků:
    a. Neveřejné části AIS RPP působnostního (správcem je Ministerstvo vnitra) – již splněno.
    b. Portálu CMS (správcem je NAKIT).
    c. Service Desk DIA (správcem je DIA), kterou použije MPO pro nahlášení chyb spojených s následujícími oblastmi:
        i. Přístupy do Základních registrů,
        ii. Působnost v agendách,
        iii. Nefunkčnost eGON služeb,
        iv. Problémy SEP a IdP.
    d. RAZR (správcem je DIA).
        i. Registrační autorita základních registrů RAZR je webová aplikace, kterou subjekty oprávněné k přístupu do základních registrů používají k žádosti o přístup do základních registrů pro své informační systémy.
        ii. RAZR vyřizuje žádosti o přístup do produkčního i testovacího prostředí základních registrů. Certifikáty vydané pro přístup do základních registrů lze používat i pro využívání služeb produkčního i testovacího prostředí ISSS.

5. Oznámení výkonu agendy JePEK správcem JePEK v RPP,
6. Registrace AIS v RPP – částečně připraveno,
7. Připojení JePEK k CMS (2 nebo 2.5),
8. Registrace JePEK v RAZR v jednotlivých krocích,
9. Nasazení JePEK v různých fázích k CMS, ISSS, ISZR a tyto fáze v RAZR dokumentovat.

6.7. eGSB/ISSS

eGSB/ISSS je zkratkou pro e-goverment service bus respektive informační systém sdílené služby, který zpřístupňuje data státních registrů a vybraných agendových informačních systémů. Jde o technologickou komponentu v rámci CMS, která plní i další úlohy typicky tvořené technologií middleware a to řízení přístupu, nepopiratelnosti užití, informovanost, auditovatelnost, žurnálování a podobně.

Přístup je řízen systémem RPP, kde musí být schválen a uveden relevantní zákonný důvod pro užívání eGON služeb a případně dat jiných AIS.

Kromě čtení dat základních registrů bude systém vystavovat několik webových služeb, respektive metod formou publikace datových kontextů.

6.8. RPP

Registr práv a povinností (RPP, celý název je základní registr agend, orgánů veřejné moci, soukromoprávních uživatelů údajů a některých práv a povinností) slouží jako zdroj údajů pro informační systémy základních registrů při řízení přístupu uživatelů k údajům v jednotlivých registrech a agendových informačních systémech.

Součástí projektu bude aktualizace ohlášení systému JePEK tak, aby byly pokryty správně:

- Činnostní role,
- Vystavené služby a k nim nastavený přístup pro relevantní kontrolní orgány – a také udržování tohoto napojení aktuální s tím, jak bude pokračovat zapojování kontrolních orgánů,
- Využití jednotlivých údajů základních registrů systémem JePEK.

Dále pro publikaci služeb bude potřeba zajistit:

- Registraci administrátora JePEK v RPP, což se provádí žádostí poslanou datovou schránkou na DIA. Tento krok zajistí MPO,
- Potvrdit statutárním zástupcem MPO (v Katalogu OVM) na adrese https://rpp-ais.egon.gov.cz/AISP/verejne/, že správce JePEK je evidovaný v RPP.

6.9. ISZR

ISZR zajišťuje integritu, zabezpečuje komunikaci s relevantními informačními systémy veřejné správy, zajišťuje aktuálnost dat, bezpečné sdílení dat mezi jednotlivými úřady, možnost výměny dat s ostatními členskými zeměmi EU, oprávněný přístup občanů k údajům uvedených v registru a sdílení dat takovým způsobem, který umožní jejich efektivní pořizování a sdílení s odpovídající mírou zabezpečení přenášených dat a požadovanou dostupností služeb.

Informační systém základních registrů poskytuje komplexní služby definované v katalogu eGON služeb. Tyto služby nad základními registry poskytuje všem subjektům s ohledem na jejich aktuální oprávnění v registru práv a povinností:

- Publikuje služby základních registrů (eGON služby),
- Ověřuje oprávnění pro přístup do základních registrů,
- Zaznamenává a ukládá všechny logy do základních registrů.

Rozhraní Informačního systému základních registrů je realizováno na technologii Komunikační infrastruktury veřejné správy (KIVS) s bezpečnostními prvky poskytovanými CMS2.

Protože JePEK bude využívat více služeb základních registrů je nutné, aby se stal agendovým informačním systémem, což bylo zajištěno v první fázi projektu zavedením registrace systému JePEK do RPP. Součástí dalších

fází projektu bude aktualizace této registrace na detailnější úroveň podle toho, jak bude systém JePEK detailně navržen a naprogramován.

Dále bude JePEK registrován v RAZR dle postupu uvedeného u systému CMS.

6.10. ROS

Základní registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci, zkráceně registr osob (dále též „ROS“), slouží k evidenci osob uvedených v § 25 zákona č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů a jejich referenčních údajů uvedených v § 26 ZZR, např. údajů o statutárních zástupcích a provozovnách. Jednoznačný identifikátor osoby v ROS, identifikační číslo osoby (IČO), přidělují editoři údajů osob v agendách, které editoři i osoby vykonávají. Systém JePEK bude připojen k systému ROB prostřednictvím eGON služeb vystaveným ISZR na eGSB/ISSS.

Systém JePEK bude data využívat ke dvěma účelům:

1. K určení, firem a k nim evidovaných kontrol, které může vidět přihlášený uživatel.
2. K možnosti zadání kontroly na podnikatele, případně jeho provozovnu.

6.11. REZA

Registr zastoupení je dalším ze státních registrů zjednodušující administraci a ověřování zastupování právnických a fyzických osob.

REZA je, který implementován jako modul Registru Práv a Povinností, eviduje NĚKTERÁ oprávnění k zastupování. Systém poskytuje referenční údaje o evidovaných oprávněních k zastupování - standardizovaný vztah dvou osob z ROB/ROS, který popisuje právo zastupujícího jednat jménem zastupovaného. Systém bude obsahovat:

- Implicitní vztahy – takový vztah, který vyplývá z údajů evidovaných v informačních systémech veřejné správy a které nelze jednostranně zrušit ze strany zastupovaného,
- Explicitní vztahy – z vůle zastupovaného (typicky plná moc) – lze jednostranně zrušit ze strany zastupovaného.

Kromě vlastního registru (backend funkčnosti) systému REZA bude řešení obsahovat i AIS ReZa - agendový informační systém ve správě DIA, zapisující údaje do registru ReZa, současně i spravuje historii, šablony a evidenci certifikátů.

Systém JePEK bude využívat vybrané implicitní vztahy typu zastupování nezletilých nebo evidovaná zastupování firem.

Zároveň v rámci systému ReZA bude systém JePEK evidovat vlastní agendu k zastupování osob z ROB tak, aby zajistila možnost evidence plných mocí k zastupování pro používání systému JePEK.

Požadavky na systém REZA a AIS REZA:

- Zajištění přístupu (prostředky eGSB/ISSS),
- Vytvoření vlastní JePEK šablony v rámci AIS REZA.

6.12. MS2021+

Monitorovací systém MS2021+ je určen pro žadatele/příjemce pro zadávání žádostí o podporu a správu projektů po celou dobu jejich životního cyklu pro programové období 2021–2027.

V rámci systému jsou evidovány, plánovány a zaznamenávány desetitisíce kontrol, které budou převedeny do systému JePEK tak, aby mohly být použity jako základ pro koordinaci dalších plánovaných kontrol od kontrolních orgánů, které budou systém JePEK používat.

Systém MS2021Plus:

- bude pro systém JePEK poskytovat na eGSB/ISSS publikovat kontext (s plánovanými a realizovanými kontrolami,

- systém JePEK bude v pravidelných intervalech načítat tento kontext a změny propagovat do vlastní databáze.

Systém JePEK bude ale evidenční záznamy o kontrolách z MS2021+ zpracovávat odlišným způsobem než evidenční záznamy o kontrolách ze systémů jiných kontrolních orgánů. Tyto evidenční záznamy budou převzaty jako autoritativní data, a nikoliv jako kontroly, které jsou předmětem koordinace a na které se vztahují pravidla datové kvality či notifikací.

6.13. FKVS

Informační systém FKVS slouží k podpoře provádění a vyhodnocování finančních kontrol dle zákona č. 320/2001 Sb., o finanční kontrole v platném znění, a dle vyhlášky Ministerstva financí č. 416/2004 Sb., kterou se provádí zákon o finanční kontrole.

Pro kooperaci se systémem JePEK je relevantní modul MKP – Modul koordinace plánování veřejnosprávních kontrol veřejné finanční podpory. V rámci tohoto modulu dochází k dílčí koordinaci a plánování kontrolních akcí poskytovatelů veřejné finanční podpory.

Systém FKVS:

- bude pro systém JePEK poskytovat exportní soubor (alternativně zapisovat změny prostřednictvím webové služby) s plánovanými a realizovanými kontrolami,
- odesílat exportovaný soubor ke zpracování do systému JePEK.

Systém JePEK bude ale evidenční záznamy o kontrolách z FKVS zpracovávat odlišným způsobem než evidenční záznamy o kontrolách ze systémů jiných kontrolních orgánů. Tyto evidenční záznamy budou převzaty jako autoritativní data, a nikoliv jako kontroly, které jsou předmětem koordinace a na které se vztahují pravidla datové kvality či notifikací.

6.14. CzechPoint

Czech POINT (Český Podací Ověřovací Informační Národní Terminál) je projekt, který usnadňuje komunikaci občanů s veřejnou správou. CzechPoint automatizuje množství akcí kontaktu mezi občany a státní správou.

Systém JePEK bude ze systému CzechPoint využívat část číselníků, které použije pro svoji činnost. Automatizace aktualizace číselníků bude zajištěna funkčností systému JePEK. Není tedy požadavek na úpravy nebo konfigurace systému kromě informování o případných změnách číselníků, což ale nebude automatizováno, jen bude pracovníky MPO systém JePEK ohlášen jako odběratel veřejných dat CzechPoint.

6.15. Reportingový nástroj - Business inteligence

Reportingový nástroj bude použit pro realizaci:

a) Sledování business použití systému JePEK – Business kokpit,
b) Statistického zpracování údajů o kontrolách a použití systému JePEK – analytické studio,
c) ETL procedury z db JePEK do datového úložiště DataLake,
d) OLAP datové kostky.

Účel a základní popis:

Navrhovaný reportovací nástroj bude sloužit k analýze a vizualizaci dat získaných z Jednotného portálu evidence kontrol (JePEK), který umožňuje koordinaci kontrol podnikatelských subjektů. Nástroj bude zajišťovat přehledné zpracování dat pro potřeby Ministerstva průmyslu a obchodu (MPO). Hlavní funkcionalitou bude filtrování, třídění a zobrazování kontrolních dat v různých kategoriích a časových obdobích.

Klíčové vlastnosti reportovacího nástroje:

1. Třídění a filtrování dat:

- Podle regionu: Okresy, kraje, nebo specifické geografické oblasti.
- Podle stavu kontroly: Plánované, probíhající, ukončené.
- Podle druhu kontroly: Například finanční, hygienická, živnostenská apod.

- Podle výsledku: Úspěšné, neúspěšné, s nálezy nebo bez nich.
- Podle subjektu: Filtrace na úrovni jednotlivých podnikatelských subjektů nebo provozoven.

2. Vizualizace dat:

- Interaktivní grafy (např. sloupcové grafy, koláčové diagramy) pro zobrazení:
    - Počtu kontrol v čase.
    - Podílů se zjištěním vs. bez zjištění kontrol.
    - Regionálních statistik.
- Tabulkový výstup pro přehledné zobrazení detailů o jednotlivých kontrolách.

3. Export a sdílení dat:

- Export reportů ve formátech PDF, XLSX nebo CSV pro sdílení s ostatními pracovníky či institucemi.
- Možnost zasílání reportů přes e-mail přímo z aplikace.

4. Monitorování a notifikace:

- Možnost automatické notifikace při překročení doporučeného počtu kontrol v dané provozovně.
- Upozornění na konflikty plánovaných kontrol různými orgány.

5. Historie a archivace:

- Ukládání kompletní historie kontrol pro jednotlivé podnikatelské subjekty.
- Přístup k archivovaným výsledkům kontrol i po jejich ukončení.

Technické aspekty:

1. Datová propojení:
    - Automatické napojení na informační systém JePEK, který poskytuje data o koordinaci kontrol.
    - Možnost integrace s dalšími systémy kontrolních orgánů přes API.
2. Uživatelské rozhraní:
    - Webová aplikace s intuitivním uživatelským rozhraním přístupná z počítače i mobilních zařízení.
    - Rozdělení funkcionalit podle uživatelských rolí (např. administrátor, kontrolor, analytik).
3. Bezpečnost a přístup:
    - Šifrovaný přístup k citlivým údajům.
    - Přístup na základě oprávnění podle rolí.

Objednatel dále sděluje, že výše navrhovaný reportovací systém nemusí být vyvinut jako nové řešení a pro tyto účely je možné využít standardně dostupných nástrojů, které se pro obdobný druh práce využívají – pro účely reportingu a statistického vyhodnocení mohou být využity nástroje BI umožňující online propojení na zdrojová data.

6.15.1. Business kokpit

Business kokpit slouží pracovníkům business podpory systému JePEK:

- Ke sledování použití systému JePEK,
- Vyhodnocování retence dat systému JePEK,
- Souhrnnému sledování datové kvality systému JePEK,
- Ke získání přehledu o indikátorech koordinovanosti kontrol,

a to vše v dimenzích dnů, kontrolních úřadů, respektive jejich organizačních útvarů, s možností hierarchického rozpadu až na uživatele.

V rámci Reportingového nástroje budou realizovány následující úpravy:

1. Nový dashboard/kokpit pro Business podporu systému obsahující portlety,

2. Nový datasource navázaný na databázi, do které budou odlévána data z produkční databáze o použití systému JePEK,
3. Zavedení uživatelů běžně v roli Business podpora systému JePEK.

6.15.2. Statistické zpracování - analytické studio

Systém JePEK bude datovým zdrojem pro výstupy v rámci ad-hoc přístupu k informacím (zpracování odpovědi na externí požadavek na MPO) a též jako pro publikační a prezentační činnosti MPO (MPO dle své vůle prezentuje vlastní činnosti). Obecně pro vybrané uživatele MPO bude použit reportingový systém jako platformní služba nad datovou kostkou (viz dále).

Uživatelům v rámci MPO bude reportingový systém zpřístupněn na základě žádosti a schválení uživatelských práv i rolí. Reportingový systém bude napojen na CAAIS, nebo MPO-AAD, anebo bude mít správu uživatelů stanovenu na základě architektonického rozhodnutí o způsobu správy a použití příslušného reportingového systému v MPO, což ale není součástí projektu JePEK.

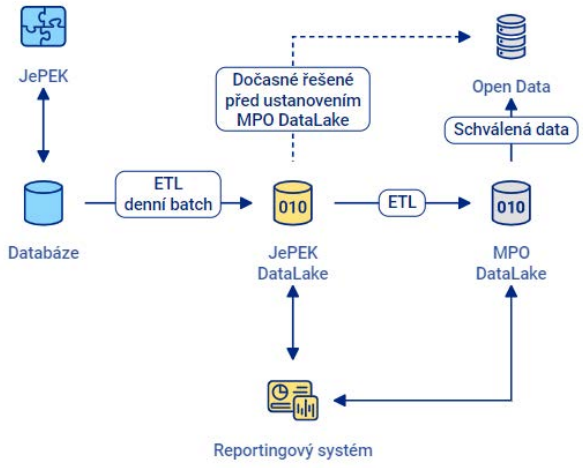
6.15.3. Příprava dat pro OpenData

V rámci ETL z databáze JePEK do Datalake proběhne transformace dat z systému JePEK na bázi denních extraktů do OLAP datové kostky, aby tato mohla být využita jak pro potřeby Open dat, tak pro potřeby ad hoc statistického zpracováním v rámci analytického studia.

6.16. NKOD a OpenData

MPO zajistí publikaci vybraných zpracovaných výstupů BI řešení (součástí řešení bude základní transformace) v rámci Národního katalogu otevřených dat (NKOD), a to formou publikačního plánu dle ministerského vzoru, a tedy dle zákona č. 106/1999 Sb. povinně zakategorizuje publikovaná data. Publikační plán podléhá povinnému schválení vedení MPO.

Zároveň MPO zajistí zpřístupnění open dat (deskriptivní data o kontrolách a jejich koordinaci) pro účely obecného zpracování uživateli open dat.



Principy zpřístupnění dat vycházejí z toho, že sám systém JePEK stanovuje podmínky pro zobrazení konkrétních dat konkrétním osobám a konkrétním firmám, což ale v případě zpřístupnění dat formou reportingového systému lze jen obtížně zajistit. Ale předzpracovaná statistická data v členění dle více dimenzí, například dle oboru podnikatelské činnosti, územního členění, časového intervalu, typů kontroly, kontrolních úřadů a též kategorií doby trvání a podobně, bude možné zveřejnit.

Data budou zpřístupněna ve formě datové kostky s hierarchickými dimenzemi a předpočítanými bazálními faktovými údaji.

6.17. Integrovaný systém kontrolního úřadu

Integrovaným systémem kontrolního úřadu je jakýkoliv systém kontrolního úřadu, který se bude integrovat na systém JePEK.

Systém JePEK bude mít principiálně dvakrát vystavená rozhraní:

- C-Rozhraní na eGSB/ISSS, které bude k dispozici pro ty kontrolní orgány, jejichž informační systémy (k integraci s JePEK) běží výhradně v rámci CMS2,
- I-Rozhraní, kdy příslušné webové služby vystavuje přímo systém JePEK pro ty kontrolní orgány, jejichž informační systémy neběží v rámci CMS2.

JePEK bude vystavovat několik webových služeb s patřičným zabezpečením. Na vedení kontrolního orgánu, který se bude integrovat na systém JePEK, bude rozhodnutí, kolik z těchto webových služeb bude integrovat. Pokud nebude možné v rámci C-Rozhraní publikovat přímo webové služby, pak bude systém JePEK publikovat přímo kontexty.

Nabízené webové služby:

- čtiKontrolydleIC - Prohlížení kontrol subjektu,
- čtiDetailKontroly - Načtení detailu kontroly dle vybraných identifikátorů,
- ověřKontrolu - ověření, zda kontrola daného typu v daném termínu na dané adrese má nebo nemá konflikty,
- zapišKontrolu – Inspection - Zapíše novou, respektive aktualizuje stávající kontrolu.

Rozpad Usecase:

Konzumovaná rozhraní/Systémy				
	INTG	M		ISZR - více služeb
	INTG	L		ROS - více služeb
	INTG	M		RUIAN
	INTG	0		RŽP - více služeb
	INTG	M		eGSB - více kontextů/služeb
	INTG	L		CAAIS služby - více služeb
	INTG	M		NIA služby - více služeb
	INTG	M		ISDS služby
	INTG	M		Email - odeslání
	INTG	M		REZA - více služeb
	INTG	M		PowerBI prostřednictvím DataLake
	INTG	S		Stažení číselníků CzechPointu
	INTG	S		Stažení číselníků ISZR
	INTG	M		Kontroly z FKVZ
	INTG	M		Kontroly Z MS2021+
	INTG	M		OpenData - řádově nižší desítky ETL
	INTG	M		Technické integrace na služby cloudového poskytovatele - jako monitoring, zálohování,
	INTG	L		DataLake - řádově vyšší desítky ETL

Poskytované služby				
	INTG	S		WS: Monitoring - Keep up
	SUC	L		WS: Vyhledání klienta na částečnou shodu, rychlé vyhledání subjektu (vrací i zapsané pobočky s adresními místy)
	SUC	L		WS: Načtení klienta s kontrolami - dle IČO/DIČ/RČ resp IČO/DIČ/IČO a IČP dostane seznam plánovaných i historických kontrol
	SUC	M		WS: Načtení individuální kontroly dle ČJ, identifikace kontroly dle KO, interního čísla kontroly
	SUC	L		WS: Ověř kontrolu sdělí informace o vhodnosti/nevhodnosti naplánovat kontrolu na daný čas vzhledem k probíhajícím kontrolám
	SUC	L		WS: Zapiš kontrolu (historickou i dopřednou)
	SUC	L		WS: Aktualizuj kontrolu (historickou i dopřednou), realizováno jako insert/update včetně verzování
	SUC	L		eGSB Kontext: Vyhledání klienta na částečnou shodu, rychlé vyhledání subjektu (vrací i zapsané pobočky s adresními místy)
	SUC	L		eGSB Kontext: : Načtení klienta s kontrolami - dle IČO/DIČ/RČ resp IČO/DIČ/IČO a IČP dostane seznam plánovaných i historických kontrol
	SUC	M		eGSB Kontext: : Načtení individuální kontroly dle ČJ, identifikace kontroly dle KO, interního čísla kontroly
	SUC	L		eGSB Kontext: : Ověř kontrolu sdělí informace o vhodnosti/nevhodnosti naplánovat kontrolu na daný čas vzhledem k probíhajícím kontrolám
	SUC	L		eGSB Kontext: : Zapiš kontrolu (historickou i dopřednou)
	SUC	L		eGSB Kontext: : Aktualizuj kontrolu (historickou i dopřednou), realizováno jako insert/update včetně verzování
	INTG	L		Vystavení služeb v rámci eGSB/ISSS v rámci CMS2 (pro AIS bez "přístupu k internetu")
	INTG	L		Vystavení služeb v mimo CMS2 pro neagendové AIS

6.18. DIP – Databáze informačních povinností

Systém JePEK bude obsahovat sám o sobě odkazy do DIP, a to ve dvou rovinách:

- Obecně - z hlavní stránky přehledu/dashboardu v JePEK zase obecně na DIP hlavní stránku,
- Specificky - z informace o detailu Typu kontroly, kde bude uvedena informace o konfigurovaných právních předpisech. Pokud je takový předpis již zpracován v rámci systému DIP a zároveň existuje v rámci DIP možnost prokliku na tento právní předpis (deeplink), nebo možnost prokliku na vyhledání konkrétního předpisu, pak systém JePEK bude obsahovat proklik do DIP.

6.19. Portál podnikatele

Systém JePEK bude jedním ze systémů poskytujících údaje na/pro Portál podnikatele.

Jelikož však k datu tvorby dokumentace nejsou přesné technické specifikace Portálu podnikatele vyjasněny, předpokládáme, že Portál podnikatele bude typu rozcestník, tedy bude obsahovat link (deeplink) na systém JePEK. Po kliknutí na takový link, pokud bude uživatel vůči Portálu podnikatele autentizován, pak uživatelova identita bude předána do systému JePEK, a tedy nebude nutné provést novou autentizaci vůči systému JePEK, ale JePEK bude pracovat s převzatou identitou z Portálu podnikatele.

Předpokládáme rovněž i opačné propojení, a to v rámci odkazů ať již příslušného portletu v rámci systému JePEK, nebo klikatelnou ikonou v rámci pásu klikatelných log na jiné systémy a řešení poskytovaná MPO.

Pokud by se Portál podnikatele v průběhu času stal skutečně portálovým řešením podle standardů JSR 168, JSR 186/286 a zároveň by vyvstal požadavek na realizaci portletu s vystihujícím obsahem, pak by vytvoření portletu bylo předmětem projektu tvorby nebo údržby Portálu podnikatele ale vytvoření obsahu takového portletu by bylo předmětem změnového požadavku na systém JePEK.

Rozpad usecase:

Portál podnikatele				
	BUC	L		Obsah portálu pro podnikatele: Subjekt (možnost výběru z více), Subjekt-detail, Kontrola, Statistiky, Aplikace (About, nápovědy, odhlásit, přihlásit), Rychlé hledání
	BUC	M		Portlet odkazy: Do DIP, do BusinessInfo, do (skutečného) Portálu podnikatele
	BL	M		Konfigurace notifikací pro podnikatele
	SUC	M		Výpočet elementárních notifikací pro podnikatele
	SUC	M		Výpočet a odeslání groupových notifikací pro podnikatele

6.20. JePEK - Specifikace případů užití

Samotný systém JePEK bude zajišťovat podporu většiny (pokud není uvedeno jinak) business procesů uvedených v předchozí kapitole. Samotná funkčnost je popsána pomocí elementů jako jsou: případy užití, business logika, integrace a další elementy sdružené pod typ ostatní.
Případy užití a business logika jsou klíčové pro popis softwarových systémů a jejich interakce s uživateli a dalšími systémy.

Uživatelské usecases popisují interakce mezi uživatelem a systémem. Jde o to, co uživatel chce od systému dosáhnout a jakým způsobem. Tyto usecasy jsou zaměřené na chování systému z pohledu uživatele a zahrnují konkrétní akce, které uživatel provádí, aby dosáhl svého cíle.
Systémové usecases popisují vnitřní chování systému a to, co by systém měl udělat v reakci na akce uživatele. Od uživatelských usecases se liší tím, že jsou více zaměřené na technické detaily a procesy, které se odehrávají na pozadí.
Systém JePEK dekomponujeme na následující typy stavebních prvků:

- Uživatelské usecases se zaměřují na to, jak uživatel interaguje se systémem.
- Systémové usecases popisují, jak systém funguje na pozadí a co provádí.
- Business logika definuje, jak by měl systém fungovat podle obchodních pravidel.
- Integrace se týká propojení a komunikace mezi různými systémy nebo moduly.

7. Datová architektura řešení

Následující oblasti sumarizují základní datové struktury, které bude obsahovat plánované řešení JePEK. Datové struktury nejsou rozpracovány na úroveň atributů ani nutně neodpovídají implementačním relačním tabulkám, ale mají dokumentovat rozmanitost struktury persistovaných údajů tak, aby mohly být použity jako základ pro implementaci, kdy další detailizace je poplatná vybrané implementační technologii, která není v okamžiku tvorby tohoto dokumentu známa.

Následující kapitoly shrnují genezi a závěry z předpokládaného a dříve komunikovaného datového obsahu základních informací v JePEK.

7.1. Identifikované údaje kontroly

Identifikované údaje dle návaznosti na právní předpisy a potřeby systému JePEK. Tato a následující kapitoly upřesňují původně poskytnuté materiály k předpokládanému datovému obsahu kontroly, který vycházel z interpretace kontrolního řádu. V průběhu diskusí s kontrolními orgány došlo ke zjednodušení ve smyslu, že:

- ne všechny původně předpokládané informace budou povinné,
- jedna informace může být poskytnuta ve více podobách (například v čase, nebo v terminologii podle kontrolního úřadu, který data poskytuje),
- alternativní informace (tedy například zadám jen konec, nebo jen začátek, a pokud zná JePEK předpokládané trvání kontroly, pak si vypočítá druhé datum sám).

7.2. Název kontrolního orgánu

Označení kontrolního orgánu dle § 12 odst. 1 písm. a), Kontrolního řádu znamená identifikaci kontrolního orgánu, který provedl, provádí nebo hodlá provést kontrolu. Pokud byla kontrola provedena více kontrolními orgány v právním stavu integrované kontroly (§ 39, hlava VIII, zákona č. 224/2015 Sb., o prevenci závažných havárií způsobených vybranými nebezpečnými chemickými látkami nebo chemickými směsmi), pak jde o kontrolní orgán, který je pověřen koordinací.

Pokud jde o kontrolu koordinovanou jen na základě kontrolního řádu (dle § 25 Kontrolního řádu), pak tuto kontrolu nahlašuje každý kontrolní orgán samostatně.

7.2.1. Způsoby zadání informace o orgánu veřejné moci

7.2.1.1. Identifikace kontrolního orgánu, za který uživatel jedná

Uživatel je identifikován prostřednictvím CAAIS (původně JIP/KAAS). Informace o kontrolním orgánu jsou předány v procesu autentizace uživatele jako tagy:

<v2_1:ZkratkaSubjektu> a <v2_1:ICSubjektu>, kdy snazší pro potřeby JePEK je pracovat s IČ.

ZkratkaSubjektu reprezentuje zkratku subjektu přihlašujícího se uživatele. Jedinečný identifikátor subjektu v rámci JIP. IcSubjektu reprezentuje IČ subjektu dotazujícího se nebo žádajícího uživatele.

Pokud může uživatel reprezentovat více kontrolních orgánů nebo obecně i dalších orgánů veřejné moci, pak systém uživateli nabídne výběr z činnostních rolí, a tedy více orgánů veřejné moci. Uživatel si pro další práci vybere právě jeden orgán veřejné moci, který bude v následujících činnostech reprezentovat.

Pokud je uživatel identifikován jiným způsobem (náhradní, uživatelské), pak v případě volání jakéhokoliv usecase vyžadujícího znalost kontrolního orgánu, bude uživatel speciálním usecasem vyzván, aby vybral kontrolní orgán ze seznamu orgánů veřejné moci (vyhledávání na částečnou shodu v názvu, respektive podle IČO).

7.2.1.2. Při manuálním zadávání prostřednictvím XLS/CSV souboru

Nahrávání aktualizovaných dat o kontrolách bude probíhat prostřednictvím přihlášeného uživatele, a tedy od jeho přihlášení odvozeným kontrolním orgánem.

7.2.1.3. Při on-line integraci pomocí webové služby

Integrace formou webové služby bude probíhat přes systémové uživatele identifikované specifickým certifikátem a zavedené v technické konfiguraci systému. Tyto certifikátem reprezentovaní systémoví uživatelé budou konfiguračně nebo automaticky přiřazeni k orgánům veřejné moci tak, aby bylo vždy jasné, ke kterému orgánu patří a nemuselo se jen spoléhat na informace, kterou předá volající v requestu.

Je-li systémový uživatel zaveden, potom je zkontrolován soulad mezi kontrolním orgánem uvedeným v přijatém requestu a konfigurací. V případě nesouladu je kontrola zaevidována s referencí na kontrolní orgán v rámci requestu, ale ve stavu vyžadující zásah obsluhy (business administrátora systému).

7.2.1.4. Při on-line integraci formou dávkového přenosu

Uplatní se stejný princip jako v případě on-line integrace pomocí webové služby, ale navíc se provede křížová kontrola, zda odpovídá soulad mezi konfigurací u certifikátu a informacemi v přijatém souboru.

V případě nesouladu je kontrola zaevidována s referencí na kontrolní orgán v rámci souboru ale ve stavu vyžadující zásah obsluhy (business administrátora systému).

7.3. Označení kontrolované osoby – název, IČO, adresa sídla, adresa kontrolované provozovny

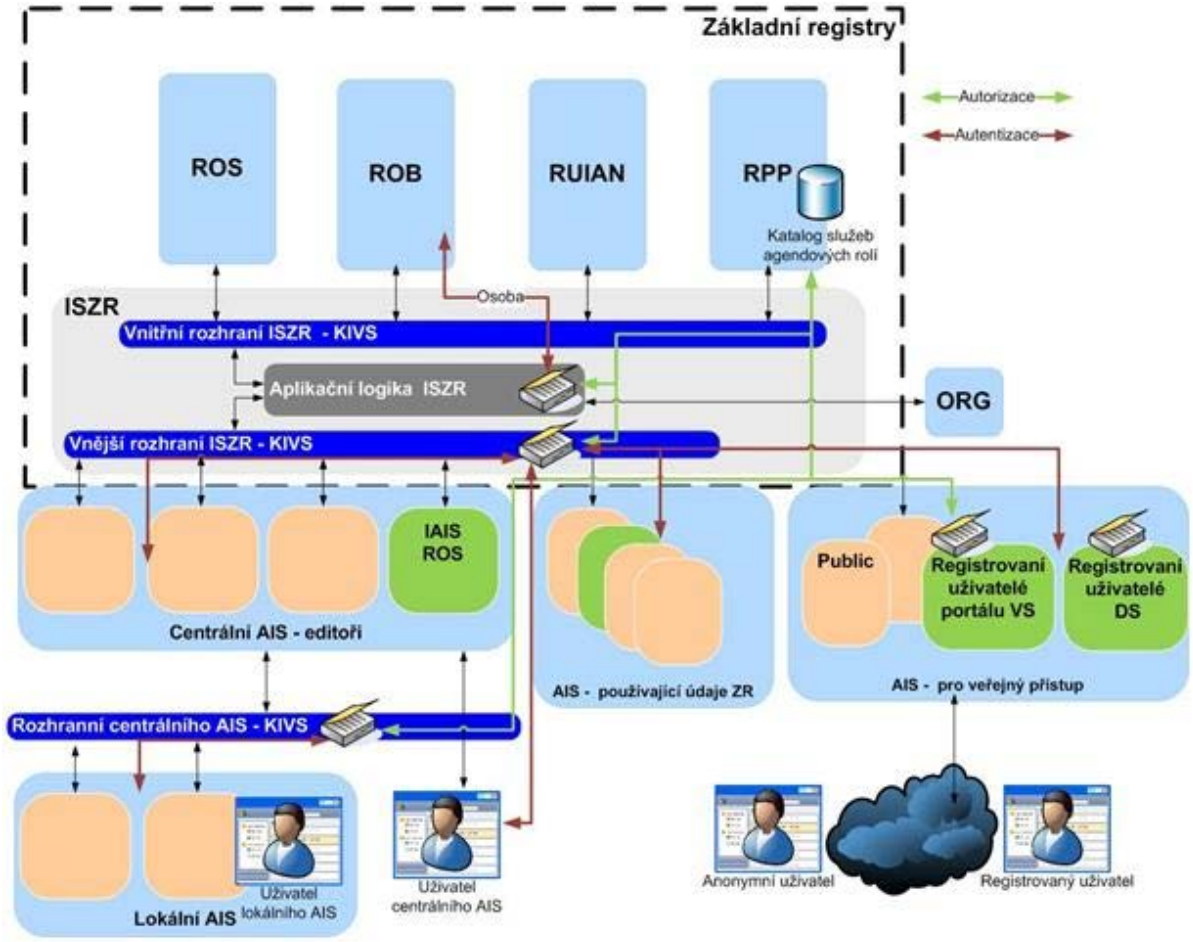
Označení kontrolované osoby dle §12 odst. 1 písm. d), Kontrolního řádu.

Systém JePEK bude pracovat zejména s identifikací IČO, a to včetně fyzických osob identifikovaných pomocí IČO a registrovaných zahraničních subjektů.

Kontroly subjektů neregistrovaných České republice budou sice v systému registrovány (pro účely statistiky dle počtu kontrol), ale nebudou ztotožňovány na příslušné právnické nebo fyzické subjekty kontroly registrovaných mimo Českou republiku.

Případné kontroly na subjekty identifikované dle DIČ (VAT ID) budou převedeny na identifikaci subjektu kontroly pomocí IČO nebo RČ.

Subjekty kontroly identifikované podle RČ (a nikoliv podle IČO) budou registrovány v JePEK jen pro potřeby statistických výstupů a uloženy budou pod náhradní anonymizovanou identitou dle principu dělené identity (více viz https://overeni.identitaobcana.cz/) tak, aby systém JePEK nespadal pod požadavky GDPR, kdy pro fyzické osoby nebude získávána a aktualizována informace z ROB pro potřeby zobrazování kontrolovaného subjektu z Registru obyvatel.



Výpočet ekonomicky spjaté skupiny pro potřeby výstupů JePEK bude proveden nikoliv na bázi primární evidence kontroly (kontrola probíhá na konkrétním subjektu), ale až na úrovni zpracování výstupu. Informace o kontrolách na celou skupinu budou evidovány i zobrazovány na GUI JePEK jen na úrovni primární evidence, zatímco pro zpracování dat JePEK na úrovni dalších výstupů bude možné kontroly ekonomicky spjatých skupin postihnout.

Informace o primárně kontrolovaném subjektu budou do systému JePEK dotaženy napojením na základní registr osob (ROS) vedený Českým statistickým úřadem (https://www.czso.cz/csu/czso/registr_osob) pomocí služby základních registrů "ČtiPodleÚdajů".

Načtena budou data o názvu právnické osoby, o sídle právnické osoby a také o složení statutárního orgánu, a to včetně odkazů do systému ROB. V rámci načtení právnické osoby (PO či FOP) systém načte jak informaci o vlastní PO, ale i o referencovaných FO v rámci statutárního orgánu.

Viz specifikace: https://www.szrcr.cz/cs/sluzby/spravci-a-vyvojari/vyvojari-agendovych-informacnich-systemu

Aktualizace informace z ROS:

Systém JePEK bude aktualizovat lokálně uložená data o právnických osobách-subjektech kontrol. Systém bude opakovaně načítat kompletní změny evidované v ROS. Načtené změny bude systém porovnávat s informacemi evidovanými v JePEK, a pokud bude změněná osoba evidována (ať již právnická, nebo fyzická - respektive reference na ni), pak bude systém aktualizovat uložené informace lokálně na základě předaných aktualizovaných údajů. Bližší informace viz https://www.szrcr.cz/images/dokumenty/v%C3%BDvoj%C3%A1%C5%99i/Spra%CC%81vny%CC%81_postup_pra%CC%81ce_s_notifikacemi_a_udrz%CC%8Covani_datoveho_kmene_nava%CC%81zane%CC%81ho_na_ROB_4.2023.pdf

7.3.1. Informace o provozovně

Vycházíme z označení kontrolované osoby dle § 12 odst. 1 písm. d), KŘ, provozovnu považujeme za součást označení kontrolované osoby.

Kontrola vždy probíhá na konkrétních místech. Jen minimum kontrolních orgánů pracuje s evidencí provozoven dle Živnostenského rejstříku (https://www.rzp.cz/jrf/cs/assets/help/web_zalozky/provozovny.html). Informace o provozovně bude možné hlásit do systému alternativně, a to buď pomocí čísla provozovny nebo pomocí adresy, případně oběma způsoby zároveň, kdy, pokud půjde ztotožnit číslo provozovny, pak se použije, pokud nepůjde ztotožnit podle čísla, pak se použijí údaje z předané adresy.

Údaje z adresy se systém pokusí **heuristickým způsobem ztotožnit** na adresu některé pobočky, kterou má firma registrovanou, případně na místo podnikání. Pokud dojde k heuristické unifikaci s více provozovnami nebo sídlem, pak přednost má provozovna před sídlem, jinak se vybere pobočka s nejvyšším unifikačním score.

Nedojde-li k identifikaci provozovny, potom se i tak údaje o místě uloží pro zobrazení na detailu kontroly, ale pro účely zobrazování se bude pracovat se sídlem kontrolované osoby. Businessově jde například o mobilní provozovny, tržiště a podobně, tedy se v případě neidentifikace nemusí jednat o chybu.

Pokud při hlášení kontroly není uvedeno místo kontroly, za místo kontroly pro účely zobrazování bude považováno sídlo kontrolované osoby.

7.4. Označení předmětu kontroly

Pro označení předmětu kontroly bude v rámci projektu připraven konfigurační číselník či sada číselníků, který bude obsahovat několik desítek položek ke konfiguraci předmětu kontroly ve vztahu k chování kontrol.

Předmět kontroly bude spojovat informace o:

- zákonném důvodu kontroly (vazba na paragraf zákona),
  - Název kontroly
  - Zkrácený název
  - Pravidelnost kontroly (tedy zda musí být provedena v nějakém časovém období)
  - Vynucenost kontroly (zda je konkrétní provedení kontroly přímou povinností a součástí kontraktu/licence/dotace)
  - Povinně koordinovaná kontrola
  - Identifikace právního předpisu
  - Název právního předpisu
  - Odkaz na právní předpis (MPO: businessinfo.cz)
  - Datumy novelizace
- Kategorizaci kontroly,
  - Místní
  - Dokladová/administrativní
  - Jiná
- Vazbách Typy kontrol (v případě rozvoje právního prostředí, které jsou předchozí a navazující typy kontrol):
  - na předchozí,
  - následující typy kontrol
- Vazbách na kontrolní orgány, které typ kontroly mohou provádět
- Vazbě na kontroly, které mají příbuzný účel kontroly (a tedy mají být plánovány ve stejný den jako jiné kontroly kontrolních orgánů)
- Kategorizaci dopředné viditelnosti kontroly (zda je viditelná všech včetně kontrolovaného subjektu, viditelní kontrolním orgánům, viditelná jen pro specifickou podmnožinu kontrolních orgánů, jen pro specifické subjekty (policie, celní správa, ...), jen pro samotný kontrolní orgán, jen pro hlásící organizační jednotku v rámci kontrolního orgánu (kdy kontrolní orgán utajuje kontroly i před jinými kontrolory v rámci sebe sama)

- Vazbě Dopředná viditelnost pro kontrolní orgány (tedy které KO mohou vidět kontrolu dopředu)-- specifická podmnožina KO pro čtení typu kontroly,
- Kategorizaci zpětné viditelnosti kontroly,
- Typických hodnotách provedení kontroly (použije se v případě neúplnosti dat od kontrolních orgánů, kdy typicky data nejsou ve strojově zpracovatelné podobě)
    - Typické trvání kontroly
    - Typická doba kontroly na místě u kontrolovaného
    - Typický interval mezi provedením “kontroly na místě, kdy je vyžadována součinnost kontrolovaného” a datumem protokolu.

Detailní popis je uveden v souboru:

> https://d.docs.live.net/a298b71527140d53/Dokumente/MPO_JePEK/DatModel/Jepek-Kontrola-Datmodel_v05-Kopie%20pro%20ČMI.xlsx

7.5. Kontrola zahájena na základě podnětu

Nahrazeno Kontrola ex-offo s odlišným (ale volně souvisejícím) významem.

Informace o podnětu nebude explicitně předávána. Nicméně na kontrole bude možné zadat informaci, zda jde o kontrolu ex-offo z rozhodnutí samotného kontrolního úřadu (tedy zda se rozhodl ke kontrole sám kontrolní orgán), ale uvedení této informace nebude povinné.

Předání informace bude možné všemi kanály systému JePEK: z GUI, z Excelu nebo prostřednictvím integrace na systém kontrolního úřadu. Dále pak bude možné odvodit informaci z typu kontroly.

Smyslem evidence atributu je odpověď na otázku, proč kontrolní orgán kontroluje (znovu, v tento termín, opakovaně, tak často atp.). Tedy pokud kontrolní orgán nezapíše své vlastní rozhodnutí (a tím ale přebírá odpovědnost za konflikt termínů nebo významnou frekvenci kontroly), pak může sdělovat, že kontrolu vykonat musel. Jaký je důvod toho, že kontrolu vykonat musel ale nesděluje.

Případná koordinace přes konflikty s obdobným významem se uplatní v případě, kdy se jedná o plánovanou kontrolu. Naopak příznak ex-offo se uplatní i v případě kontrol, které se do JePEK zapisují až zpětně.

7.5.1. Kontrola ve spolupráci s jiným kontrolním orgánem

Informace o vykonané kontrole ve spolupráci s jiným kontrolním orgánem nebude vyžadována, neboť informace:

- buď již známa z typu kontroly, neboť je zákonnou povinností některých typů kontroly tyto kontroly provádět v součinnosti například v případě prevence závažných havárií (https://www.e-sbirka.cz/sb/2015/224?zalozka=text) kontrola orgány integrované inspekce,
- nebo to je dáno místní a časovou shodou mezi kontrolami jednotlivých kontrolních orgánů,
- nebo jde o samostatné kontroly.

7.5.2. Zahájení kontroly

Z vazby na kontrolní řád je špatně rozlišitelná informace o kontrole z hlediska kontrolujícího orgánu a kontrole z hlediska kontrolované osoby nebo jiné osoby, tj. kontrolním úkonu, který reálně podnikatele zatěžuje. Datum skutečného zahájení může být:

1. Datum (doručení) oznámení o zahájení kontroly kontrolované osobě,
2. Datum kontrolní úkonu, jímž byla kontrola zahájena,
3. Datum předložení pověření ke kontrole kontrolované osobě nebo jiné osobě, která kontrolované osobě dodává nebo dodala zboží nebo ho od ní odebrala či odebírá, koná nebo konala pro ni práce, anebo jí poskytuje nebo poskytovala služby nebo její služby využívala či využívá, případně se na této činnosti podílí nebo podílela.

Na základě zjištění kontrolní orgány vedou v různé podobě začátek kontroly a typicky neevidují čas výkonu kontrolní činnosti v místě kontroly u kontrolované osoby ve strojově zpracovatelné podobě pro účely této evidence.

Proto bude možné zaevidovat do systému jeden nebo více kontrolních úkonů u kontrolované osoby (od-do), nebo jen jeden začátek kontroly, nebo nezadat žádnou z těchto informací.

Zároveň některé kontrolní orgány vůbec nedisponují strojově zpracovatelnými informacemi. Systém, aby mohl vůbec nějak zpracovat takové informace o kontrolách a naplnit tak svůj účel, bude pracovat s náhradními hodnotami pro zobrazování. Nebudou-li proto informace zadány, budou doplněny z typu kontroly, pokud konfigurace typu kontroly bude vyplněna a povolena pro zobrazování. Samozřejmě bude taková informace v systému zachycena.

7.5.3. Kontrolní zjištění

Důvody pro nahlížení na kontrolní zjištění viz kapitola Důvody nahlížení.

Pro možnost unifikace dat z různých druhů kontrol a různých kontrolních orgánů systém nebude schraňovat skutečná kontrolní zjištění, ale jen kategorizovanou informaci:

- neuvedeno,
- bez zjištění,
- zjištění v neprospěch kontrolovaného subjektu,
- zjištění (podezření na porušení zákona),
- závažná zjištění (podezření na trestný čin).

Naplnění této klasifikace bude dáno metodickým postupem jednotlivých kontrolních orgánů a zejména dle jejich způsobu klasifikace zjištění. Zároveň evidence informace o zjištěních bude pro účely registrace kontroly v JePEK nepovinná, kdy přednost má úplnost evidence kontrol před úplností informací o kontrole.

Povinné bude uvedení bez zjištění, se zjištěním. V rámci přistoupení kontrolního úřadu bude dočasně možné výstup neuvádět.

Další změny klasifikace, které nastanou po prvotním nahlášení kontroly. Budou aktualizovány buď novým nahráním informací a jejich aktualizací, nebo manuální úpravou, kdy jde například o mimořádné situace postavené na autoritativní jiné interpretaci zjištění nebo autoritativním rozporování samotných zjištění. Například po rozhodnutí soudu bude kontrolní orgán povinen evidenci opravit (typicky tedy ve prospěch kontrolovaného subjektu).

7.5.4. Datum vyhotovení protokolu

Datum vyhotovení protokolu (dle § 12 odst. 1 písmeno j) bude základním parametrem pro časové ukotvení evidované kontroly (pokud nebudou dodány informace o začátku a konci kontroly separátně). Dle zjišťování u kontrolních orgánů je právě datum vyhodnocení protokolu obecně akceptovatelným datumem, který je možné poskytnout.

Zároveň kontrolu je vhodné registrovat jako provedenou do systému JePEK po vyhotovení protokolu, případně jeho následné kontrole dle metodiky kontrolního úřadu (typicky nadřízeným). Systémy v rámci kontrolních úřadů mohou tedy registrovat kontrolu, když je uvedeno datum vyhotovení protokolu. Zda je tak bezprostředně poté, nebo po dalším kroku (kontrola), nebo časové prodlevě, nebo až po uvedení datumu ukončení kontroly a případné kontrole správnosti je na metodice příslušného kontrolního úřadu.

7.5.5. Námitky

Původní plán evidence námitek byl opuštěn v této fázi projektu, neboť nemá přímou souvislost se základním cílem, a to koordinací kontrol za účelem nižší zátěže pro podnikatelské subjekty, Tedy původní plán shromažďování informací o námitkách (Byly podány námitky proti kontrolním zjištěním uvedeným v protokolu o kontrole – ANO/NE) nebude realizován.

Nicméně zůstává možnost, pokud kontrolní orgán pracuje s námitkami a má existenci námitek ve vlastním systému, (ať již formou stavu, příznaku nebo samostatné entity), takovou informaci předat do JePEK ve formě technického stavu kontroly. Případné nastavení bude realizováno v rámci domluvy s konkrétním připojujícím se kontrolním orgánem.

7.5.6. Datum ukončení kontroly

Datum ukončení kontroly bude v systému evidováno, pokud jej uživatel zadá (případně jiný integrovaný systém předá) formou integrace. V ostatních případech pak systém sám vypočte datum na základě alespoň jednoho zadaného datumu, který bude povinný.

7.5.7. Přestupek, Trestný čin

Evidence přestupků a trestných činů nebude předmětem evidence v rámci řešení. Nicméně informace bude transformována do výsledku kontroly.

Výsledek kontroly evidují různé kontrolní orgány různě a unifikace přístupů v rámci zavedení systému JePEK není možná. Proto systém JePEK bude adresovat různou praxi a formu výsledku kontroly formou vlastního překladu poskytnutých údajů o kontrole a jejich závěrů, kdy od Kontrolního orgánu převezme JePEK informaci o výsledku kontroly tak, jak ji bude standardizovaně kontrolní orgán poskytovat (tedy dopředu v rámci připojení kontrolního orgánu k systému JePEK dojde k domluvě vlastní sady hodnot příslušného kontrolního orgánu. Na úrovni JePEK bude informace spravována:

- Z hlediska viditelnosti pro podnikatele,
- Z hlediska viditelnosti pro ostatní kontrolní orgány,
- Z hlediska kategorizace výsledku kontroly.

Pro kontrolní orgány, které již v rámci kontroly formulují podezření na závažné či nezávažné porušení zákona, bude jejich kategorizace standardizována. Pro kontrolní orgány, které v rámci kontroly nic takového neprovádějí, bude evidováno, že poskytly informaci o ukončení kontroly, kdy výsledek kontroly existuje, ale nelze jej kategorizovat.

V obou případech pak ještě zobrazení výsledku kontroly ovlivňuje nastavení typu kontroly z hlediska viditelnosti pro podnikatele a viditelnosti pro ostatní kontrolní orgány, čímž je zabezpečeno, že o výsledku kontroly nejprve komunikuje (například na podnikatele) sám kontrolní orgán, a to nezávisle na tom, zda a kdy pošle či aktualizuje informace o kontrole.

7.5.8. Správní tresty

Správní tresty jsou:

a) napomenutí,
b) pokuta,
c) zákaz činnosti,
d) propadnutí věci nebo náhradní hodnoty.

Správní řízení není předmětem agendy vázané na kontrolní řád a může být jednou z oblastí, kterou se bude systém vyvíjet do budoucna. Nyní ale není primárním účelem systému, který se plánuje, aby byl opřen o zákon (kontrolní řád), kdy zpracování informací ze správního řízení není předmětem JePEK. Ačkoliv vybrané činnosti a rozhodnutí související s kontrolou mohou spadat jak pod kontrolní řád, tak pod správní řád, tak v tomto případě správní tresty spadají jednoznačně pod správní řád.

7.5.9. Práce s datumy na kontrole

7.5.9.1. Práce vypočtenými i zadanými datumy na kontrole

Systém bude u každého datumového údaje rozlišovat, zda jde o datum zadaný uživatelem, nebo datum vypočtený systémem.

Uživatelem nezadané datumové údaje na kontrole, které bude možné vypočíst ze stávajících zadaných uživatelem (či předaných integračním tokem, které bude systém JePEK také považovat za zadané uživatelem jen v jiném systému) systém vypočte dle připravených pravidel z konfiguračních dat o kontrole.

Příklad: Pokud mám v systému nakonfigurováno, že pro „typ kontroly“ trvá provedení kontroly průměrně 2 dny, a zároveň na kontrole (konkrétní instanci kontroly) mám zadáno pouze datum předpokládaného začátku kontroly, pak mohu vypočíst předpokládaný konec kontroly. Pak pokud mám začátek i konec kontroly, mohu kontrolu zobrazit v kalendářovém zobrazení.

Předpokládáme, že kontrola bude mít desítky možných datumů vážících se ke kontrole a k jednotlivým úkonům v rámci provedení kontroly, kdy každý datum pak bude systém disponovat více pravidly, jak je jej možno vypočíst na základě zadaných jiných údajů.

Na GUI aplikace budou vypočtené datumy zobrazovány odlišně od údajů zadaných (barva, typ písma), aby nedošlo k záměně a mýlce.

7.5.9.2. Práce s plánovanými a skutečně realizovanými datumy na kontrole

Na kontrole budou jak datumové údaje předpokládané, tak datumové údaje skutečné. Systém bude pracovat s údaji, které budou odpovídat stavu a kontextu použití příslušných údajů.

Příklad: Pokud budu mít jen plánované údaje o kontrole, pak budu kontrolu zobrazovat v plánovaných datumech. Pokud ale budu mít jak plánovaný začátek kontroly a také skutečně realizovaný začátek kontroly, pak systém bude zobrazovat kontrolu již ve skutečných hodnotách. Nicméně použití vhodného datumového údaje samozřejmě bude záviset na kontextu použití.

7.6. Princip viditelnosti kontrol

Každá kontrola má svoji konfiguraci a v ní určenu viditelnost.

Viditelnost se uplatňuje typicky pro reprezentanty jiných kontrolních orgánů a pro podnikatele. V případě, kdy kontrolní úřad utajuje plán či provedení některých kontrol i mezi různými organizačními jednotkami (územními pracovišti, odbory) v rámci kontrolního orgánu, bude možné nastavit v konfiguraci i omezenou viditelnost kontroly.

7.6.1. Módy viditelnost kontrol

Módy viditelnost kontrol:

- Plný detail - Plný detail znamená zobrazení Předmětu kontroly a Kontrolního orgánu.
- Jen Kontrolní orgán - Použije se v situaci, kdy nechceme zobrazit pro kontrolní orgány typ nebo předmět kontroly, ale z důvodu případné koordinace potřebuje kontrolní úřad vědět, jak koho případně kontaktovat (ať již z titulu koordinace stejného začátku nebo stejného konce kontroly, nebo jiného datumu kontroly), nebo prostě z důvodu, aby se inspektor kontrolního orgánu nedozvídal o jiné probíhající kontrole od kontrolované osoby.
- Jen informace o (nějaké) kontrole - zobrazuje pro uživatele jen informaci (typu rezervace času), ale bez udání detailů, o jakou kontrolu jde. Toto nastavení se typicky použije pro situace, kdy je kontrolní činnost předmětem konkurenčního boje, a to i ze zveřejnění informace kontrolního úřadu, co za kontrolu bude provedeno.

7.6.2. Parametrizace viditelnosti kontrol

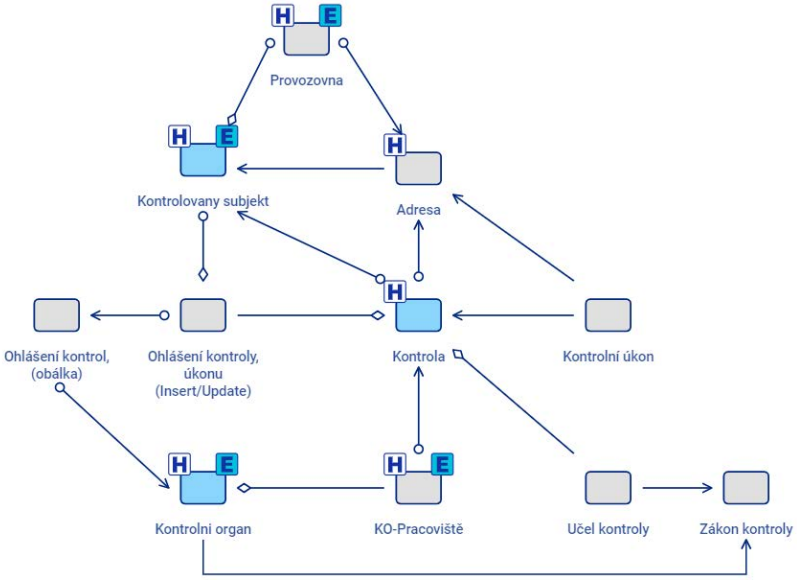
V rámci parametrizace kontroly bude, mimo jiné, parametrizována viditelnost kontrol, a to pomocí více parametrů tak, jak je z business pohledu uvedeno v následující tabulce. V cílovém řešení pak ještě může být parametrizace detailnější, a to s ohledem na technické aspekty realizace.

Parametr	Hodnota	Popis
Zveřejnit plán kontroly pro podnikatele před začátkem	0	Počet dní před plánovaným začátkem kontroly, kdy může být kontrola zveřejněna podnikateli, pokud nevyplněno nebo 0, nezveřejňovat.
Zveřejnit kontrolu pro podnikatele s odkladem od datumu protokolu	0	Počet dní, kdy se od ukončení kontroly může podnikatel dozvědět detaily kontroly, zejména výsledek (první mu to má sdělit KO).
Zveřejnění detailu kontroly pro podnikatele	Plný detail	Plný detail/Jen kontrolní orgán/Jen informace o nějaké kontrole -Tedy zveřejňuji v daném čase, že tam je ta a ta kontrola od toho a toho kontrolního orgánu, nebo jen že právě tento Kontrolní orgán tam plánuje kontrolu, nebo že prostě nějaká kontrola je plánována (bez detailů kdo a proč).
Zveřejnění detailu kontroly pro ostatní KO do začátku kontroly	Plný detail	Plný detail/Jen kontrolní orgán/Jen informace o nějaké kontrole - Tedy zveřejňuji v daném čase, že tam je ta a ta kontrola od toho a toho kontrolního orgánu, nebo jen že právě tento Kontrolní orgán tam plánuje

		kontrolu, nebo že prostě nějaká kontrola je plánována (bez detailů kdo a proč).
Viditelnost pro jiné organizační útvary kontrolního orgánu	Ano	Parametr určující, zda v případě, kdy má kontrolní úřad vice organizačních útvarů, bude či nebude chtít zneviditelnit (plánované) kontroly i mezi jednotlivými útvary. Pokud bude parametr nastaven, pak kontroly uvidí všichni pracovníci stejného kontrolního orgánu bez ohledu na případné organizační členění. Bez nastavení tohoto parametru kontroly založené pracovníky, kteří v rámci kontrolního orgánu budou mít definovaný právě jeden domovský organizační útvar, uvidí právě jen pracovníci stejného kontrolního orgánu a stejného organizačného útvaru, a pak ti pracovníci stejného kontrolního orgánu, kteří nemají uveden organizační útvar.

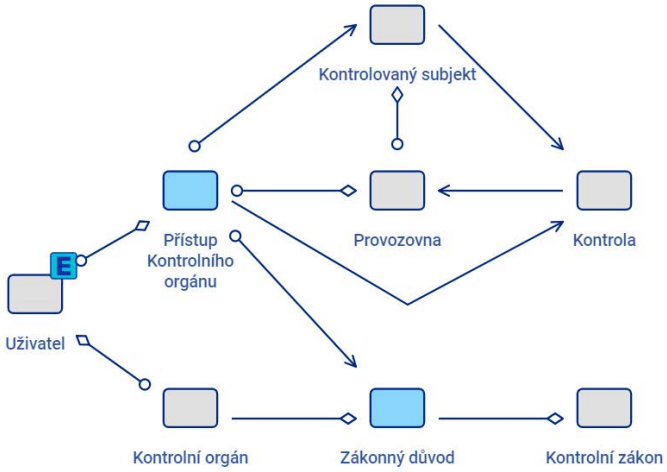
7.7. Kontext Kontroly

Základní datovou strukturou pro celé řešení JePEK je typ entity Kontrola. Aby byla kontrola pro JePEK relevantní, je potřeba vědět, co je to za kontrolu, musí být vhodně ukotvena v čase a typicky znát kontrolovanou osobu a kontrolní orgán. V ojedinělých případech ale je kontrolovaná osoba teprve dále upřesněna (na základě fyzické osoby, u které není nejprve jasné, jakou právnickou osobu reprezentuje). Termíny kontroly se budou týkat jak samotné kontroly, tak jednotlivých úkonů, které mohou být realizovány v rámci kontroly. Systém bude podporovat jak evidenci úkonů, tak evidenci bez úkonů, tedy jen informaci o konkrétní kontrole, a to podle toho, jaká data daný kontrolní orgán bude poskytovat.



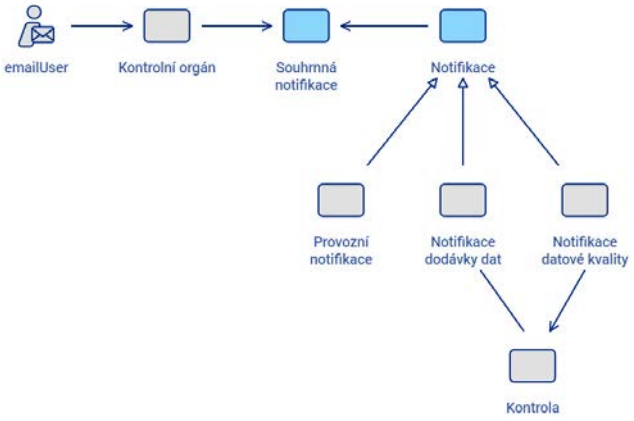
7.8. Kontext přístupu ke kontrole (čtení)

Kontext přístupu kontrolního orgánu k výsledkům kontroly je použit pro účely koordinace kontroly a také v případě přístupu reprezentanta kontrolního orgánu a rovněž evidence důvodu, kvůli kterému se seznamoval s kontrolami u kontrolované osoby.



7.9. Kontext notifikací

Notifikace se budou sestávat z různých druhů zjištění datové kvality, dodávky dat nebo provozních zpráv, které dohromady tvoří elementární notifikace. Pro určené uživatele formou role (tedy jeden nebo více za kontrolní orgán) jsou z elementárních notifikací skládány podle specifických pravidel souhrnné notifikace obsahující sdružené informace za celý kontrolní orgán tak, aby měl určený uživatel kompletní přehled o tom, na co je vhodné zareagovat.



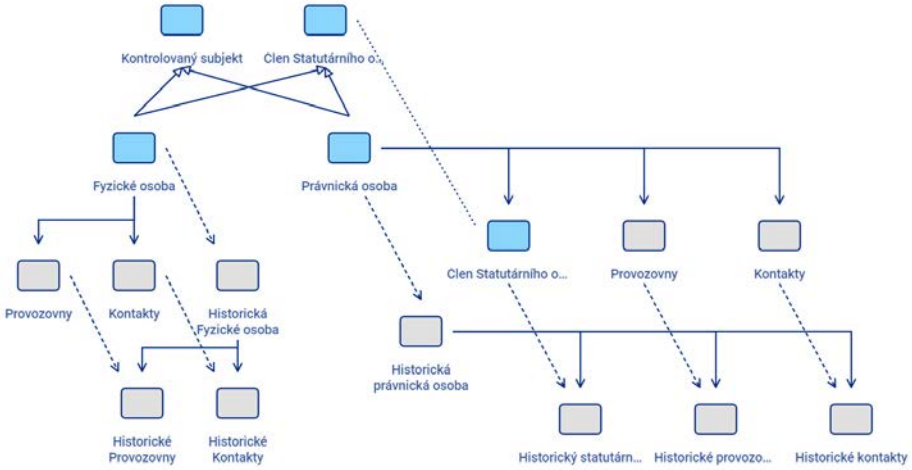
Rozpad usecase:

Zjištění a Notifikace				
	BL	M		Konfigurace pravidel datové kvality - neaktuálnost
	BL	L		Konfigurace pravidel datové kvality - povinnost údajů dle stavu kontroly
	SUC	M		Výpočet zjištění datové kvality pro neaktualizaci kontrol
	SUC	M		Výpočet zjištění datové kvality pro chybějící datovou kvalitu
	SUC	M		Výpočet ostatních zjištění koordinace nad kontrolami

	SUC	M		Výpočet zjištění pro notifikace na dodávku dat
	SUC	M		Výpočet notifikací nad zjištěními datové kvality
	SUC	S		Technické odeslání notifikací

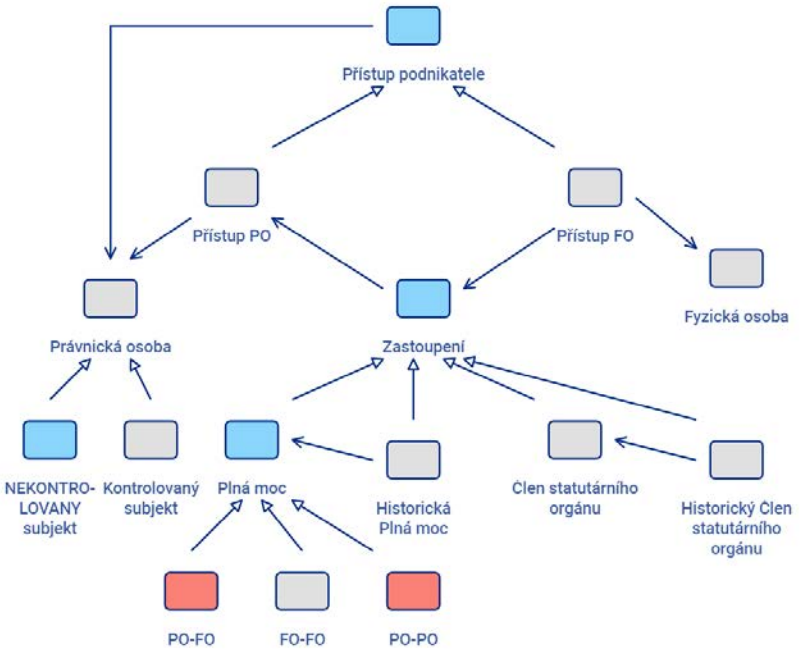
7.10. Kontext Kontrolovaného subjektu

Kontrolovaným subjektem může být fyzická osoba - podnikatel nebo právnická osoba. V rámci systému nastává významný počet změn podnikatelských subjektů, kdy v rámci potřeby je nutné respektovat, jak byly kontroly naplánovány a jak se jeví dnes (po změně názvu firmy, sídla, nebo fúzi). Otázky rozdělení nebo odprodeji části podniku nebude možné v rámci JePEK pokrýt jinak než heuristikou podle provozovny, kdy kontroly určité provozovny jsou převedeny k jiné firmě, pokud změnou je prodej/vyčlenění části podniku.



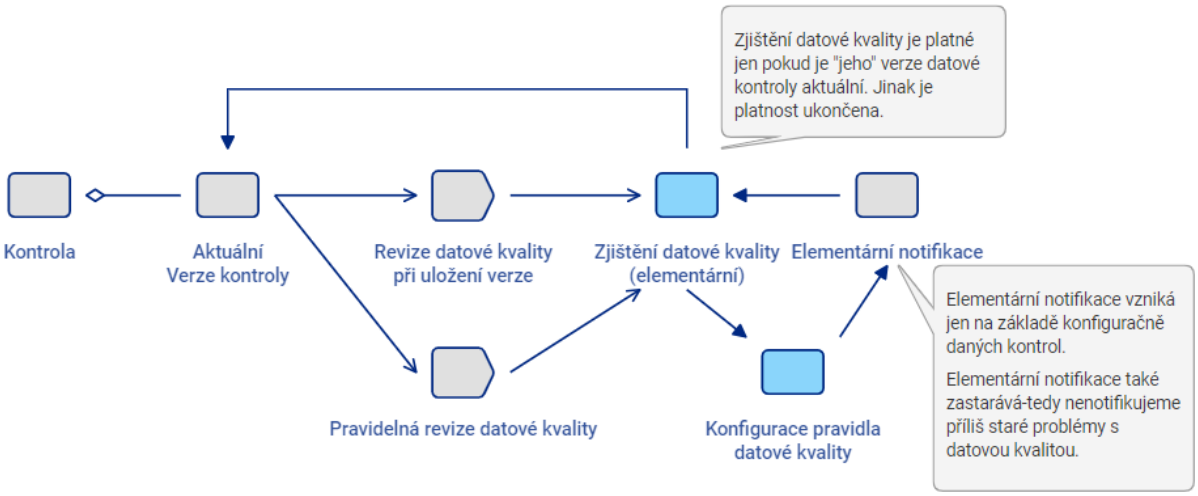
7.11. Kontext Zastoupení

Zastupování bude v systému JePEK řešeno pomocí příslušnosti, nebo členství ve statutárním orgánu, případně na základě plné moci v rámci systému REZA.



7.12. Kontext Zjištění datové kvality

Zjištění datové kvality bude systém generovat na základě aktuálních verzí kontrol, a to při uložení verze kontroly, a pak pravidelně (kvůli zastarávání dat) dle konfigurace příslušných jobů. Notifikace vznikne na základě nalezení Zjištění datové kvality jen pokud je konfigurováno, že vzniknout má a zároveň není příliš zastaralá, kdy již nebude notifikována.



8. Doplňkové funkčnosti systému

Zařazení doplňkových funkčností do informačního systému je často klíčovým krokem k tomu, aby byl systém nejen efektivní, ale i uživatelsky přívětivý. Cílem těchto doplňků je zlepšit pracovní prostředí uživatelů, zvýšit jejich produktivitu a zajistit, aby se jim se systémem lépe pracovalo. Jedním z takových doplňků je Poznámkový subsystém, který uživatelům umožňuje ukládat a spravovat důležité poznámky přímo v systému. Tento modul poskytuje uživatelům snadný způsob, jak si zaznamenat myšlenky, informace či úkoly, aniž by museli opustit pracovní prostředí. Zároveň zajišťuje přehlednost a organizaci práce, protože všechny poznámky jsou centralizované a dostupné na jednom místě, což zjednodušuje jejich vyhledávání a údržbu.

Další důležitou funkcionalitou je modul zpráv, který zajišťuje interní komunikaci mezi business administrátory a uživateli systému. Tento modul umožňuje snadnou a rychlou výměnu informací přímo v rámci pracovního prostředí, čímž se minimalizuje nutnost využívat externí komunikační kanály. Uživatelé tak mohou efektivně spolupracovat, sdílet důležité informace a upozornění bez toho, aby byli vyrušováni jinými nástroji. Modul zpráv navíc zvyšuje bezpečnost komunikace, protože veškerá interní korespondence zůstává v rámci informačního systému, což minimalizuje riziko úniku citlivých dat.

Mezi další užitečné doplňky může patřit například modul pro sledování termínů a úkolů, který uživatelům umožňuje mít lepší přehled o svých povinnostech a plánování. Díky automatickým upozorněním a přehledným seznamům úkolů se výrazně snižuje riziko zapomenutí na důležité termíny či schůzky. Tento modul rovněž podporuje týmovou spolupráci, protože umožňuje přiřazovat úkoly jednotlivým členům týmu a sledovat jejich postup. Celkově tyto doplňkové funkčnosti přispívají k tomu, aby byl informační systém více přizpůsobený potřebám uživatelů, zefektivnil jejich každodenní práci a podpořil jejich produktivitu.

8.1. Poznámkový subsystém

Systém bude podporovat typizované i ad-hoc poznámky ke kontrolám tak, aby tyto poznámky zobrazily reálné změny provedené na kontrole.

Poznámky budou typicky vázány k verzi záznamu kontroly a budou odkazovat na změnu verze nebo změnu stavu.

Typizované poznámky budou ve vlastním číselníku JePEK. Každá poznámka bude identifikována vlastním kódem.

Pokud je poznámka zapsána na kontrolu, pak vždy s autorem nebo označením, že poznámku přidal samotný systém.

Poznámky na kontrole není možné zapsat na základě vstupu nebo na základě automatické akce. Seznam všech automatických akcí bude určen v rámci projektu, nicméně takové akce budou obsahovat minimálně:

- založení kontroly,
- změna technického stavu/aktualizace kontroly,
- zjištění datové kvality na kontrole,
- vyřešení problému datové kvality na kontrole/aktualizace kontroly,
- změna výsledku nebo jiná aktualizace kontroly,
- změna na kontrolované osobě nebo na kontrolním orgánu.

Rozpad usecase:

Informační/Poznámkový subsystém				
	BUC	S		Portlet pro poznámkový/informační subsystém
	BUC	M		Editace položky/poznámky k zobrazení
	BUC	S		Zobrazení přehledu poznámek
	SUC	S		Zobrazení detailu poznámky

8.2. Organizační struktura úřadu a její použití

V rámci konfigurace pro zapojení úřadu bude k dispozici možnost definice organizační struktury úřadu a to tak, aby jednotlivé části organizační struktury mohly plánovat a realizovat kontroly (respektive jejich aktualizaci) v rámci jednoho úřadu.

Pokud je praxí kontrolního úřadu, že utajuje kontroly mezi organizačními složkami, tedy že nemá plánované kontroly vidět ani podnikatel, ani jiný kontrolní úřad a ani jiné organizační složky téhož úřadu, pak použije definování organizační struktury úřadu jako součást parametrizace při integraci kontrolního úřadu na systém JePEK.

Konfigurována může být taková vnitřní struktura úřadu jak v plné, tak i zjednodušené podobě. Součástí konfigurace jednotlivých útvarů pak bude i personální obsazení jednotlivých útvarů, které musí odpovídat uživatelům systému CAAIS.

Utajení lze dosáhnout:

- Konfigurací typu kontroly tak, aby nebyla viditelná pro jiné kontrolní úřady a zároveň neumožnit přímý přístup pracovníkům kontrolního úřadu do systému JePEK (kromě vybraných pracovníků, kteří takový přístup mají nebo mohou mít).
- Ustanovením organizačních složek a jejich samostatné působnosti v rámci jednoho kontrolního orgánu, pak ale je nutno realizovat funkčnosti vázané na jednotlivé organizační útvary, a to jak z hlediska viditelnosti, tak správy uživatelů.

8.3. Modul informací/zpráv

Jednou z možností, jak informovat hromadně uživatele o technických informacích ohledně provozu a změn systému JePEK, integrovaných kontrolních úřadů a stejně tak informací ohledně vlastní kontrolní činnosti.

V rámci řešení bude prezentační vrstva v rámci frontendů pro podnikatele i pro kontrolní orgány, formou portletu s prokliky na jednotlivé zprávy tak, jak je ukázáno v Aplikaci JePEK ve fázi 1.

Vlastní redakční systém, tedy příprava jednotlivých zpráv, zadání jejich zobrazovací platnosti a schvalování a také, zda je zpráva určena pro podnikatele a/nebo pro kontrolní orgány bude součástí frontendu pro business správu.

8.4. Speciální uživatelé

Vybrané orgány veřejné a státní moci (Policie ČR, Celní správa ČR) budou mít možnost také nahlížet do systému JePEK na vybrané podnikatele, a naopak nebudou mít možnost zadávat a editovat kontroly. Je požadavkem, aby o detailní aktivitě těchto uživatelů nebyly v systému detailní záznamy, které by mohly identifikovat oblasti zájmu těchto uživatelů.

O aktivitě těchto uživatelů budou rozdílné logovací záznamy:

- Budou pouze auditní záznamy o přihlášení/odhlášení uživatelů,
- Nebudou registrovány informace o prohlížení (přístupy pro následný výpočet koordinace kontroly),
- Nebudou aplikační logy o přístupu k jednotlivým podnikatelům a kontrolám,

9. Přístup uživatele

Různé druhy aktorů/typů uživatelů budou využívat jednotlivé části aplikace/mikroslužby, které budou obsahovat příslušné funkčnosti nutné pro příslušné skupiny procesů.

Uživatelé, kteří budou identifikováni jako podnikatelé se budou přihlašovat do systému JePEK pro podnikatele. Typicky uživatelé - zaměstnanci kontrolních orgánů budou využívat aplikaci JePEK pro kontrolní orgány. Zatímco typičtí uživatelé MPO budou přistupovat k administrační konzoli celého řešení, respektive k nástrojům pro statistické zpracování a vizualizaci dat.
Uvedené členění ale neznamená, že zaměstnanec příslušného kontrolního orgánu, respektive zaměstnanec MPO nemůže být také podnikatelem nebo zastupujícím člena statutárního orgánu podnikatele.

9.1. Soulad s aplikační roadmapou řešení

Řešení navazuje na verzi informační koncepce MPO z roku 2024:

- K datu rozpracovaného souboru je zveřejněna koncepce z roku 2019, která byla inovována a nyní je ve stadiu schvalování a publikace,
- https://www.mpo.gov.cz/cz/rozcestnik/ministerstvo/o-ministerstvu/informacni-koncepce-ministerstva-prumyslu-a-obchodu--243831/.

Předpokládá se řešení v Cloudu, a tedy Poskytovatel musí být zveřejněn v katalogu Cloud Computingu:

- https://app.powerbi.com/view?r=eyJrIjoiYjEwNTIwNjAtZWQ4MC00MzljLWJhMTktMmQyMDQ1MjdhODQ3IiwidCI6IjViNmI4NWNkLTQ0ZWYtNGQ2Ni04NmQ0LTYwM2RkMjE2MDc4MCIsImMiOjI9.

Systém JePEK podléhá schválení DIA, odboru hlavního architekta.

10. BEZPEČNOST

10.1. IDENTIFIKACE BUSINESS HROZEB A ZRANITELNOSTÍ

ID	Riziko	Vliv	Pravděpo-dobnost	Opatření k předcházení / eliminaci
R1	**Technická rizika**			
R1.1	Nedostatky v projektové dokumentaci / technickém zadání projektu	Velký	Nízká	Projektová dokumentace bude zpracována odborným Poskytovatelem, který bude vybrán v rámci veřejné zakázky. Součástí soutěže o návrh bude i prokázání kvalifikace Poskytovatele a pracovníků jeho týmu.
R1.2	Výběr nekvalitního Poskytovatele	Velký	Nízká	MPO jakožto veřejný Objednatel má bohaté zkušenosti s realizací zadávacích řízení. Součástí podmínek zadávacího řízení budou reference Poskytovatele, požadavek na záruku a servis na dobu pěti let provozu.
R1.3	Nedodržení termínu dodávky	Malý	Nízká	Termín dodávky bude s Poskytovatelem smluvně ošetřen. Pro případ nedodržení termínu dodávky budou stanoveny sankční podmínky. Zároveň bude implementace zajišťována odborným realizačním týmem, který bude průběžně monitorovat stav plnění a předpoklad termínu dodávky.
R1.4	Technické problémy při realizaci projektu	Střední	Nízká	Navržené řešení minimalizuje pravděpodobnost závažných technických problémů, jedná se o prověřený a standardizovaný způsob řešení obvyklých úloh. Realizační tým se skládá ze zkušených odborníků. Na realizaci projektu bude dohlížet systémový integrátor.
R1.5	Nedostatečná kvalita pořízeného řešení	Velmi velký	Nízká	Toto riziko může být eliminováno pouze důkladným výběrem Poskytovatele řešení. Poskytovatel bude vázán smlouvou, ve které bude dohodnuta pokuta za případnou špatnou kvalitu řešení. I v tomto případě bude kvalita řešení průběžně monitorována realizačním týmem tak, aby bylo možné včas identifikovat vady díla.
R2	**Organizační a procesní rizika**			
R2.1	Nezkušený projektový tým MPO	Velký	Nízká	Členové projektového týmu budou vybráni na základě své specializace, odbornosti a zkušeností. Členové týmu mají přesně stanovené kompetence a odpovědnosti a na jejich činnost dohlíží vedoucí projektu.
R2.2	Nedostatečná koordinace implementačních prací	Střední	Nízká	Koordinaci zavádění nového řešení bude zajišťovat vedoucí projektu spolu s pracovníky odboru informatiky. Tito členové projektového týmu budou zajišťovat dohled nad Poskytovatelem a vytvářet potřebné

				podmínky pro rychlou a kvalitní koordinaci. Pro snížení rizik implementace a zajištění kvality díla budou využity služby systémového integrátora.
R2.3	Nedostatečná kapacita pro realizaci projektu	Střední	Vysoká	MPO zajistí dostatečnou kapacitu pro realizaci projektu. Budou vytvořeny veškeré podmínky, aby byla zajištěna plynulá realizace projektu. Projekt svým rozsahem nevyžaduje velký počet členů týmu.
R2.4	Změna politických priorit	Velmi velký	Střední	Projekt je výsledkem poslanecké iniciativy, byl opakovaně projednáván se zainteresovanými stranami a má podporu vedení MPO. Nicméně věcné zaměření projektu zůstává potenciálně citlivým politickým tématem. Politická se shoda se může v čase změnit.
R2.5	Odpor uvnitř ministerstva či ze strany resortních organizací	Velmi velký	Střední	Projekt byl průběžně projednáván jak uvnitř ministerstva, včetně jeho vedení, tak s kontrolními orgány v gesci MPO. Proběhlo několik jednání a worskhopů. Organizace budou zapojeny do testování JePEK.
R3	**Informační rizika**			
R3.1	Nezvládnuté zabezpečení a uložení dat	Velký	Velmi nízká	Provozovatel musí být certifikovaným poskytovatelem cloudových služeb. Uložení dat a jeho zabbezpečení bude probíhat pravidelným auditům organizovaných MPO. Přístupem k datům budou disponovat pouze oprávněné osoby. Vzhledem k velkému nárůstu objemu dat bude potřeba data pravidelně zálohovat a zajišťovat retenci části dat, neboť řást dat bude zachována pro business účely v hlavní db.
R3.2	Nízké zabezpečení práce s osobními daty	Nízký	Nízká	V přípravné fázi projektu byla podrobně zvážena a projednána problematika práce s daty a jejich zabezpečením. Navržený systém i technologická platforma budou dostatečně zabezpečeny a budou splňovat všechny legislativní požadavky.
R4	**Právní rizika**			
R4.1	Nedodržení pravidel pro zadávání veřejných zakázek	Střední	Velmi nízká	MPO jakožto veřejný Objednatel má bohaté zkušenosti s realizací zadávacích řízení.
R4.2	Právní problémy s registrací JePEK v Registru práv a povinností	Střední	Vysoká	Řešit co nejdříve
R5	**Ostatní rizika**			
R5.1	Nedostatek finančních prostředků v provozní fázi projektu	Velmi velký	Střední	MPO má s provozem obdobných investic zkušenosti. Prostředky budou zajištěny v rámci běžného rozpočtu MPO, náklady

				provozní fáze nepředstavují nadměrné zatížení rozpočtu.
R5.2	Nedostatečná poptávka ze strany podnikatelů a cílových skupin	Velký	Nízká	Pro první etapu realizace projektu je pravděpodobnost rizika nízká, neboť se předpokládá zapojení kontrolních orgánů v gesci MPO.

10.2. POŽADAVKY NA DOSTUPNOST, DŮVĚRNOST A INTEGRITU DAT

Vzhledem k tomu, že ze známých skutečností lze vyvodit důležitost poptávaného informačního systém a naplňované agendy/služby, Objednatel očekává jeho zařazení mezi významné informační systémy identifikované dle vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění vyhlášky č. 360/2020 Sb. , resp. Objednatel bude poskytovatelem regulované služby v režimu vyšších povinností dle návrhu vyhlášky o regulovaných službách. Z těchto důvodů bude od Poskytovatele vyžadováno naplňování odpovídající legislativy.

Aktuální zákon:

> https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

Návrh zákona dle NIS2:

> https://portal.nukib.gov.cz/

Regulace cloud computingu:

> https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/materialy-k-regulaci-cloud-computingu/

10.2.1. Obecné bezpečnostní požadavky

MPO zpracovává metodiku, která bude v průběhu projektu schválena a bude závazná pro dodávku JePEK. Tyto požadavky je nutné splnit i přesto, že bude systém provozovaný v eGC. Důvodem je možná exitová strategie. Metodika bude obsahovat následující body:

1. IS musí naplňovat požadavky vyhlášky 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), zejména ve smyslu (autentizace, autorizace, logování včetně úspěšných a neúspěšných přihlášení, systém musí podporovat logování při umístění za reverzní proxy, mít garantovaný jednotný čas).
2. Bude-li v rámci IS využito služeb cloudu SaaS, musí tato infrastruktura naplňovat vyhlášku č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci, vyhlášku č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu a související právní předpisy.
3. Před uvedením do testovacího provozu, nebo v rámci něj, požadujeme provedení vulnerability testů dle běžných standardů a jejich vyhodnocení. (Cena bude součástí dodávky.)
4. Objednatel si vyhrazuje právo před akceptací díla a uvedením do provozu provést penetrační testy Informačního systému a code review. (Testování bude prováděno dle obvyklých metodik, např. OWASP)
5. Součástí dodávky je dokumentace všechny stupňů (low level design, high level design, architektura skutečného stavu, provozní dokumentace, bezpečnostní dokumentace, administrátorský manuál, uživatelský manuál, plány záloh, disaster recovery procedura navazující na plány záloh, exitová strategie …).
6. Informační systém musí podporovat současné využití IPv4 i IPv6 (včetně logování).

10.2.2. Dostupnost

Informační systém musí splňovat požadavky na vysokou dostupnost, přičemž provoz bude zajištěn v cloudovém prostředí s možností škálování dle aktuální zátěže.

Systém musí využívat **load balancer** a minimálně dva uzly, což zajistí plynulý provoz i při výpadku jednoho z nich. Horizontální škálování musí být plně podporováno, aby bylo možné dynamicky reagovat na zvýšenou zátěž. Dávkové úlohy musí být navrženy tak, aby bylo možné jejich zpracování rozložit na více serverů, čímž se minimalizuje dopad na výkon systému.

Celkové vyhodnocení úrovně bezpečnostního aktiva dle platných směrnic: 2

10.2.3. Důvěrnost

Přístup k datům a jejich sdílení musí být založeno na **předkonfigurovaných bezpečnostních principech (security by design)**, které zajistí, že citlivé informace budou dostupné pouze oprávněným uživatelům. Role a oprávnění musí být definovány předem, s možností jejich centrální správy a auditovatelnosti.

Celkové vyhodnocení úrovně bezpečnostního aktiva dle platných směrnic: 3

10.2.4. Doba odezvy

Systém musí zajistit odpovídající dobu odezvy pro běžné uživatelské operace:

- **Základní uživatelské scénáře (UC)** – maximální odezva 3 sekundy pro 90. percentil.
- **Nahrání a zpracování velkých souborů (např. Excel s 100 000 kontrolami)** – zpracování asynchronně, doba zpracování do **3 hodin** na 90. percentilu.

10.2.5. Integrita dat

Systém musí zajistit vysokou kvalitu a konzistenci dat prostřednictvím následujících opatření:

- **Priorita dostupnosti dat** – v případě nedostupných hodnot musí systém umět data **dopočítat pomocí spekulativních hodnot** namísto jejich absence, jde zejména o situace, kdy nebude informace o kontrole dostatečně specifikována, ale z typu kontroly bude dovoditelné jak by mohla nebo měla proběhnout, pak budou použity standardní/defaultní hodnoty například pro zobrazení v kalendářovém zobrazení kontrol. Dopočítaná data však budou vyznačena oproti standardnímu textu.
- **Verzování dat** – všechny změny v datech musí být verzovány, aby bylo možné zpětně dohledat historii úprav.
- **Řízení datové kvality** – musí být zavedeny mechanismy pro kontrolu konzistence, validaci vstupních i výstupních dat a pravidelný audit datových záznamů.

Celkové vyhodnocení úrovně bezpečnostního aktiva dle platných směrnic: 3

10.2.6. Aktuální technologie

Soubor požadavků v předchozích odstavcích směřuje k zajištění, že informační systém bude nejen dostupný a škálovatelný, ale také bezpečný, výkonný a odolný vůči nekonzistenci dat. Poskytovatel je nad tento rámec povinen přijmout opatření k zajištění dostupnosti, bezpečnosti a výkonnosti informačního systému na úrovni aktuálního stavu použitých technologií.

10.3. POŽADAVKY NA LOGOVÁNÍ UDÁLOSTÍ A BEZPEČNOSTNÍ MONITORING

Informační systém musí obsahovat robustní mechanismus pro logování událostí na několika úrovních s cílem zajistit transparentnost, dohledatelnost a bezpečnost provozu.

10.3.1. Logování na úrovni technologie

Systém musí zaznamenávat technické logy zahrnující:

- Chyby a výjimky aplikace, včetně detailních chybových hlášení a diagnostických informací.
- Výkonové metriky a monitoring infrastruktury (např. CPU, paměť, využití diskového prostoru).
- Záznamy o síťové komunikaci, přístupu k databázím a operacích se souborovým systémem.
- Volání API a integrace s dalšími systémy včetně latence a výsledků odpovědí.

10.3.2. Logování na úrovni businessu

Na business úrovni musí systém uchovávat logy o klíčových uživatelských akcích a obchodních procesech, zejména:

- Přihlášení a odhlášení uživatelů včetně času, IP adresy a použitého zařízení.
- Změny v datech (vytvoření, úprava, smazání) včetně uživatelské identifikace a verze změny.
- Spuštění a dokončení klíčových procesů, včetně workflow schvalování a zpracování transakcí.
- Neúspěšné pokusy o přístup nebo změny, které mohou signalizovat podezřelé aktivity.

10.3.3. Bezpečnostní monitoring a požadavky NIS2

V souladu s požadavky směrnice NIS2 musí informační systém poskytovat centralizovaný bezpečnostní monitoring zahrnující:

- Monitorování anomálií (např. podezřelé přihlašování, hromadné změny dat).
- Auditní stopy všech kritických akcí v systému s nemodifikovatelnou historií.
- Integraci s bezpečnostními nástroji (SIEM, IDS/IPS) pro aktivní detekci hrozeb.
- Mechanismy pro reportování a notifikace odpovědným osobám při zjištění bezpečnostního rizika.
- Všechny logy musí být ukládány bezpečně, s ochranou proti neoprávněné manipulaci, a splňovat legislativní požadavky na uchovávání dat a auditní záznamy.

10.4. DETEKCE, PREVENCE A ZVLÁDÁNÍ INCIDENTŮ

Efektivní řízení bezpečnostních incidentů vyžaduje zavedení systematického přístupu k jejich **detekci, prevenci a následnému zvládání**. Klíčovým prvkem je **pravidelná kontrola** provozního a bezpečnostního stavu informačního systému, včetně automatizovaného monitoringu, analýzy logů a provádění bezpečnostních auditů. Tyto kontroly slouží k včasné detekci podezřelých aktivit a potenciálních bezpečnostních hrozeb. Tyto činnosti budou součástí Provozu informačního systému JePEK zajištěného Poskytovatelem.

Způsob zpracování hlášení incidentů bude podporovat **automatizovanou kategorizaci incidentů** a jejich přesměrování k odpovědným týmům podle povahy a kritičnosti problému.

Součástí procesu řízení incidentů jsou **pravidelné revize stavu řešení** s cílem sledovat pokrok, řešit případné **prodlevy** a provádět **urgenci** nevyřízených případů. Pokud není incident vyřešen v předepsaném termínu, musí být možné jej **eskalovat** na vyšší úroveň řízení.

Důležitým prvkem je také „**problem management“**, který se zaměřuje na hlubší analýzu opakujících se problémů, hledání jejich kořenových příčin a návrh opatření pro jejich odstranění. Tento proces musí být úzce propojen s

reportingem, který zajistí pravidelné přehledy o výskytu, řešení a prevenci incidentů. Reporty musí být přizpůsobeny jednotlivým úrovním řízení, od **operativních přehledů pro IT týmy** až po **manažerské souhrny** pro strategické rozhodování.

Kombinace těchto opatření s cílem zajistit rychlou reakci na incidenty, ale také dlouhodobé zvyšování odolnosti systému a zlepšení jeho bezpečnostní politiky je předmětem výběru provozování systému.

10.5. POŽADAVKY NA HARDENING ICT SYSTÉMŮ

Realizace hardeningu informačního systému zahrnuje bezpečnostní nastavení a striktní oddělení konfigurací od samotné aplikace, čímž se minimalizuje riziko neoprávněných změn a bezpečnostních incidentů.

Konfigurace musí být pravidelně kontrolována z hlediska konzistence, aby se zajistilo jednotné a bezpečné nastavení v celém systému.

Automatizované mechanismy konfigurace budou implementována pro jednotlivá prostředí (vývoj, test, produkce) s jasně definovanými bezpečnostními politikami.

Pro zajištění dlouhodobé bezpečnosti je nutné provádět pravidelnou údržbu systému, zahrnující revizi konfigurací, analýzu nových vektorů útoků a aktualizaci bezpečnostních opatření minimálně jednou za dva roky.

10.6. ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Informační systém zpracovává osobní údaje v souladu s obecným nařízením o ochraně osobních údajů (GDPR) a zajišťuje odpovídající úroveň zabezpečení datových operací. Všechny osobní údaje jsou zpracovávány pouze za účelem, pro který byly získány, a jejich uchovávání podléhá zákonným požadavkům na ochranu soukromí. Subjekty údajů mají v souladu s GDPR definovaná práva, která mohou uplatnit vůči správci osobních údajů.

10.6.1. Právo na přístup k osobním údajům (čl. 15 GDPR)

Každý uživatel má právo požádat o přístup k osobním údajům, které jsou o něm v systému evidovány. Na základě žádosti subjektu údajů musí správce poskytnout souhrn informací o zpracovávaných údajích, včetně účelu zpracování, kategorií zpracovávaných údajů a doby jejich uchování.

10.6.2. Právo na opravu osobních údajů (čl. 16 GDPR)

V případě, že osobní údaje uvedené v systému jsou nepřesné nebo neaktuální, má uživatel právo požadovat jejich opravu. Zejména zaměstnanci, jejichž údaje jsou evidovány v souvislosti s testováním nebo jinými procesy, mají právo zajistit správnost a aktuálnost svých dat.

10.6.3. Právo na výmaz osobních údajů (čl. 17 GDPR)

Subjekt údajů může požadovat výmaz svých osobních údajů pouze v případech, kdy již pominul účel jejich zpracování nebo pokud správce nemá pro další uchovávání oprávněný právní důvod. Toto právo se nevztahuje na údaje, které musí být uchovávány pro splnění právních povinností nebo pro ochranu oprávněných zájmů správce.

10.6.4. Právo na omezení zpracování (čl. 18 GDPR)

Omezení zpracování osobních údajů lze uplatnit pouze ve specifických situacích, například pokud subjekt údajů zpochybňuje správnost zpracovávaných údajů, nebo pokud jsou osobní údaje potřebné pro určení, výkon nebo obhajobu právních nároků. V ostatních případech systém umožňuje zpracování údajů v rozsahu nezbytném pro plnění zákonných a smluvních povinností.

Zajištění souladu s GDPR je nedílnou součástí provozu informačního systému, přičemž veškeré procesy zpracování osobních údajů podléhají pravidelným kontrolám a auditům s cílem minimalizovat rizika neoprávněného přístupu nebo zneužití dat.

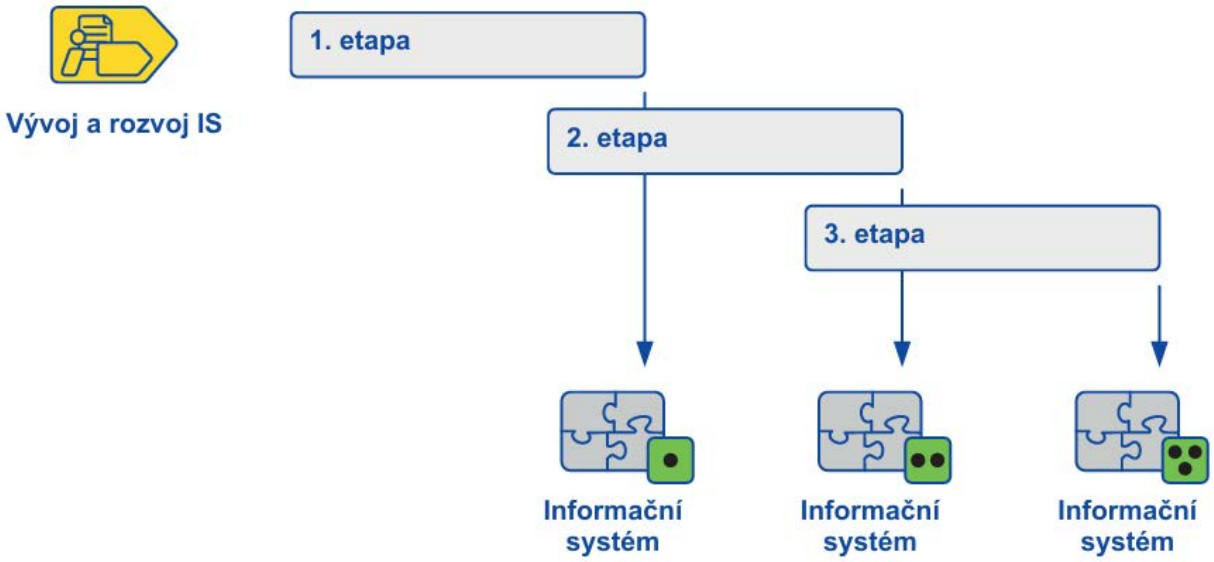
10.6.5. Právo podat stížnost u Úřadu jako dozorového úřadu (čl.77 obecného nařízení)

Každý subjekt údajů (pokud se domnívá, že došlo k porušení obecného nařízení) má právo podat stížnost Úřadu pro ochranu osobních údajů, Pplk. Sochora 27, 170 00 Praha 7, tel. +420 234 665 111, e-mail posta@uoou.cz.

11. REALIZACE A NASTAVENÍ

11.1. Etapizace

Systém JePEK bude dodáván v jednotlivých rozvojových etapách a následně pak v iteracích, kdy etapa dodá systém, který je použitelný a mohl by být nasazen k použití.



Dodávka bude realizována maximálně v tříměsíčních iteracích, kdy na konci každé iterace bude dodána provozuschopná verze systému, byť v omezené funkčnosti.

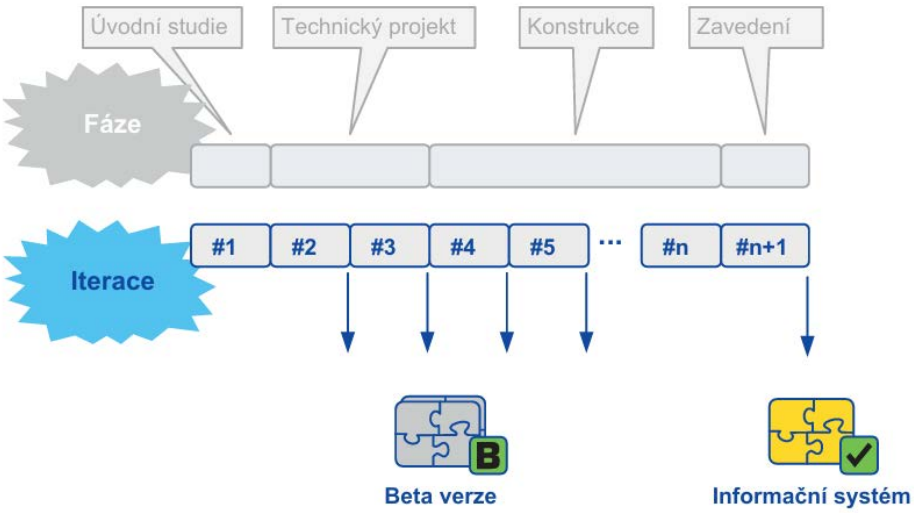
Rozdělení funkčnosti do jednotlivých iterací bude v kompetenci Poskytovatele.

11.1.1. Migrace dat

Migrace dat kontrolních orgánů při jejich přistoupení k informačnímu systému JePEK bude vždy koordinována s konkrétními kontrolními orgány, a to v souladu s jejich připraveností. V rámci tohoto procesu je nezbytné, aby Poskytovatel veřejné zajistil migraci dat nejvhodnějším způsobem pro přistupující kontrolní orgány k systému JePEK, čemuž bude MPO dohlížet a garantovat, že budou převedeny veškeré potřebné údaje.

11.1.2. Životní cyklus

Požadavkem je, aby dodávka probíhala v iteracích, kdy jednotlivé iterace dodávají dílčí funkčnosti nebo ukazují dílčí postupné kroky.



Přehled na jednotlivých iteracích ukazuje i pokrok v rámci projektu. Objednatel očekává, že vždy výsledky každé iterace budou presentovány vybraným pracovníkům MPO.

11.1.3. Popis release aplikace

Při plánování a vydávání nové verze aplikace je nezbytné definovat jasné požadavky na release, které zahrnují specifické potřeby pro instalaci, testování a správu verzí.

11.1.3.1. Požadavky na instalaci v kontejnerech

Aplikace by měla být navržena tak, aby byla plně kompatibilní s instalací v kontejnerech. Kontejnerizace zajišťuje jednoduchou a flexibilní instalaci a nasazení aplikace na různých systémech. Při každém release by měl být součástí také nový kontejnerový image, který obsahuje všechny potřebné závislosti a verze aplikace. Instalace by měla být plně automatizovaná, aby minimalizovala potřebu manuálních zásahů a urychlila nasazení nové verze.

11.1.3.2. Automatická instalace

Součástí požadavků na release je také automatická instalace, která zahrnuje mechanismus pro stahování, konfiguraci a spuštění aplikace bez nutnosti manuálního zásahu. Automatizovaný proces by měl být robustní, aby minimalizoval riziko chyb při nasazování nové verze aplikace. To zahrnuje validaci konfigurací, kontrolu dostupnosti požadovaných závislostí a zajištění, že všechny komponenty aplikace budou správně nainstalovány a připraveny k běhu. K tomu mohou být použity nástroje jako CI/CD pipeline, které umožní automatizovat celý proces nasazení a testování.

11.1.3.3. Základní automatický regresní test

Každá release by měla obsahovat minimálně základní sadu automatických testů, které ověří základní funkčnost aplikace. Tyto testy by měly pokrýt kritické oblasti aplikace, jako je připojení k databázi, základní uživatelské akce a interakce mezi hlavními komponentami systému. Automatické testy pomáhají zajistit, že nová verze aplikace neporušuje základní funkce, a tím zvyšují důvěru ve stabilitu release. Automatizace testů by měla být součástí například zmíněného, CI/CD pipeline, pokud bude použito, a měla by být součástí každé nové verze, ať už se jedná o minor nebo major release.

11.1.3.4. Manuální testy na funkčnosti nepokryté automatickými testy

Kromě základních automatických testů by měla být provedena také sada manuálních testů na ostatní oblasti aplikace. Tyto testy mohou zahrnovat specifické funkce, které nejsou snadno testovatelné automatizovaně, nebo testování aplikace v reálném prostředí, kde mohou nastat nečekané interakce mezi různými komponentami. Manuální testy mohou zahrnovat testování UI/UX, validaci nových funkcí, kompatibilitu s různými zařízeními a operačními systémy, nebo provádění zátěžových testů.

11.1.3.5. Minor releasy a opravy chyb

Minor releasy by měly přinášet drobné vylepšení nebo opravy chyb, které neovlivňují celkovou stabilitu aplikace. Požadavky na release pro minor verze zahrnují související opravy chyb, které byly identifikovány v předchozích verzích aplikace. Automatické testy by měly být provedeny nejen na existujících funkcích, ale i na nových úpravách, aby se zajistila stabilita systému. Kromě toho by měly být provedeny manuální testy na nové změny, aby se ověřilo, že nedošlo k nežádoucím vedlejším efektům.

11.1.3.6. Major releasy

Major releasy představují zásadní změny v aplikaci, které mohou zahrnovat nové funkce, změny v architektuře nebo významné úpravy uživatelského rozhraní. Před vydáním major release je nezbytné provést podrobné plánování, testování a validaci nových funkcí. Kromě automatických testů je třeba také provádět komplexní manuální testy na všechny klíčové oblasti aplikace, aby se zajistilo, že nové funkce neohrozí stabilitu systému a že aplikace bude fungovat jak pro nové, tak pro stávající uživatele. U major release je rovněž důležité důkladně dokumentovat všechny změny a připravit odpovídající školení pro uživatele, pokud to bude potřeba.

11.1.3.7. Obecné požadavky na releasování

Aktualizace systému budou probíhat podle předem definovaného harmonogramu po dohodě s vybraným Poskytovatelem.

11.1.4. Útlum nahrazených aplikací

Systém JePEK nebude nahrazovat žádné existující systémy, ale bude navazovat na vybrané funkčnosti systémů, které ale neplánuje nahradit v blízkých etapách rozvoje.

11.2. INFRASTRUKTURA

11.2.1. Multicloud a hybridcloud

Při dodávce informačního systému je klíčové zajistit jeho dlouhodobou udržitelnost a flexibilitu. Protože nelze v horizontu cca 10 let s jistotou predikovat nejvýhodnější způsob provozu systému JePEK je požadováno použití kontejnerizační technologie, která bude umožňovat nasazení systému jak v cloudových řešeních různých poskytovatelů, tak na lokálních serverech uvnitř MPO, čímž poskytuje potřebnou nezávislost a eliminuje riziko vendor lock-in efektu.

Kontejnery poskytují standardizované a izolované prostředí pro běh aplikací, což zjednodušuje nasazení, škálování a správu systému bez ohledu na konkrétního poskytovatele infrastruktury. Díky využití kontejnerové orchestrace lze systém provozovat v hybridním režimu s možností přechodu mezi cloudovými a on-premise prostředími dle aktuálních potřeb organizace.

Tento přístup umožňuje optimalizaci nákladů i zajištění dostupnosti v případě regulatorních nebo bezpečnostních požadavků na provoz systému JePEK.

Použití kontejnerových platforem umožňuje flexibilní migraci systému mezi poskytovateli cloudu (např. AWS, Azure, Google Cloud či jinými) i mezi lokálními servery, aniž by bylo nutné zásadně měnit architekturu aplikace. Tento přístup podporuje strategii multicloud a/nebo hybridcloud, kdy lze aplikaci provozovat současně ve více prostředích a využívat výhod jednotlivých platforem podle aktuálních požadavků na výkon, bezpečnost nebo cenu.

11.2.1.1. Požadavky na dodávku systému v cloudu

Poskytovatel musí zajistit, že celý systém bude navržen a dodán ve formě kontejnerizovaných služeb s odpovídající dokumentací a automatizovanými deploymenty, aby bylo možné jeho snadné přemístění mezi prostředími. Součástí dodávky musí být také monitorovací a logovací nástroje, které zajistí přehled o výkonu a provozu aplikace v různých prostředích. Pro zajištění dlouhodobé udržitelnosti a nezávislosti na konkrétním poskytovateli infrastruktury je nutné minimalizovat využití proprietárních služeb jednotlivých cloudových platforem a preferovat otevřené standardy.

Tento přístup poskytuje organizaci maximální flexibilitu, umožňuje reagovat na budoucí technologické změny a zároveň chrání investice do informačního systému tím, že umožňuje jeho provoz v různých prostředích podle aktuálních potřeb a strategií Objednatele.

Objednatel požaduje, aby uchazeč v době podání nabídky **byl v katalogu Cloud computingu**[1] v minimální **úrovni 2 – střední.**

11.2.2. Škálování prostředí

Pro efektivní využití cloudových zdrojů je nutné, aby aplikace podporovala horizontální škálování, kdy se v případě zvýšené zátěže automaticky přidávají další instance služeb. Kromě škálování aplikační vrstvy je důležité efektivně pracovat se zátěží i na úrovni zpracování úloh. Zde hraje klíčovou roli asynchronní zpracování, které umožňuje rozdělit složité operace do front, minimalizovat zatížení hlavních aplikačních serverů a zajistit plynulý chod systému i při velkém množství požadavků.

Díky kombinaci správně nastaveného škálování, optimalizovaného rozložení zátěže a průběžného monitorování výkonu lze zajistit, že systém bude efektivně využívat cloudové zdroje, poskytovat konzistentní výkon uživatelům a zároveň minimalizovat provozní náklady.

Poskytovatel navrhne a implementuje odpovídající strategii škálování, a také bude průběžně vyhodnocovat výkon aplikace a optimalizovat nastavení podle skutečného zatížení systému.

11.2.3. Sizing prostředí

Při návrhu a dodávce informačního systému provozovaného v cloudu je klíčové, aby Poskytovatel provedl sizing prostředí a zajistil vhodné škálování. I když bude systém využívat autosizing formou horizontálního škálování, je nezbytné mít představu o základních požadavcích na výkon a spotřebu zdrojů. Tato analýza je zásadní nejen pro zajištění optimálního výkonu aplikace, ale také pro odhad provozních nákladů, které budou hrát důležitou roli při plánování rozpočtu na provoz systému.

Níže uvedené odhady obsahují předpokládané informace k využití systému:

- Do 1 roku: znamená do 1 roku od spuštění systému,
- Do 3 let znamená ročně od 1 roku do 3 let po spuštění systému,
- Nad 3 roky znamená ročně od čtvrtého roku běhu systému.

Tabulka podkladů od odhady sizingu:

Oblast	Podoblast	Do 1 roku	Do 3 let	Nad 3 roky	Poznámka
Odhad počtu uživatelů GUI>	Uživatel typu Podnikatel:	5 000	20 000	100 000	
	Uživatel typu Representant kontrolního úřadu	100	500	1 000	
	Business správce, MPO	10	10	10	
	Ostatní uživatelé	10	50	100	
Odhad počtu souběžně		< 50	< 100	< 200	

[1] [1] https://www.dia.gov.cz/oha/katalog-cloud-computingu/

pracujících uživatelů					
Odhad počtu uživatelů webových služeb		5 000	10 000	20 000	Jde o uživatele, kteří pracují s vlastním IS, který pak volá webové služby systému JePEK.
Odhad počtu evidovaných kontrol		100 000	200 000	350 000	Roční hodnoty nově evidovaných kontrol

Poznámka: Uvedené odhady jsou předběžné a negarantované, ukazují rámcové požadavky.

11.2.4. Požadavky na technologické komponenty

Řešení musí být nasaditelné do public i private cloudu za použití kontejnerové virtualizace a splňovat vlastnosti cloud-native řešení. Tedy musí být bez programátorské změny nasaditelné jak v public cloudu, tak on premise serverech v rámci perimetru MPO.

Platforma řešení musí obsahovat podporu pro cloudové runtime prostředí, které řešení automatizovaný deployment nových služeb, infrastrukturu pro logování a auditní logování, monitoring stavu služeb a souvisejících zdrojů.

Řešení musí být škálovatelné a musí jej být možné nasadit v režimu vysoké dostupnosti (high-availibility) přes více datových center.

Veškeré funkčnosti řešení musí být dostupné pomocí API, kde každé volání API musí být autorizováno a šifrováno. Všechna API musí být zdokumentováno pro možné použití třetími strany (URI, vstupy, výstupy, chybové stavy).

Front-end bude vytvořen jako webová aplikace, která je spustitelná v běžném webovém prohlížeči. Front-end bude responzivní, takže bude použitelný na různých typech zařízení (desktop, notebook, tablet, smartphone).

Řešení musí disponovat možností pro tvorbu webového obsahu (portály, dashboardy, ..) z vizuálních komponent koncovými uživateli. Platforma musí nabízet katalog ready-to-use komponent (rich text editor, tabulka, grafy, obrázky, ..) a tento katalog může být dále rozšiřován o další, specifické komponenty.

Vestavěna podpora multitenancy, kde je možné jednoduše a efektivně oddělit data jednotlivých tenantů a je možné jednoduše, bez programování, zavést nového tenanta (například nový kontrolní subjekt).

Platforma, na které bude řešení postaveno, musí nativně obsahovat základní funkčnosti content managementu a document managementu, které budou využity v dalších fázích projektu JePEK.

Platforma, na které bude řešení postaveno, musí nativně podporovat práci s úkolováním konkrétních uživatelů nebo rolí v systému, včetně inboxu (soupisu úkolů s možnosti zobrazení úkolu i objektu, kterého se úkol týká), aby tato funkčnost mohla být využita v dalších fázích rozvoje systému JePEK.

11.3. LICENCE

11.3.1. Aplikační licence

V rámci návrhu předpokládáme řešení postavené i na licencovaném SW, kdy veškeré licenční poplatky budou součástí díla.

Při uvádění licencí a licenčních poplatků softwarových produktů je klíčové zajistit jejich transparentnost a srozumitelnost pro MPO. Veškeré potřeby licencí je nutné jasně označit a specifikovat, zda se jedná o jednorázovou licenci, nebo o opakující se poplatky. Požadujeme vždy tyto náklady zahrnout do konečné ceny díla nebo do pravidelných měsíčních či ročních plateb za provoz díla.

Současně budou licenční podmínky uvedeny v přílohách smlouvy nebo v obchodních podmínkách, aby byly právně vymahatelné a přehledně zdokumentované.

11.3.2. Infrastrukturní licence

Veškeré požadavky na infrastrukturní licence:

- v případě využití lokálních zdrojů a lokální sítě MPO budou zajištěny objednatelem,
- v případě provozování SW řešení v cloudu budou veškeré infrastrukturní licence součástí ceny (vytvoření nebo provozu díla)

11.3.3. Návrh licenčního pokrytí

Pro navrhované řešení předpokládáme pouze využití serverových licencí za databázi, ostatní licence pak předpokládáme, že budou součástí cloudových subskripcí.

12. TESTOVÁNÍ A ŠKOLENÍ

12.1. NÁSTROJ PRO ŘÍZENÍ TESTOVÁNÍ

V rámci projektu je vhodné použití nástroje pro řízení testování tak, aby bylo možné nezávisle ověřit protestovanost a výsledky jednotlivých testů v rámci jednotlivých kol testování.

12.2. TESTOVACÍ SCÉNÁŘE

Testy budou prováděny na základě předem připravených způsobů ověření – testovacích scénářů. Přehled a popis testovacích scénářů pro každou jednotlivou dodávku bude schvalovat pracovník MPO.

V rámci testování je možné požadovat pro každý dodávaný usecase, algoritmus nebo integraci dodat několik pozitivních a negativních testovacích scénářů pro otestování vybrané funkčnosti. Rozsah pokryté testovacími scénáři pak bude pozitivně korelován se složitostí testované komponenty softwarového řešení. Tyto testovací scénáře budou být dokumentované a verifikovatelné.

Výsledky provedení testovacích scénářů v jednotlivých kolech testování pak budou předmětem reportingu.

12.2.1. Uživatelské aplikační testy

MPO požaduje, aby Poskytovatel provedl nejprve testy sám před předáním příslušné části díla. Testy budou provedeny na všech smluvených scénářích.

12.2.2. Testy infrastruktury

Na infrastruktuře budou provedeny zátěžové testy, kdy zejména bude prověřena schopnost škálování. Požadované parametry pro testy infrastruktury budou odpovídat best practice a zároveň velikosti systému v čase, tak, jak naznačuje kapitola 11.2.3.

12.2.3. Bezpečnostní a penetrační testy

Poskytovatel prokáže provedení penetračních testů pomocí renomovaných nástrojů schválených MPO. Poskytovatel prokáže výsledky testů a opravu nebo komentáře k nálezům.

Dle výsledků pak MPO bude výsledky akceptovat případně provede penetrační testy samo, nebo s pomocí třetí strany s cílem nezávisle ověřit provedené testy a opravené chyby.

V případě závažných zjištění bude MPO opakovat provedení bezpečnostních a penetračních testů, ale finanční náročnost jde k tíži Poskytovatele.

12.3. ŠKOLÍCÍ PROSTŘEDÍ a ŠKOLENÍ

Pro zajištění efektivního využívání informačního systému JePEK budou školení organizována s ohledem na specifické potřeby jednotlivých skupin uživatelů. Každá skupina bude mít jiný rozsah a formu školení přizpůsobenou jejich roli v systému, frekvenci využívání a potřebné úrovni odbornosti.

12.3.1. Školící prostředí

Školící prostředí je diskutováno dále v kapitole Neprodukční prostředí.

Datově však bude obsahovat starší zálohu dat z produkčního prostředí nebo testovací, anonymizovaná data. Stáří zálohy bude dle rozhodnutí MPO (typicky 6 měsíců).

12.3.2. Školení pro podnikatele

Podnikatelé budou klíčovými koncovými uživateli systému JePEK, avšak vzhledem k jejich potenciálně vysokému počtu nebude možné organizovat klasická školení. Proto bude školení řešeno formou elektronických vzdělávacích materiálů.

Základní principy práce se systémem budou podnikatelům vysvětleny prostřednictvím:

- **Podrobně strukturovaného textového manuálu** – obsahujícího přehled hlavních funkcionalit, nejčastější scénáře užívání a řešení základních problémů.
- **Interaktivních video-návodů** – které uživatele provedou konkrétními úkony v systému, například přihlášení nebo přístup k firemním údajům.
- **Často kladených dotazů (FAQ)** – zaměřených na řešení nejběžnějších problémů a nejasností.

Tento přístup zajistí maximální dostupnost školení bez nutnosti organizace prezenčních kurzů. Současně podnikatelé získají možnost kdykoliv si používání systému zopakovat a vyhledat potřebné informace dle své aktuální potřeby.

12.4. Školení pro pracovníky MPO

Pracovníci Ministerstva průmyslu a obchodu (MPO) budou mít zásadní roli při správě a metodickém vedení systému JePEK. Proto budou proškoleni **v rámci implementačního projektu**, a to v rozsahu odpovídajícím jejich pracovním úkolům.

Zaškolení bude zahrnovat:

- Obecné seznámení se systémem a jeho funkcionalitami.
- Metodické postupy a pravidla práce v systému.
- Správu uživatelských účtů a oprávnění v rámci MPO.
- Řešení specifických případů a komunikaci s kontrolními orgány a podnikateli.

Školení bude organizováno prezenční i online formou, aby byla zajištěna maximální efektivita a dostupnost pro všechny potřebné pracovníky MPO.

12.4.1. Školení pro kontrolní orgány

Kontrolní orgány budou využívat systém JePEK ke koordinaci kontrolní činnosti a přístupu k datům potřebným pro jejich práci. S ohledem na jejich potřeby bude školení organizováno **hybridní nebo plně online formou**, přičemž zajištění zaškolení bude koordinovat MPO ve spolupráci vedením a metodickým vedením příslušného kontrolního orgánu a také s Poskytovatelem systému.

Školení pro kontrolní orgány bude zahrnovat:

- Úvodní seznámení se systémem – základní orientace v rozhraní, vyhledávání, vstupy dat.
- Postupy kontroly a validace údajů v systému.
- Zpracování výsledků kontrol a komunikace s MPO.
- Bezpečnostní pravidla a oprávnění při práci s citlivými daty.

V případě změn v systému nebo nových funkcionalit bude zajištěno centrální školení jednou pro všechny kontrolní orgány.

12.4.2. Pravidelné přeškolování kontrolních orgánů

Struktura školení bude mezi Poskytovatelem a Objednatelem navržena tak, aby odpovídala specifickým potřebám jednotlivých skupin uživatelů a umožnila efektivní osvojení si systému JePEK.

Četnost školení je dále definována v SLA podmínkách, případně bude odpovídat ad hoc potřebám v návaznosti na update systému, či jiné uživatelsky významné události.

13. PROVOZ SYSTÉMU

Provoz systému bude realizován na základě jednotlivých provozních služeb a z nich odpovídajících činností. Tyto služby budou definovány a nabídnuty Poskytovatelem. Provozní služby budou součástí katalogu služeb, kdy Poskytovatel popíše jejich účel, typické kroky, spouštěcí impulzy, typická trvání, očekávaní četnosti provedení, výstupy.

O provedených službách bude Poskytovatel vést provozní deník a reportovat o nich v provozní zprávě, se kterou bude pravidelně seznamovat odborné útvary MPO.

13.1. ZÁLOHOVÁNÍ

Požadavky na zálohování, obnovu a testování zálohování zaměřeny na zajištění vysoké dostupnosti a ochrany dat proti ztrátám nebo poškození.

Zálohování bude prováděno pravidelně, ideálně automatizovaně, s přiměřenou frekvencí, která odpovídá dynamice změn dat (například denně nebo týdně).

Zálohy budou uchovávány na více geografických místech pro zvýšení odolnosti proti výpadkům v dané lokalitě.

Obnova dat by měla být rychlá a snadno proveditelná, přičemž obnova by měla být testována pravidelně, aby se zajistilo, že systém je schopen plně obnovit jakýkoli typ ztráty dat, a to v co nejkratším čase dle parametrů RPO a RTO domluvených v průběhu projektu. Testování zálohování bude zahrnovat ověření integrity záloh a provedení simulovaných scénářů obnovy, aby se zajistilo, že proces bude fungovat správně i v reálných podmínkách, například při kritických selháních. Na tomto testování se budou podílet i pracovníci MPO tak, aby obnovy v případě nutnosti byli schopni provést vlastními silami.

Celý proces zálohování a obnovy bude navržen Poskytovatelem a průběžně Poskytovatelem dokumentován.

13.2. Aplikační monitoring a dohled

Z business pohledu bude monitoring aplikace zaměřen především na sledování klíčových ukazatelů, které přímo ovlivňují obchodní výkon a uživatelskou spokojenost.

Aplikační monitoring bude obsahovat:

- sledování frekvence použití systému JePEK jednotlivými uživateli, což pomáhá identifikovat vzory chování a optimalizovat kapacity systému dle aktuální poptávky.,
- množství zpracovaných záznamů o kontrolách, což ukazuje na výkon a efektivitu systému JePEK, zejména v obdobích špičkového zatížení,
- sledování typických chyb a incidentů, jako jsou neúspěšné přihlášení, chyby při ukládání dat nebo problémy při komunikaci mezi frontendovými aplikacemi a centrální databází, což je klíčové pro rychlou detekci a nápravu problémů, které mohou negativně ovlivnit uživatelskou zkušenost nebo zpomalit procesy,
- schopnost generovat reporty a analýzy, které poskytují MPO přehled o výkonu aplikace, identifikují potenciální úzká místa nebo příležitosti pro optimalizaci, a umožňují včasné reakce na problémy, které by mohly mít vliv na funkčnost systému.

13.3. Infrastrukturní monitoring a dohled

Požadavky na monitoring systému zahrnují nasazení robustního nástroje pro sledování výkonu, dostupnosti a bezpečnosti všech klíčových komponent systému, včetně serverů, databází, aplikací a síťových zařízení.

Monitoring by měl pokrývat širokou škálu metrik, jako je využití CPU, paměti, diskového prostoru, latence síťového připojení, a stavy služeb.

Použitý monitorovací nástroj bude schopný generovat alarmy v reálném čase na základě definovaných prahových hodnot, čímž umožní rychlou reakci na případné problémy. Důležitou součástí je možnost shromažďování a vizualizace historických dat pro analýzu trendů a predikci možných problémů.

Vyhodnocování monitoringu by mělo být automatizováno tak, aby bylo možné snadno identifikovat anomálie a kritické incidenty, a to jak v reálném čase, tak v dlouhodobém horizontu. Administrátoři by měli mít možnost konfigurace notifikací a eskalace problémů v případě, že určité události zůstanou nevyřešeny. Systém bude umožňovat integraci s dalšími nástroji pro správu incidentů, aby se zajistilo rychlé a efektivní řešení problémů bez nutnosti manuálních zásahů.

Poskytovatel komplexně zajistí služby dle parametrů SLA, které jsou specifikovány v příloze č. 4 - SLA.

13.4. STRATEGIE OBNOVY

13.5. Strategie obnovy

Způsob zálohování, archivace a obnovy záloh nebo dat z archívů navrhne a zajistí Poskytovatel. Postupy a převzetí know-how pracovníky MPO budou předmětem akceptační procedury.

13.6. Patchování, upgrade

Pravidelné patchování a upgrady infrastruktury budou předmětem provozních a servisních služeb (provoz a maintenance), které bude zajišťovat Poskytovatel.

Vlastní zajištění aktuálnosti infrastrukturních technologií bude vycházet z jejich aktualizací a kritičnosti patchů a upgradů, kdy Poskytovatel zajistí, aby se u žádné technologie nedostal mimo podporu výrobce.

Způsob, postup, testy a komunikaci o plánovaném a prováděném patchování a upgradech zajistí Poskytovatel.

13.7. Aktualizace neprodukčních prostředí

Aktualizace neprodukčních prostředí bude probíhat dle specifických nároků jednotlivých prostředí pomocí stejných či obdobných dokumentovaných postupů.

13.8. Neprodukční prostředí

Každé prostředí má svůj specifický účel a slouží k jiným fázím životního cyklu systému. Produkční prostředí je určeno pro reálný provoz, zatímco neprodukční prostředí podporují vývoj, testování a školení uživatelů.

Neprodukční prostředí budou připravena tak, aby splnila požadavky na systém vyžadované tímto dokumentem. To znamená, že jejich konfigurace, dostupnost a výkon budou odpovídat potřebám jednotlivých fází vývoje a provozu. MPO předpokládá, že budou vytvořena následující prostředí:

- **Produkční prostředí** – Slouží k ostrému provozu systému s reálnými daty a uživateli. Toto prostředí musí splňovat vysoké požadavky na dostupnost, bezpečnost a výkon. Jakékoli změny nebo aktualizace systému zde musí být nasazovány řízeným způsobem, například přes proces řízení změn (Change Management).
- **Školící prostředí** – Je určeno pro výcvik a zaškolování uživatelů systému. Obvykle obsahuje data simulující reálné scénáře, ale nepracuje s citlivými produkčními informacemi. Toto prostředí umožňuje uživatelům bezpečně se seznámit s funkcemi systému bez rizika ovlivnění reálného provozu. Může být shodné s testovacím prostředím, pokud bude objednatel v rámci spolupráce tak požadovat.
- **Testovací prostředí** – Slouží k provádění funkčních a integračních testů. Toto prostředí by mělo co nejvěrněji odpovídat produkční konfiguraci, aby bylo možné identifikovat a odstranit chyby před nasazením systému do ostrého provozu. V rámci testovacího prostředí mohou být vytvořeny další specifické podvarianty, například pro automatizované testování nebo bezpečnostní audity.
- **Vývojové prostředí** – Určeno pro práci vývojářů při implementaci nových funkcionalit a opravách chyb. Na rozdíl od testovacího prostředí zde mohou probíhat časté změny a experimentování. Vývojové prostředí nemusí mít stejnou infrastrukturu jako produkční systém, ale mělo by umožnit snadný přenos změn do testovacího prostředí.

- **Referenční prostředí** (na základě konkrétní domluvy) – Slouží k ověřování produkčních chyb, které se vyskytly v ostrém provozu. Toto prostředí by mělo obsahovat co nejpřesnější kopii produkčních dat (s anonymizací citlivých údajů) a umožnit reprodukci a analýzu chyb bez zásahu do běžícího provozu.

Každé z uvedených prostředí by mělo být správně odděleno a řízeno tak, aby se minimalizovala rizika spojená s nekontrolovanými zásahy do produkčního provozu. Přístupová práva, monitoring a pravidla nasazování změn by měly být přizpůsobeny konkrétnímu účelu každého prostředí.

13.9. Servisní model

Efektivní správa a provoz informačního systému JePEK a jeho související infrastruktury vyžaduje jasně definované procesy a postupy, které zajistí jeho stabilitu, bezpečnost a plynulý chod. Veškeré činnosti související se změnami aplikace, jejích dat nebo infrastruktury, které je nutné administrátorsky provádět, budou systematicky spravovány v rámci provozního katalogu služeb.

Tento katalog bude zahrnovat všechny známé postupy zásahů do systému, které mohou být iniciovány různými podněty, například:

- **Monitoring IT stavu aplikace** – pravidelná kontrola výkonu, zátěže, dostupnosti a bezpečnostních událostí, na základě které mohou být prováděny optimalizace konfigurace, rozšíření infrastruktury či preventivní zásahy eliminující rizika výpadků.
- **Monitoring business stavu aplikace** – sledování obchodních procesů a metrik, jako je objem zpracovaných žádostí, rychlost odezvy systému, chybovost transakcí nebo trendy v uživatelském chování, které mohou indikovat potřebu úprav systému pro zajištění jeho optimální funkčnosti.
- **Pravidelně opakované úkony** – činnosti, které je třeba provádět v předem definovaných intervalech, jako jsou databázové údržby, revize oprávnění, kontrola logů, zálohování, archivace dat či aplikace bezpečnostních aktualizací.
- **Změny na vyžádání uživatelů** – úpravy nastavení systému, správa přístupových práv, konfigurace specifických funkcionalit nebo změny ve struktuře datových výstupů podle potřeb uživatelů.

Vedle standardních administrátorských úkonů katalog služeb zahrne také **servisní a maintenance služby**, které typicky řeší:

- **Nové a neočekávané problémy** – incidenty, které vyžadují rychlou analýzu, diagnostiku a řešení, například při nečekaných chybách systému, narušení provozu nebo výpadcích služeb.
- **Vyjasnění požadavků s uživateli** – situace, kdy je třeba konzultovat specifické požadavky či problémy se zástupci uživatelů, ať už jde o nejasnosti v chování systému, potřebu změny workflow nebo validaci nových funkcionalit.
- **Analýzu systémových anomálií a zajištění stability provozu** – například v případech, kdy se objeví neobvyklé chování systému, které nevede k okamžitému výpadku, ale může indikovat hlubší technické problémy vyžadující důkladné šetření.

Tyto dva hlavní okruhy služeb – **provozní katalog služeb** a **servisní a maintenance služby** – dohromady vytvářejí **servisní model péče o systém JePEK a jeho související infrastrukturu**. Tento model stanoví rámec pro řízení změn, reakce na incidenty a průběžnou optimalizaci provozu systému JePEK.

Dokumentace servisního modelu bude důležitou součástí celkové správy systému a stane se předmětem formálního schválení a akceptace pracovníky MPO. Tento proces zajistí, že všechny definované služby odpovídají potřebám uživatelů, provozním požadavkům systému a bezpečnostním standardům, a umožní jasné vymezení odpovědností mezi provozovatelem systému a uživateli.

13.10. Obecná definice SLA

13.10.1. ZÁKLADNÍ POJMY

13.10.1.1. SLEDOVANÉ OBDOBÍ

Dodržování garantovaných parametrů se sleduje v průběhu s Poskytovatelem domluveného intervalu.

13.10.1.2. VADA SLUŽBY

Vadou poskytované služby se rozumí stav, kdy jeden nebo více parametrů služby jsou horší než technické parametry uvedené v technické specifikaci služby nebo stav, kdy je provoz služby znemožněn z důvodů na straně Poskytovatele.

13.10.1.3. UDÁLOSTI VYŠŠÍ MOCI

Za Vadu ve smyslu SLA se nepovažuje Vada způsobená vyšší mocí, tj. živelnou pohromou (záplavy, požár, zemětřesení, plošné výpadky rozvodu elektrické energie apod.), válečným konfliktem nebo teroristickým útokem anebo jinými podobnými událostmi, jež nastaly nezávisle na vůli Poskytovatele a brání mu ve splnění jeho povinnosti, jestliže nelze rozumně předpokládat, že by Poskytovatel tuto vadu nebo její následky odvrátil nebo překonal a dále, že by v době vzniku závazku tuto překážku předvídal. Uvedené případy nejsou považovány za poruchy na straně Poskytovatele a nejsou započítávány ani do dostupnosti, ani do délky vady.

13.10.1.4. ZAČÁTEK VADY

Za začátek vady se pro určení doby trvání vady služby považuje čas jejího ohlášení Objednatelem v době trvání vady postupem uvedeným dále.

13.10.1.5. DOBA REAKCE

Doba mezi začátkem vady, začátkem identifikace její příčiny a informováním Objednatele o krocích vedoucích k jejímu odstranění a o předpokládané době jejího ukončení je nazývána Doba reakce (odezvy).

13.10.1.6. PRŮBĚŽNÁ INFORMACE O VADĚ

V případě, že délka vady překročí Termín pro odstranění, bude Poskytovatel pravidelně 1x denně informovat Objednavatele o stavu řešení poruchy, jejím rozsahu a předpokládaném termínu nápravy.

13.10.1.7. PŘERUŠENÍ Z DŮVODU PLÁNOVANÝCH PRACÍ NEBO ÚDRŽBY

Přerušení z důvodu plánovaných prací nebo údržby je takové přerušení služby, které je oznámeno Objednateli **do 15:00 hodin** dne předcházejícímu dne plánovaných prací. Veškerá údržba a práce budou plánovány tak, aby byl minimalizován dopad přerušení služby na Objednatele, a budou vykonávány v čase mezi **24:00 až 7:00** s výjimkou prací, které je nutno provést v denní době.

13.10.2. NAHLÁŠENÍ VAD

1.1. Hlášení Vad Poskytovateli bude provedeno Ohlašovatelem, a to přímým zadáním Vady do Helpdesku, odesláním e-mailu nebo telefonátem na kontaktní číslo Helpdesk, přičemž Ohlašovatel je povinen uvést popis Vady, a to v následujícím rozsahu:

a) krátký a rámcově výstižný název Vady;

b) identifikace části Předmětu Plnění, které se Vada týká;

c) určení prostředí (Testovací prostředí, Produkční prostředí);

d) detailní popis Vady, průvodních jevů a všech významných souvisejících informací;

e) kategorii Vady (**A, B, C**);

f) identifikaci Ohlašovatele.

1.2. V případě, že některá z náležitosti dle výše uvedeného odstavce **2.**Chyba! Nenalezen zdroj odkazů. chybí nebo je nedostatečná a Poskytovatel si ji nemůže sám zajistit, může si Poskytovatel vyžádat její doplnění od Ohlašovatele; tato skutečnost však nemá vliv na určení Času nahlášení Vady, ledaže bez tohoto doplnění hlášení Vady postrádá informaci natolik podstatnou, že bez ní objektivně nelze přistoupit k řešení Vady.

1.3. Je-li Vada nahlašována zadáním do Helpdesku, pak se za Čas nahlášení Vady považuje čas vytvoření ticketu v Helpdesku. Je-li Vada nahlašována písemně na e-mailovou adresu, pak se za Čas nahlášení Vady považuje čas odeslání e-mailu z e-mailového serveru Ohlašovatele, nebo v případě hlášení Vady telefonicky čas ukončení telefonického hovoru. Poskytovatel je povinen prokazatelným způsobem bezodkladně potvrdit přijetí nahlášení Vady, a to vždy prostřednictvím Helpdesku. Nepotvrdí-li Poskytovatel přijetí Vady, nemá to vliv na Čas nahlášení Vady.

1.4. Poskytovatel se zavazuje po dobu poskytování Plnění evidovat všechny nahlášené Vady a způsob jejich řešení, včetně časových údajů o průběhu řešení jednotlivých Vad ve Výkazech.

1.5. Není-li v Servisní smlouvě, jejích přílohách anebo Technické specifikaci stanoveno jinak, za Čas nahlášení Vad považuje Čas nahlášení Požadavku.

13.10.3. Klasifikace poruchových stavů (vad a poruch) a režim časové podpory

13.10.3.1. Kategorie vad a poruch

- **Vada kategorie A** znamená kritickou vadu, která má zásadní dopad na základní funkce Sytému, kdy se například nejde do Systému přihlásit. Dále je ohrožena bezpečnost dat a výsledky zpracování dat vykazují zjevné faktické chyby/vady. Dochází k poruchám v databázi a souvisejících aplikačních služeb, které způsobují výpadky Systému. Nedochází k přenosu dat mezi Systémem a externími Systémy mimo perimetr Objednatele.
- **Vada kategorie B** znamená vadu umožňující provoz základních funkcí Systému, kdy dochází k bezvadnému přenosu dat mezi cílovým Systémem a externími Systémy mimo perimetr Objednatele. Zároveň tento druh vady nemá vliv na kvalitu ani na bezpečnost dat a výsledky zpracování výsledných dat. Nejsou například funkční nadstavbové reportovací nástroje nebo filtrování dat je nedostupné.
- **Vada kategorie C** znamená vadu, která není Vadou kategorie A anebo B (např. špatná grafická úprava aplikace, špatný pravopis u nápovědy apod.).

13.10.3.2. Za provozní vadu systému se pro účely této Smlouvy nepovažuje:

- Plná či částečná nedostupnost Systému, způsobená omezením služeb externího systému mimo správu Poskytovatele, na kterém je Systém funkčně závislý (např. používané základní registry a rejstříky státní správy, aj.).
- Objednatelem schválená provozní odstávka Systému.
- Nedostupnost a zotavení Systému z katastrofy způsobené vyšší mocí.

13.10.3.3. Pro dohodu o úrovni poskytovaných služeb Systému (SLA) platí tato základní pravidla

- **Vada kategorie A**

  Termín pro odstranění Vady kategorie A je určen na 1 den (24h). Odstraněním vady Systému kategorie A se rozumí i výrazné snížení dopadů dotčené vady, které způsobí její rekvalifikaci na provozní vadu Systému kategorie B. Rekvalifikace vady Systému musí být Poskytovatelem navržena a Objednatelem schválena.

Případná sankční sleva je vždy zahájena ihned po uplynutí Termínu pro odstranění vady. Za každou započatou hodinu trvání vady kategorie A bude na měsíční cenu Služby provozu a dostupnosti aplikována sleva ve výši závislé na typu provozního režimu a časového období takto:

Provozní režim Systému	Časové období	Sleva za každou hodinu (z ceny měsíčního provozu)
Normální	Pracovní týden (Po - Pá)	0,6 %
	Víkend (So-Ne, svátek)	0,3 %

Provozní odstávka Systému musí být Poskytovatelem písemně oznámena a Objednatelem schválena minimálně 48 hodin před jejím započetím (pro vyloučení pochybností Objednatel není povinen oznámenou odstávku Systému schválit). Objednatelem neschválená provozní odstávka Systému nebo Přerušení mimo vymezený čas či nahlášení pozdě je provozní vadou kategorie A.

- **Vady kategorie B a C**

Kategorie	Termín pro odstranění vady	Sleva za den
Vada kategorie B	Do 2 dnů	Dohodnutá sleva 4,7 % Kč za každý započatý den po termínu pro odstranění vady
Vada kategorie C	Do 5 dnů	Dohodnutá sleva 3,3 % Kč za každý započatý den po termínu pro odstranění vady

Odstraněním vady Systému kategorie B se rozumí i výrazné snížení dopadů dotčené vady, které způsobí její rekvalifikaci na provozní vadu Systému kategorie C. Rekvalifikace vady Systému musí být Poskytovatelem navržena a Objednatelem schválena. V okamžiku potvrzení rekvalifikace vady Systému ze strany Objednatele dojde k zahájení termínu pro odstranění vady Systému kategorie C.

Pozn.: Všechny slevy se počítají z cen bez DPH.

13.10.4. ČASOVÉ REŽIMY GARANTOVANÉ Funkčnosti

Poskytovatel poskytuje podporu a dohled za smluvně sjednaných cenových podmínek v **následujících časových režimech**, kdy je nezbytné **garantovat funkčnost**:

Časový režim	Požadovaná doba dostupnosti	Maximální doba výpadku	Maximální součet výpadků
Pracovní den	24 hodin za den	24 hodin	96 hodin za rok
Nepracovní den	12 hodin za den, tj od 8:00 do 20:00	48 hodin	144 hodin za rok

Sankce za překročení maximálního součtu výpadků je 1,2 % z roční ceny Služeb provozu a dostupnosti za každou započatou hodinu.

13.10.5. Další požadované služby

13.10.5.1. Strategický rozvoj systému

- Poskytovatel se zavazuje **průběžně analyzovat** potřeby objednatele a navrhovat vylepšení.
- Poskytovatel předloží na základě požadavku Objednatele roadmapu s navrhovanými zlepšeními, a to v čase po vzájemné dohodě.
- Minimálně 1x ročně proběhne strategické setkání k diskusi o rozvoji systému.

13.10.5.2. Proaktivní monitoring a optimalizace výkonu

- Průběžná pravidelná analýza výkonu systému s cílem prevence problémů.
- Průběžná povinnost navrhovat optimalizační opatření.
- Na základě předchozího požadavku zajištění škálovatelnosti systému, a to v čase po vzájemné dohodě.

13.10.5.3. Pravidelné konzultace a podpora

- Minimálně 60 hodin odborných konzultací ročně.
- Pravidelná fyzická školení uživatelů (minimálně 8 hodin ročně).
- Pravidelné on-line školení uživatelů (minimálně 25 hodin ročně).
- Analytické práce a integrační práce s jinými systémy (minimálně 100 hodin ročně).

13.10.5.4. Distribuce aktualizací a správa verzí

- Pravidelný release management (např. kvartálně/pololetně).
- Kritické opravy aplikovány do 24 hodin.
- Povinnost testování aktualizací před nasazením.
- Rollback plán pro případné problémy.

13.10.5.5. Uživatelská dokumentace a návody

- Kompletní dokumentace dostupná online a pravidelně aktualizovaná.
- Každá větší aktualizace doprovázena popisem změn (release notes).
- Dokumentace obsahuje uživatelské manuály, FAQ a technickou dokumentaci.

13.10.5.6. Helpdesk a podpora uživatelů

- Dostupný helpdesk minimálně ve standardní pracovní době.
- Systém ticketingu pro sledování stavu požadavků.
- Možnost prioritizace požadavků podle dopadu na provoz.

13.10.5.7. Pravidelný reporting a zpětná vazba

- Přehledy SLA metrik (dostupnost, incidenty, doba řešení) v rámci Sledovaného období.
- Čtvrtletní setkání se zákazníkem k hodnocení provozu.
- Pravidelné průzkumy spokojenosti uživatelů.

13.10.5.8. Plán obnovy po havárii (Disaster Recovery Plan)

- Poskytovatel musí mít zpracovaný a pravidelně aktualizovaný plán obnovy systému.

- Plán musí zahrnovat procesy obnovy v případě výpadku, katastrofy nebo kybernetického útoku.
- Pravidelné testování obnovy systému minimálně 1x ročně.
- Povinnost informovat objednatele o výsledcích testování a případných vylepšeních plánu.

14. ŘÍZENÍ PROJEKTU

V rámci řízení projektu je kladeno velké důraz na správu, kontrolu a koordinaci mezi jednotlivými zúčastněnými stranami, a to jak na úrovni projektového týmu, tak na straně Objednatele. Následující požadavky a principy vycházejí z role Objednatele a specifických očekávání pro efektivní řízení a realizaci projektu.

14.1. Projektový manažer

Projektový manažer (PM), je klíčovou osobou, která zajišťuje každodenní řízení a koordinaci projektu. PM je odpovědný za plánování, řízení rizik, alokaci zdrojů a kontrolu postupu projektu podle stanoveného plánu. Zároveň bude pravidelně komunikovat se všemi stranami zúčastněnými na projektu, monitorovat rozpočet a časový rámec, a také řídit kvalitu výstupů projektu. PM bude informován ze strany Poskytovatele o všech aspektech projektu a jeho odpovědnost spočívá v identifikaci potenciálních problémů a jejich řešení ještě před tím, než se stanou kritickými.

14.2. Steering Committee (Řídící výbor)

Řídící výbor, je skupina vysoce postavených zástupců MPO a kontrolních orgánů, kteří dohlíží na strategické rozhodování a poskytují podporu projektu na vyšší úrovni. Výbor byl ustanoven již v předchozích fázích projektu. Tento výbor je odpovědný za pravidelnou kontrolu pokroku projektu, vyhodnocování jeho výsledků a rozhodování o případných změnách v rozsahu, termínech nebo rozpočtu. Stejně tak rozhoduje o vysoce důležitých záležitostech, které projektový manažer nemůže vyřešit sám.

14.3. Statusy a reporting

Pravidelný reporting a statusové schůzky jsou klíčovým nástrojem pro sledování postupu projektu. Objednatel vyžaduje, aby byly pravidelně připravovány statusy, které poskytují jasný a strukturovaný přehled o aktuálním stavu projektu. Tyto statusy by měly zahrnovat nejen dosažené milníky a pokrok, ale také identifikované problémy, rizika a navržená opatření. Informace budou součástí pravidelných setkání s projektovým manažerem a ředitelem odboru, a také komunikovány ostatním zúčastněným stranám, aby bylo zajištěno, že všechny strany mají aktuální informace o stavu projektu.

14.4. Věcná a odborná koordinace, role IT oddělení MPO

Projekt bude podroben koordinaci jak na věcné, tak na odborné úrovni. Věcná koordinace je odpovědná za kontrolu souladu s požadavky a cíli projektu, zatímco odborný odbor zajišťuje, že aplikované technické a odborné metody jsou v souladu s standardy a metodikami MPO v dané oblasti. IT oddělení, ačkoli nemá ambici vykonávat přímo operativní práci na projektu, požaduje důkladné obeznámení s projektovými procesy a projektovými (mezi)výstupy, aby bylo schopno včas reagovat na mimořádné události nebo problémy v technologické oblasti.

14.5. Přebírání know-how – role IT

IT oddělení bude připraveno převzít zodpovědnost za projekt v případě mimořádných událostí, ale jeho role při běžném provozu bude omezená na podporu a dozor.
IT tým musí rozumět technickým aspektům projektu, zajišťovat správnou implementaci IT systémů a služeb, ale nemá ambici vykonávat denní operativní úkoly nebo spravovat samotný výstup projektu—systém JePEK.
V případě nutnosti ale IT MPO musí disponovat schopností řešit technologické problémy, proto přebírá veškerou dokumentaci a účastní se dílčích projektových činností s cílem získání know how.

14.6. HARMONOGRAM REALIZACE

Předpokládáme, že realizace proběhne etapově, dle harmonogramu a s ohledem na best practise, jednotlivé etapy budou podléhat dílčímu akceptačnímu řízení a vyhodnocení. Obecně předpokládáme tyto etapy s tím, že detailní harmonogram díla určí Zhotovitel s vědomím termínů dodání díla a jeho klíčových milníků, které určuje objednatel takto:

Klíčový milník A - Analýza systému

V rámci tohoto milníku je očekáváno provedení komplexní analýzy systému vycházející z business požadavků, vstupního zadání MPO a vlastní expertízy pracovníků Zhotovitele.

Předpokladem je provedení těchto činností:

1. Business a procesní analýza - Shromáždění a analýza požadavků od klíčových stakeholderů (MPO, kontrolní orgány, podnikatelé, veřejnost), mapování procesů souvisejících s kontrolami a jejich optimalizace v souladu s legislativními požadavky (kontrolní řád, GDPR, NIS2), definice klíčových funkcionalit systému – evidence kontrol, plánování, reportování, notifikace.
2. Návrh UI/UX (uživatelského rozhraní a zkušenosti) - Identifikace uživatelských scénářů a typů uživatelů (kontrolor, podnikatel, MPO administrátor), wireframy a prototypy hlavních obrazovek systému – navigace, dashboardy, formuláře, uživatelský výzkum a testování prototypu s vybranými uživateli pro zpětnou vazbu, zajištění přístupnosti a použitelnosti v souladu se standardy pro eGovernment.
3. Technický návrh systému - Definice technologické architektury – výběr vhodných technologií, návrh databázového modelu, API, integrace s externími registry (RŽP, ISZR, NIA, MPO), bezpečnostní analýza – návrh řízení přístupu (RBAC, certifikáty, OTP), auditních logů a souladu s NIS2, výkonová analýza a škálovatelnost – návrh infrastruktury umožňující budoucí rozšíření systému.
4. Testování konceptu a validace návrhu - Ověření navržené architektury z hlediska výkonu a bezpečnosti, validace UI/UX návrhu s vybranými uživateli a zapracování zpětné vazby, schválení specifikace systému a technologického návrhu MPO a klíčovými stakeholdery.

Klíčový milník B - 1. Funkční verze Aplikace AIS JePEK

V rámci tohoto milníku je očekáváno dodání první funkční verze JePEK umožňující realizovat základní činnosti určené jednotlivým uživatelským rolím systému.

Klíčový milník C - 1. Funkční verze Aplikace AIS JePEK v 1. fázi integrace

Nad rámec 1. funkčního prototypu (MVP) jsou dále implementovány funkce umožňující integraci na interní systémy dotčených kontrolních úřadů -> provedena základní integrace dat z následujících kontrolních orgánů:

- Český metrologický institut,
- Český úřad pro zkoušení zbraní a střeliva,
- Úřad pro technickou normalizaci, metrologii a státní zkušebnictví,
- Puncovní úřad,
- 1x útvar Ministerstva průmyslu a obchodu, který provádí kontroly.

Výše uvedené kontrolní orgány realizují ročně přibližně 3 000 až 5 000 kontrol.

Klíčový milník D - Funkční verze AIS JePEK (plná verze)

V rámci tohoto milníku bude po vybraném Poskytovateli požadováno v rámci akceptačního řízení, aby AIS JePEK byl: a) Finálně vyvinut, tzn. byly dokončeny vývojové práce z předchozího milníku, byl hotov UI/UX Design a byl dokončen Frontend a Backend vývoj. b) Byla provedena další integrace dat z následujících kontrolních orgánů:

- Krajské živnostenské úřady, Obecní živnostenské úřady, nebo
- Česká obchodní inspekce,

Výše uvedené subjekty jsou připraveny data dle potřeby na straně svých systémů poskytnout k integraci.

Výše uvedené kontrolní orgány realizují ročně přibližně 20 000 kontrol.

Komplexní přehled hodnocení milníků a jejich akceptace viz. **Příloha č. 6 – Harmonogram (Klíčové milníky, akceptace, fakturace).xlsx**

14.7. Rozvojové požadavky

Po dokončení vývojové fáze a akceptaci díla: Agendového informačního systému Jednotného portálu evidence kontrol (JePEK) by Objednatel měl zájem realizovat rozvojové požadavky zpravidla v níže uvedených základních oblastech, jejichž přesné vymezení bude známo až v čase realizace.

Současně Objednatel deklaruje, že na tyto rozvojové požadavky je alokováno maximálně 1 300 člověkodní, které budou po vzájemné dohodě Objednatele a objednatel, v předem odsouhlaseném rozsahu, postupně čerpány. V neposlední řadě Objednatel sděluje, že rozvojové požadavky předpokládá realizovat v období od roku 2027 do roku 2032.

Zamýšlené základní oblasti rozvoje: další rozvoj a zlepšení uživatelského rozhraní, integrace s dalšími systémy, rozšíření funkcionality, aplikace umělé inteligence (AI), školení a podpora uživatelů v souvislosti s rozvojem, konzultační služby ve vztahu k rozvoji.

Konzultace s uživateli: Poskytovatel se zapojí do pravidelných konzultací s klíčovými uživateli (úředníky i veřejností) za účelem pochopení jejich potřeb a požadavků. Na základě těchto konzultací poskytne návrhy na úpravy a rozvoj systému.

Zajištění kontinuálního vývoje: Poskytovatel zajistí průběžnou údržbu a rozvoj systému v souladu s novými legislativními a technologickými požadavky. Bude sledovat změny relevantní pro systém a navrhovat jejich implementaci tak, aby bylo zajištěno dlouhodobé fungování a efektivita řešení.

14.8. ANALÝZA RIZIK PROJEKTU

Zpracována v kapitole IDENTIFIKACE BUSINESS HROZEB A ZRANITELNOSTÍ

14.9. SOUČINNOST

Úspěšná implementace informačního systému pro koordinaci kontrolní činnosti vyžaduje aktivní součinnost na jeho straně. V této souvislosti žádáme Poskytovatele, aby detailně specifikoval požadovanou součinnost ze strany objednatele, a to jak z hlediska poskytování vstupních dat, tak z pohledu organizačních, technických a procesních aspektů. Zároveň očekáváme, že Poskytovatel identifikuje klíčové oddělení či role, které budou do procesu zapojeny (např. IT oddělení, právní oddělení, provozní složky či vedení organizace), a uvede rozsah jejich zapojení. Na základě těchto požadavků bude možné naplánovat potřebné kapacity a zajistit hladký průběh implementace.

MPO deklaruje, že počítá se zabezpečením součinnosti v následujících oblastech:

- Spolupráci v rámci detailního designu, kdy pracovníci MPO budou zajišťovat revize a oponentury navržených designů. Počet dní na revizi bude odvozen od počtu stran dokumentu, kdy na každých 20 stran je požadován jeden pracovní den.
- Zajištění a organizace spolupráce s kontrolními orgány. MPO bude zajišťovat schůzky, respektive součinnost kontrolních orgánů při integraci na úrovni managementu.
- Zajištění spolupráce s ostatními odbory ministerstva a dále zajištění spolupráce s jinými ministerstvy (ministerstvo vnitra, ministerstvo pro místní rozvoj, ministerstvo financí).
- Spolupráce s agenturami typu DIA.

Poskytovatel je očekáván jako aktivní a samostatný partner při návrhu a realizaci systému JePEK. Vedle splnění technických a funkčních požadavků MPO klade důraz na kreativní přístup, hledání optimálních řešení a schopnost přicházet s vlastními návrhy na vylepšení na základě vlastní znalosti problematiky. MPO bude zastávat především

kontrolní a koordinační roli, poskytovat zpětnou vazbu a nastavovat taktické a strategické směry rozvoje, přičemž se spoléhá na odborné know-how a iniciativu Poskytovatele při detailním návrhu a implementaci systému. Poskytovatel bude přicházet s řešeními a doporučeními, která MPO pouze schvaluje/neschvaluje.

Od Poskytovatele se dále očekává, že zajistí odbornou asistenci MPO v oblastech potřebných k zajištění registračních a schvalovacích procesů, které se týkají fungování dodávaného informačního systému jako systému státní správy.

Poskytovatel dále zajistí součinnost MPO pro presentace a zaškolení systému JePEK pro jiné orgány státní správy.

Poskytovatel nesmí požadovat nadměrnou nebo nepřesně definovanou součinnost, a dále by měl jasně stanovit, jak často a v jaké formě poskytne zpětnou vazbu.

14.10. AKCEPTAČNÍ KRITÉRIA

Detailní nastavení akceptačních kritérií bude obsahem návrhu smlouvy s Poskytovatelem. Obecně jde ale o splnění funkčních i nefunkčních požadavků stanovených tímto dokumentem případně dalšími výstupy, které vzniknou v průběhu realizace projektu.

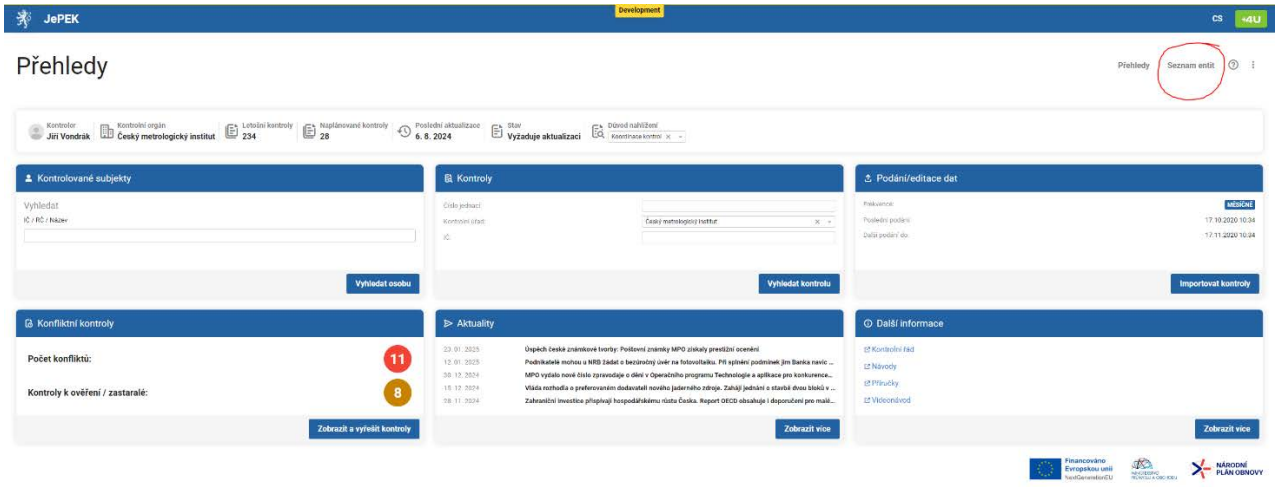
Obecně bude požadováno:

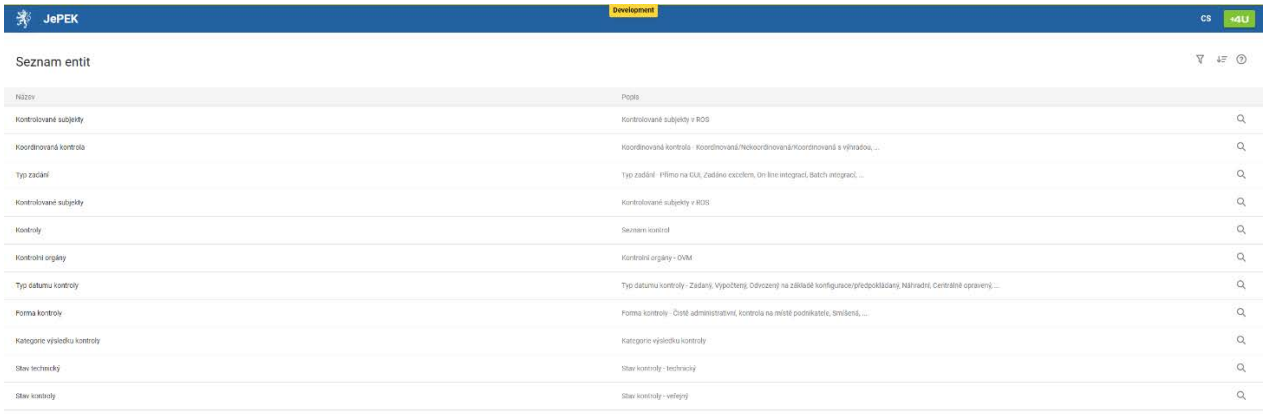
- Úspěšné provedení testů:
  - Factory acceptance testy (FAT)
  - User acceptance testy (UAT)
  - Penetrační testy
- Převzetí a schválení dokumentace odborem IT MPO
- Existuje exit plán odstoupení od cloudového provozování a realizace provozu on premise bez nutnosti programování aplikace.
- Data – importovaná data od KO (pokud bude nějaká forma importu součástí příslušné iterace)
- Pilotní provoz, kterým se rozumí potvrzení spolupráce s vybranými kontrolními orgány

15. Ukázka Aplikace JePEK fáze 1 (návrh možného řešení – konceptu)

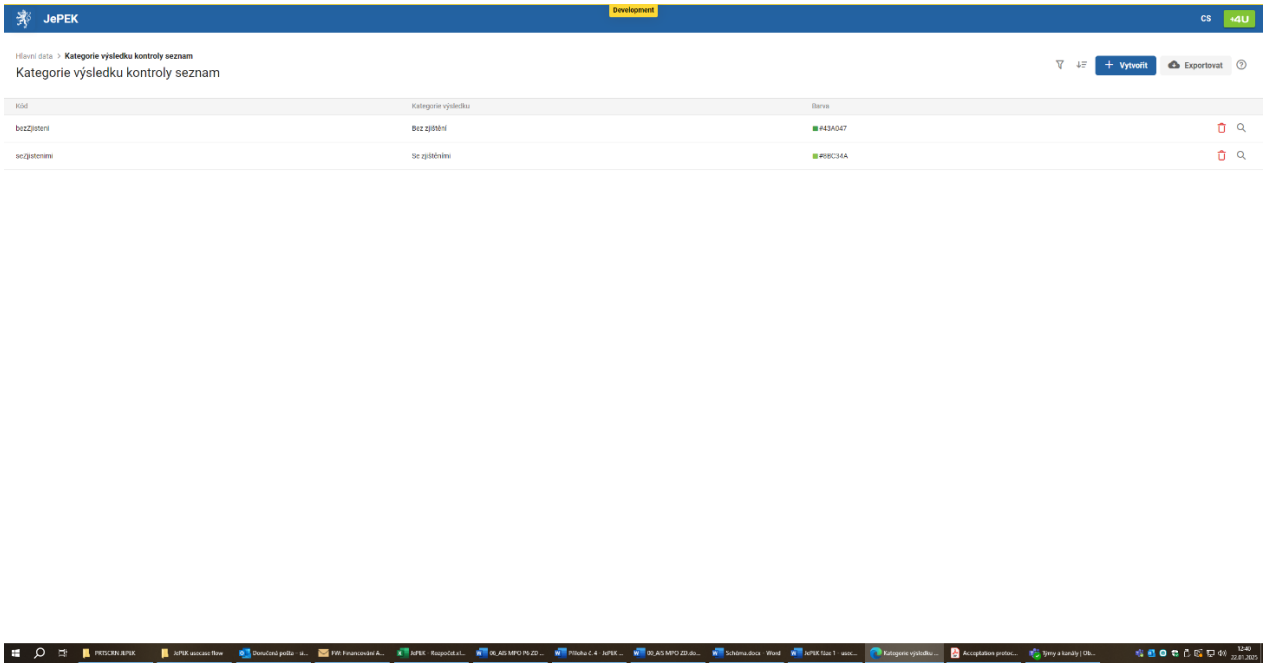
15.1.1. Seznam entit

Seznam entit poskytuje informace a popis jednotlivých parametrů.

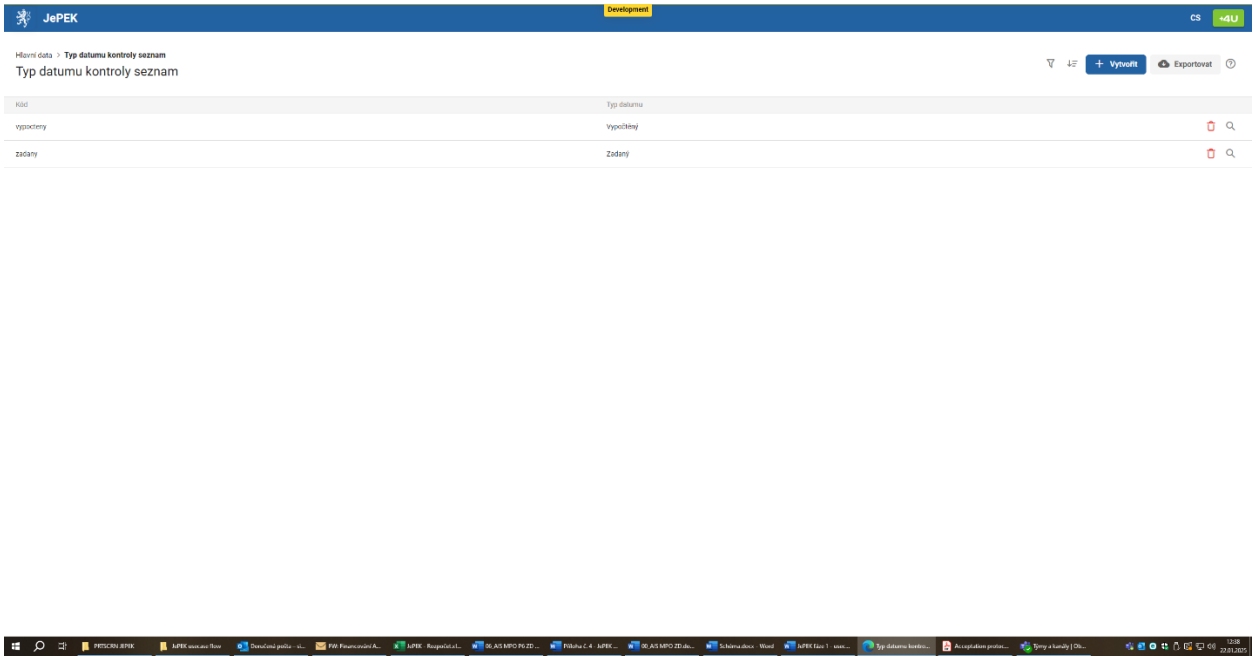




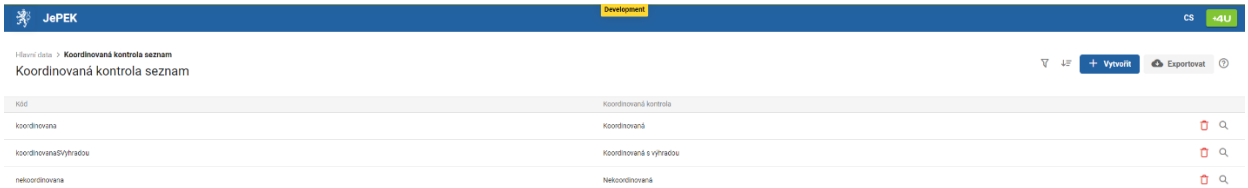
Seznam entit – Kategorie výsledku kontroly



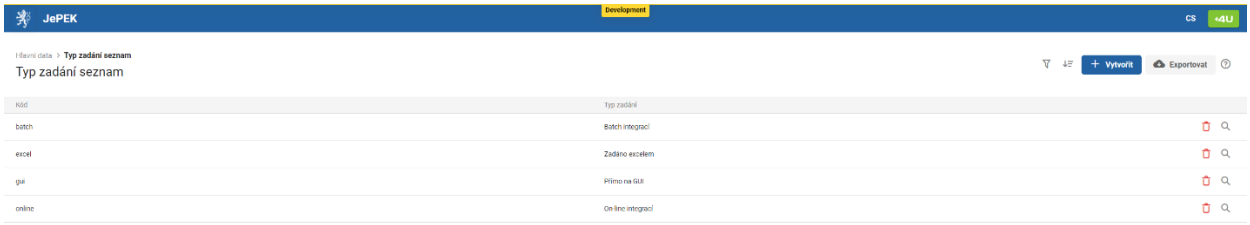
Seznam entit – Typ datumu kontroly



Seznam entit – Koordinace kontroly

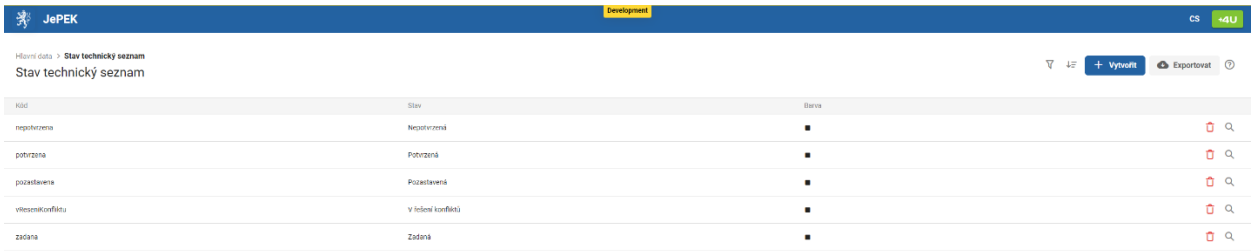


Seznam entit – Typ zadání

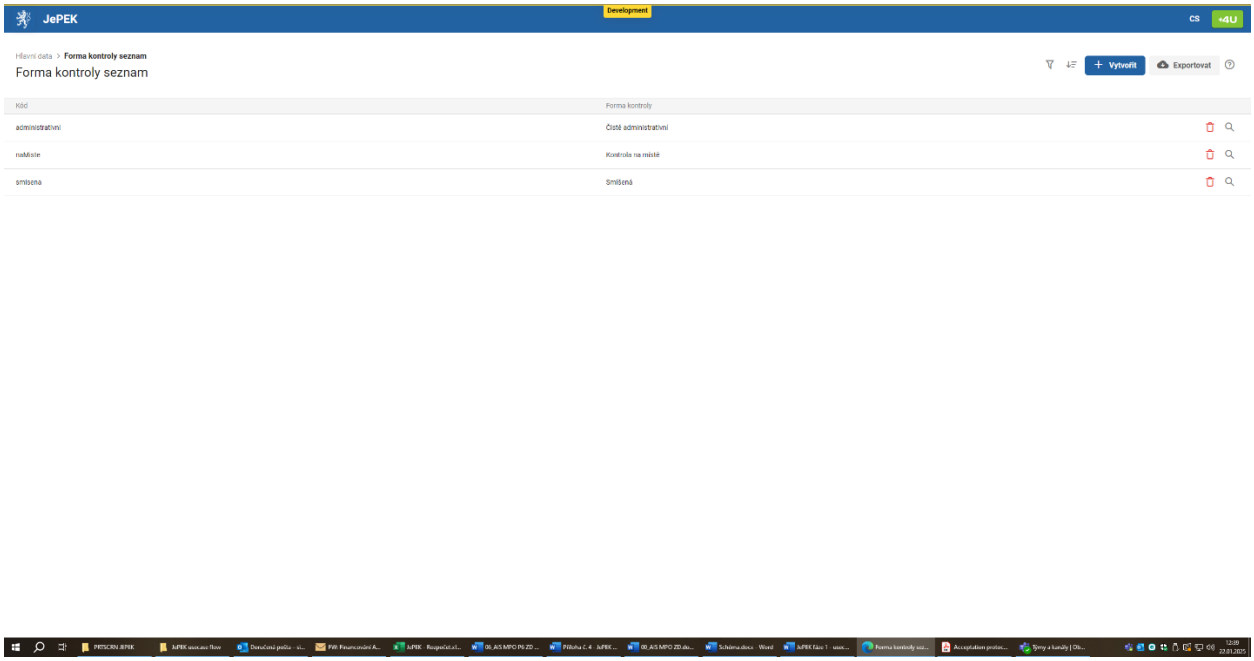


Seznam entit – Stav kontroly

Seznam entit – Stav technický

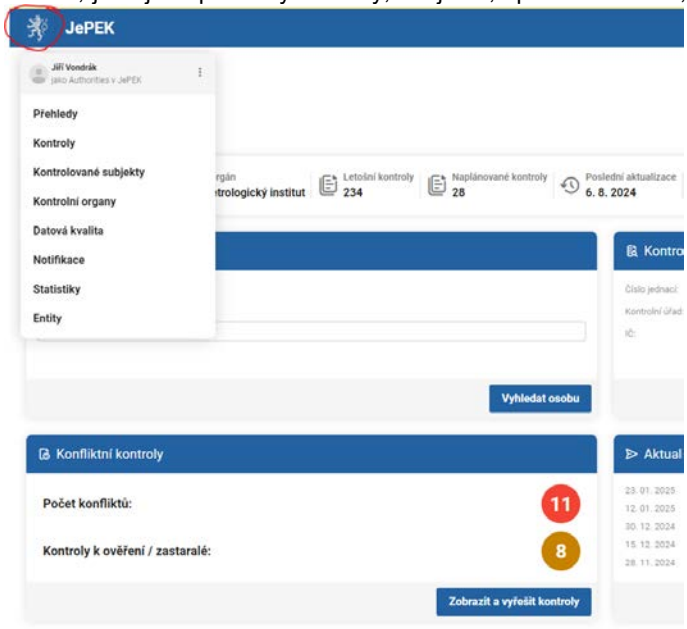


Seznam entit – Forma kontroly



15.1.2. Menu

Otevřením menu na hlavní obrazovce bude uživateli umožněna rychlá orientace v nabízených službách systému JePEK, jako jsou přehledy kontroly, subjektů, správa notifikací, statistické přehledy, správa datové kvality apod.



Rozpad ucecase:

Portál pro úředníka				
	BUC	L		Menu: Orgán (možnost výběru z více), Subjekt, Kontrola, Statistiky, Aplikace (About, nápovědy, odhlásit, přihlásit), Rychlé hledání

Pro Aplikaci JePEK ve fázi 1 byly použity následující technologie a licence:

Vrstva GUI

- HTML5
- CSS3
- JavaScript
- React (licence MIT)

Aplikační vrstva

- NodeJS (licence MIT)
- expressJS (licence MIT)

Databázová vrstva

- MongoDB (licence MongoDB SSPL - https://www.mongodb.com/legal/licensing/server-side-public-license)
- Azure BLOB storage (komerční licence Microsoft)

Obecně pro platformu jsou technologie viz obrázek.

16. Příloha: Algoritmus návrhu datumů koordinace kontroly

Algoritmus návrhu termínů pro koordinaci kontrol může být v budoucnu upravován o další pravidla či aspekty plánované nebo budoucí kontroly s tím, že příslušná pravidla mohou ovlivnit doporučení datumů pro plánovanou realizaci kontroly:

Vstupní data:

- ID_kontroly – povinné,
- Stav_věcný,
- Datum začátku (myšleno výkonu kontroly u kontrolované osoby),
- Datum konce (myšleno výkonu kontroly u kontrolované osoby),
- Typ kontroly,
- Flag vynutit koordinaci (override již koordinované kontroly, například pro editaci a změnu datumů),

Algoritmus zpracování:

1. **Zda se tím vůbec zabývat**
    1. Nezabýváme se případy:
        1. Pokud je kontrola na vstupu již koordinovaná (uvedeno na kontrole Koordinovaná = true a je vyplněn datum koordinace kontroly) a zároveň není nastaven flag vynutit koordinaci, pak návratový kód 03-Již koordinovaná
        2. Pokud je stav_veřejný již Probíhající, nebo Ukončený (případně další), pak návratový kód 01-Nemá smysl koordinovat-probíhající, ukončená
        3. Pokud datumy začátku na kontroly (respektive odvozený datum začátku) je v minulosti, pak návratový kód 01-Nemá smysl koordinovat-probíhající, ukončená
        4. Typ kontroly je vyplněn a v konfiguraci je uvedeno, že jde o čistě administrativní kontrolu (Administrativni = true), pak návratový kód 02-Nespadá do koordinace
    2. Systém vrátí na výstup příslušný stav a algoritmus končí
2. **Upravit datumy, aby je šlo použít**
    1. Pokud není vyplněno ano datum začátku ani datum konce kontroly, pak chyba CHYBNE_ZADANI_KONTROLY_KE_KOORDINACI (alespoň jeden datum musí být vyplněn) a algoritmus končí s návratovým kódem 00-Chybné údaje)
    2. Pokud není vyplněn Typ kontroly, pak Delka_trvání bude 1 (den) a pokračuji krokem výpočtu chybějících datumů tj. 2.4
    3. Dle Typu kontroly v číselníku/konfiguraci vyhledám hodnotu Typické trvání kontroly ve dnech
        1. Pokud naleznu hodnotu:
            1. Pokud je kratší než 1, pak Delka_trvání bude 1 (den)
            2. Jinak Delka_trvání bude vzata z konfigurace jako TypickaDelkauKO a zaokrouhlena na celá čísla nahoru
        2. Pokud nenalezeno, pak Delka_trvání bude 1 (den)

4. Pokud není vyplněn datum konce (logicky vyplněno datum začátku), pak datum konce := datum začátku + Delka_trvání -1
5. Pokud není vyplněn datum začátku (logicky vyplněno datum konce), pak datum konce := datum konce - Delka_trvání +1
6. Poznámka: Jednodenní kontrola trvá například od 16.8.2024 do 16.8.2024

3. **Nalezení termínového konfliktu**
    1. Systém nalezne všechny jiné kontroly na stejnou kontrolovanou osobou (*Pozor! Stejná neznamená stejné IČO nebo název, protože v lednu jsem mohl plánovat kontrolu na firmu Alfa s IČO1, která se přejmenovala/sloučila a od února vystupuje pod identitou Beta a IČO2, takže když nyní plánuji na jiné IČO, pak jde o konflikt*),
    na kterou je uvedena kontrola na vstupu (dle id_kontroly), které:
        1. Pokud je uvedena na kontrole na vstupu Provozovna (tj. vím, kde kontrola bude provedena, takže konflikt by byl je na stejné provozovně)
            1. Porovnám datumově kontroly na stejnou osobu a stejnou provozovnu, abych získal termínové konflikty formou porovnání intervalů na překryv tj jeden začne dříve, ale skončí po začátku druhého nebo začne po začátku ale před koncem druhého. Pozor rovnost hodnot znamená překryv, tedy jeden začne 18.8. a druhá skončí 18.8., pak se překrývají.
                1. Pokud nemám na kontrole vyplněny údaje, pak musím poradit podobně jako v bodě 2. s tím, že:
                    1. Pokud mám Datum protokolu, pak z typu kontroly pracuji hodnotami TypickaDobaOdMistaDoProtokolu, TypickaDelkauKO
                    2. Pokud mám Datum začátku, pak jako v bodě 2 (bereme, že začátek kontroly je začátek kontrolní činnosti na místě u kontrolované osoby)
                    3. Pokud mám Datum ukončení, pak jako v bodě 2 (bereme, že konec kontroly je konec kontrolní činnosti na místě u kontrolované osoby)
                    4. Poznámka: zvážit, zda již dopředu hodnoty nepředpočítat
            2. Pokud nějaké překrývající se kontroly naleznu, pak
                1. Systém nalezne dle konfigurace příbuzné kontroly tj. v číselníku Příbuzné kontroly, která obsahuje dvojice typů kontroly, které jsou navzájem příbuzné. Pak platí, že když A je příbuzné s B, pak B je příbuzné s A, tedy stačí jeden řádek (A, B).
                2. Z překrývajících se kontrol vyloučím ty kontroly, které jsou příbuzné s koordinovanou kontrolou
                3. Pokud nějaké konfliktní kontroly zbyly, pak nastavím návratový kód na 04-Konflikty a tyto kontroly uvedu do kolekce konfliktních kontrol na výstup a pokračuji dalším hlavním bodem tj. 4

3. Jinak porovnám datumově kontroly na stejnou osobu a jakoukoliv jinou tj. i nevyplněnou provozovnu, abych získal termínové konflikty na firmu jako takovou.
    1. Pokud takové jsou,
        1. Z překrývajících se kontrol vyloučím ty kontroly, které jsou příbuzné s koordinovanou kontrolou
        2. Pokud nějaké konfliktní kontroly zbyly, pak návratový kód nastavím na 11-Koordinovaná varování (konflikt na jiné provozovně) a pokračuji dalším hlavním bodem tj. 4
        3. Pokud nenaleznu, pak návratový kód nastavím na 10-Koordinovaná
    2. Pokud takové nenaleznu, pak návratový kód nastavím na 10-Koordinovaná

2. Pokud není uvedena na kontrole na vstupu Provozovna (poznámka: kde bude kontrola opravdu nevím, tak je konflikt všechno, protože centrála je taky provozovna)
    1. Porovnám datumově kontroly na stejnou kontrovanou osobu ať na porovnávané kontrole je a nebo není provozovna uvedena, abych získal termínové konflikty formou porovnání dvou intervalů na překryv.
    2. Pokud nějaké naleznu, pak
        1. Z překrývajících se kontrol vyloučím ty kontroly, které jsou příbuzné s koordinovanou kontrolou
        2. Pokud nějaké konfliktní kontroly zbyly, pak návratový kód nastavím na 04-Konflikty a tyto kontroly uvedu do kolekce konfliktních kontrol na výstup a pokračuji dalším hlavním bodem tj. 4
        3. Pokud nenaleznu, pak návratový kód nastavím na 10-Koordinovaná
    3. Pokud nenaleznu, pak návratový kód nastavím na 10-Koordinovaná

4. **Nalezení alternativního návrhu dle příbuznosti**
    1. Poznámka: jde o princip, že když jdou různé kontrolní orgány na stejnou nebo podobnou věc, pak ať přijdou společně
    2. Pokud je zjištěn v předchozím návratový kód jiný než 04-Konflikty, pak se tento hlavní krok neuplatní a systém pokračuje následujícím hlavním krokem
    3. Systém nalezne dle konfigurace příbuzné kontroly, tj. v číselníku Příbuzné kontroly, která obsahuje dvojice typů kontroly, které jsou navzájem příbuzné. Pak platí, že když A je příbuzné s B, pak B je příbuzné s A, tedy stačí jeden řádek (A, B).
    4. *Poznámka: následující princip ještě převést na výpočty v pracovních dnech.*
    5. Systém nalezne v konfliktních kontrolách ty kontroly, které jsou příbuzné s Koordinovanou kontrolou:
        1. Pokud žádné nejsou, pak systém nebude uvádět na výstup navrhované termíny dle příbuznosti a pokračuje dalším hlavním bodem

6. Systém vytvoří kolekci, která bude obsahovat Typ Start-Start i typ Konec-Konec pro každou příbuznou konfliktní kontrolu. Hodnoty v kolekci:
    1. Koordinovaná kontrola, s ní konfliktní příbuzná kontrola, Typ Start Start, Navrhované datum začátku koordinované kontroly := Datum začátku konfliktní koordinované kontroly, Navrhované datum konce koordinované kontroly := Navrhované datum začátku koordinované kontroly + Delka_trvání -1, Skore
    2. Koordinovaná kontrola, s ní konfliktní příbuzná kontrola, Typ Konec Konec, Navrhované datum začátku koordinované kontroly := Datum konce konfliktní koordinované kontroly - Delka_trvání +1 , Navrhované datum konce koordinované kontroly := Datum konce konfliktní koordinované kontroly , Skore
    3. Vyloučíme ty záznamy, kdy navrhované datum začátku kontroly - hodnota MinDníProPlánováníKOntroly z číselníku Typ kontroly pro datý typ kontroly - 1 <= Dnešní datum
    4. Skore vypočteme jako: Počet dní, ve kterých by byla kontrola dle navrhovaných datumů v souběhu s nějakou jinou příbuznou kontrolou (konflikt s příbuznými kontrolami jsou kladné body), mínus počet dní, při kterých by byla kontrola dle navrhovaných datumů v souběhu s nějakou jinou nepříbuznou kontrolou (konflikt s nepříbuznými kontrolami jsou záporné body body).
7. Na výstup vybereme takové navrhované hodnoty (záznamy z kolekce):
    1. pro každý typ tj Start Start a Konec Konec (pokud existují a nebyly vyloučeny) hodnotu s nejvyšším skore (to může bát i záporné),
        1. pokud by bylo takových variant více, pak vyberu takové hodnoty, které se v daném typu liší o menší počet dnů od původních hodnot ze vstupu (tedy minimální Absolutní hodnota (datum začátku ze vstupu do BR001 - Navrhované datum začátku koordinované kontroly)
        2. a pokud by takových bylo více, pak minimální hodnota Navrhované datum začátku koordinované kontroly
        3. a pokud i tak by bylo více, pak záznam v kolekci, který byl technicky dříve vytvořen

5. **Nalezení alternativního návrhu dle odstupu**
    1. Poznámka: jde o princip, že když jdou různé kontrolní orgány na stejnou nebo podobnou věc, pak ať přijdou jindy, aby podnikatel také mohl pracovat
    2. Pokud je zjištěn v předchozím návratový kód jiný než 04-Konflikty, pak se tento hlavní krok neuplatní a systém pokračuje následujícím hlavním krokem
    3. Systém najde pro tuto kontrolu data začátku a konce kontroly, aby měla odstup od ostatních kontrol právě globálním parametrem nastavený počet pracovních dnů (globální parametr MinDnyOdstup například na hodnotu 3).
        1. Výpočet posunu kontroly do minulosti:
            1. Opakuj, dokud (nenalezneš takové navrhované hodnoty pro posun do minulosti, které nebudou mít konflikt s žádnou jinou kontrolou) nebo (navrhované datum začátku kontroly - hodnota MinDníProPlánováníKOntroly z číselníku Typ kontroly pro datý typ kontroly - 1 <= Dnešní datum)

1. Naplnění navrhovaných hodnot:
    1. Vezmi minimální datum začátku kontroly všech konfliktních kontrol (tedy buď zadanou nebo předpočtenou hodnotu), od ní odečti hodnotu MinDnyOdstup, a dále odečti 1. Výslednou hodnotu použij jako Navrhované datum konce kontroly u kontrolované osoby.
    2. Jako Navrhované datum začátku kontroly u kontrolované osoby pak použit hodnotu Navrhované datum konce - Delka_trvání +1.
2. Nalezni konfliktní kontroly oproti navrhovaným datumům stejným způsobem, jako v bodě 3 Nalezení termínového konfliktu

2. Pokud byly nalezeny hodnoty, pak bude uvedena varianta na výstupu. Pokud nebyl nalezen termín posunu do minulosti, pak varianta uvedena na výstupu nebude.
3. Příklad:
    1. Je 1.1., MinDníProPlánováníKOntroly je 30 dnů tedy kontrolu musím naplánovat 20 dnů dopředu, Kontrola má typické trvání 1 den. Odstup je 3 dny a již naplánované kontroly jsou 31.1. - 2.2. a 8.1.-9.1. A já, pokud jsem plánoval na 9.1.-9.1. původně, pak nelze nalézt vhodný datum směrem do minulosti.

2. Výpočet posunu kontroly do budoucnosti:
    1. Opakuj, dokud nenalezneš takové navrhované hodnoty pro posun do budoucnosti, které nebudou mít konflikt s žádnou jinou kontrolou:
        1. Naplnění navrhovaných hodnot:
            1. Vezmi maximální datum konce kontroly všech konfliktních kontrol (tedy buď zadanou nebo předpočtenou hodnotu), k ní přičti hodnotu MinDnyOdstup, a dále přičti 1. Výslednou hodnotu použij jako Navrhované datum začátku kontroly u kontrolované osoby.
            2. Jako Navrhované datum konce kontroly u kontrolované osoby pak použit hodnotu Navrhované datum zařítku + Delka_trvání -1.
        2. Nalezni konfliktní kontroly oproti navrhovaným datumům stejným způsobem, jako v bodě 3 Nalezení termínového konfliktu
        3. Poznámka: nějaké datum do budoucnosti by mělo jít najít vždy

6. **Override Koordinace, pokud si kontrolovaný subjekt kontrolní orgán již prohlížel**
    1. Systém zjistí, zda si v poslední době (DisplayPeriodForCoordination, konfigurační parametr systému) nějaký reprezentant stejného kontrolního orgánu jako je zjišťovaná kontrola zobrazoval IČO klienta a jeho kontroly.
    2. Z id_kontroly systém zjistí, který kontrolní orgán plánuje kontrolu udělat.

3. Následně z tabulky přístupů (logy zobrazení) zjistí, zda už nějaký jiný reprezentant za poslední dobu (parametr DisplayPeriodForCoordination) již přistupoval k dané kontrolované osobě buď vizuálně přes UC Zobrazení detailu kontrolované osoby
4. Poznámka: kontrolovat, že zobrazení bylo v časovém období, které zahrnuje zjišťovanou kontrolu (protože budou existovat více variant zobrazení s omezeným datumovým rozsahem).
5. Pokud je nalezen takový záznam (někdo z KO si již klienta prohlížel) a zároveň byly nalezeny konflikty viz výše, pak
    1. návratový kód bude 12-Koordinovaná s konflikty
    2. jinak návratový kód bude 10-Koordinovaná, nebo 11-Koordinovaná varování (konflikt na jiné provozovně)), ale to je již nastaveno z předchozích kroků

7. Vytvoření výstupních struktur
    1. Vytvořím z výpočtů výše relevantní strukturu pro zpracování volajícím UC
    2. Vytvořím kolekce příbuzných kontrol pro varianty spojení příbuzných kontrol

Výstupy

Výstupní atributy:

- ID_kontroly
- Dnešní datum
- Návratová kód koordinace (enum: 00-Chybné údaje, 01-Nemá smysl koordinovat-probíhající, ukončená, 02-Nespadá do koordinace, 03-Již koordinovaná, 04-Konflikty, 10-Koordinovaná, 11-Koordinovaná varování (konflikt na jiné provozovně)), 12-Koordinovaná s konflikty
- Kolekce konfliktů - jen pro kód 04 Konflikty
    - id konfliktní kontroly (dle původního zadání)
    - typ konfliktu (Termínový, frekvenční)
- Návrh alternativ - jen pro kód 04 Konflikty
    - Alternativa spojení příbuzných kontrol – uvedeno, jen když existuje
        - Varianta A: konec-konec - jen když existuje
            - kolekce příbuzných id_kontrol, které jsou v konfliktu s navrženým datumem kontroly (poznámka: ty by se měly dostat až k uživateli, protože těm orgánům, co budou provádět tyto kontroly zavolá a domluví se s nimi)
            - Navrhované datum začátku
            - Navrhované datum konce
        - Varianta B: začátek-začátek – uvedeno, jen když existuje
            - kolekce příbuzných id_kontrol, které jsou v konfliktu s navrženým datumem kontroly
            - Navrhované datum začátku

- Navrhované datum konce

- Alternativa odstupu
  - Varianta C: Posun do minulosti – uvedeno, jen když existuje
    - Navrhované datum začátku
    - Navrhované datum konce
  - Varianta D: Posun do budoucnosti – uvedeno vždy
    - Navrhované datum začátku
    - Navrhované datum konce

Logy:

1. volání i výstup jsou logovány pro možnost dohledání, zpracování

16.1.1. Ostatní požadované usecases, rozpad:

Ostatní				
	OST	L		Webová nápověda k používání aplikace
	OST	L		Webová nápověda k metodice (obecně veřejná)
	OST	M		Informace - disclaimer - zpracování osobních údajů
	OST	M		Informace - disclaimer - přístupnost
	OST	M		Informace Disclaimer - podpora
	OST	XS		Přijatý deeplink z DIPu do JePEK
	OST	XS		Linky u předmětu kontroly do DIP a eSbirky
	OST	L		Anglická mutace pro podnikatele
	OST	M		Video k používání aplikace
	OST	XL		Vystavení jedné aplikace jak v CMS tak běžně v Internetu tj. dvojdoménovost (cms2.cz a gov.cz)
	OST	M		Specifické MPO texty a informace
	OST	XL		Vestavěna podpora multitenancy, kde je možné jednoduše a efektivně oddělit data jednotlivých tenantů a je možné jednoduše, bez programování, zavést nového tenanta (například nový kontrolní subjekt).
	OST	XL	Volitelně	Obecně prostředí pro portálovou editaci a vytvoření dashboardu z ready to use komponent (tabulka, graf, editor) pro uživatele
	OST	XL	Volitelně	Platforma umožňující komponentový obsah pro jednotlivé entity s možnosti jejich úpravy bez programování.
	OST	XL	Volitelně	Platforma podporující různou povinnost atributů pro použití v integracích tak, aby jednotlivé přistupující kontrolní úřady mohly mít vlastní sady informací ukládaných do JePEK

	OST	XL	Volitelně	Platforma obsahující možnost úkolování uživatelů formou evidence úkolů, možnosti jejich delegace a komunikace nad úkoly (pro použití v dalších etapách).
	OST	XL	Volitelně	Platforma s integrovanou umělou inteligencí (pro využití v dalších etapách)
	OST	XL		Vytvoření Souhrnného pohledu v rámci Reportingového systému, který bude obsahovat čtyři středně složité (sub)reporty v tomto nástroji postavené na datové základně JePEK

Vysvětlivky k Usecase rozpadům:

- XS, S, M, L, XL – jedná se o odhad velikosti daného case
- BUC: business usecase
- SUC: systémový usecase
- INTL: buď integrační scénář (tj. jak zřetězit volání integrací, aby byl smysluplný business výsledek, jak jej mohou usecasy využít) nebo integrační tok (tj. technická integrace)
- BL: Business logika

OST: ostatní

17. Příloha: Poskytnutá vysvětlení v rámci zadávacího řízení

V rámci zadávacího řízení (N006/23/V00017025), které proběhlo od 6. 5. 2025 do 11. 6. 2025 byla na profilu zadavatele v Informačním systému NEN uveřejněna vysvětlení zadávací dokumentace, která upřesnila tuto Technickou dokumentaci.


1_Vysvetleni zadavaci dokumenta


2_Vysvetleni zadavaci dokumenta


3_Vysvetleni zadavaci dokumenta


4_Vysvetleni zadavaci dokumenta

Případně jsou uložena i v Informačním systému NEN zde: https://nen.nipez.cz/profily-zadavatelu-platne/detail-profilu/MPO/zahajene-zakazky/detail-zakazky/N006-23-V00017025/vysvetleni-dokumentace

Příloha č. 5 – Specifikace ceny plnění

Dílo		v Kč bez DPH
Celková cena za dodání Díla		**14 250 000,00 Kč**

Provoz dodaného Díla - po akceptaci **tj. 72 měsíců (6 let)**		**za 1 měsíc** v Kč bez DPH
Cena za Služby provozu a Služby podpory AIS JePEK za 1 měsíc v období 72 měsíců (6 let) následujícím po dodání a akceptaci díla, při zapojení a integraci zamýšleného finálního počtu až 50ti kontrolních orgánů a při evidenci až 350 000 kontrol každý rok v CLOUDu, tzn. při předpokládané maximální datové zátěži:		**185 308,00 Kč**

Výše uvedená cena za měsíc provozu při předpokládané maximální měsíční datové zátěži bude v průběhu 72 měsíců (6let) různá, a to s ohledem na postupný proces napojování a integraci jednotlivých kontrolních orgánů. Výdaje na provoz a podporu budou postupně v čase trvání smlouvy růst, a to až do úrovně horní hrance měsíční ceny za provoz a podporu AIS JePEK, kterou Poskytovatel nabídl. Objednatel proto uvádí následující procentní parametr, kterým se bude cena provozu za měsíc určovat:

- Pokud bude v AIS JePEK evidováno celkem od 0 do 200 000 kontrol, přísluší Poskytovateli za provoz 60 % z horní hranice ceny za provoz a podporu za 1 měsíc, a to v měsíci ve kterém stav nastane.
- Pokud bude v AIS JePEK evidováno celkem od 200 001 do 400 000 kontrol, přísluší Poskytovateli za provoz 80 % z horní hranice ceny za provoz a podporu za 1 měsíc, a to v měsíci ve kterém stav nastane.
- Pokud bude v AIS JePEK evidováno celkem od 400 001 kontrol a více, přísluší Poskytovateli za provoz 100 % z horní hranice ceny za provoz a podporu za 1 měsíc, a to v měsíci ve kterém stav nastane.

Rozvoj dodaného a provozovaného Díla v následujících předpokládaných **oblastech rozvoje** v období od 1. 4. 2026 do 31. 3. 2032, tj. **6 let**.	**Počet člověkodnů**	**1 Člověkoden** v Kč bez DPH
Rozvoj Díla – oblast "Integrace s dalšími systémy"		6 200,00 Kč

Rozvoj Díla – oblast "Rozšíření funkcionality, zlepšení uživatelského rozhraní a aplikace AI"		6 200,00 Kč
Rozvoj Díla – oblast "Školení a podpora uživatelů"		6 200,00 Kč
Rozvoj Díla – oblast "Změna zákonných podmínek kybernetické bezpečnosti"		6 200,00 Kč
Rozvoj Díla – oblast "Konzultace"		6 200,00 Kč
**Člověkoden znamená osm (8) hodin práce jedné osoby.*		

Maximální možný rozsah Služeb rozvoje činí 1300 člověkodnů.

MINISTERSTVO PRŮMYSLU A OBCHODU

Fina
Evro
Next

NÁRODNÍ PLÁN OBNOVY

NÁRODNÍ PLÁN OBNOVY

Příloha č. 6 – Harmonogram

Název klíčového milníku	Popis a podmínky akceptace milníku	Způsob hodnocení plnění akceptačních kritérií	Výstupy milníku	Požadovaný termín splnění	Výše procenta možné fakturace z částky určené na vývoj Díla

<u>Klíčový milník A</u> - Analýza systému	V rámci tohoto milníku je očekáváno provedení komplexní analýzy systému vycházející z business požadavků, vstupního zadání MPO a vlastní expertízy pracovníků Poskytovatele. **Předpokladem je provedení těchto činností:** **1. Business a procesní analýza** - Shromáždění a analýza požadavků od klíčových stakeholderů (MPO, kontrolní orgány, podnikatelé, veřejnost), Mapování procesů souvisejících s kontrolami a jejich optimalizace v souladu s legislativními požadavky (kontrolní řád, GDPR, NIS2), Definice klíčových funkcionalit systému – evidence kontrol, plánování, reportování, notifikace. **2. Návrh UI/UX (uživatelského rozhraní a zkušenosti)** - Identifikace uživatelských scénářů a typů uživatelů (kontrolor, podnikatel, MPO administrátor), Wireframy a prototypy hlavních obrazovek systému – navigace, dashboardy, formuláře, Uživatelský výzkum a testování prototypu s vybranými uživateli pro zpětnou vazbu, Zajištění přístupnosti a použitelnosti v souladu se standardy pro eGovernment.	Posouzení věcné naplněnosti analýzy vzhledem k předaným podkladům, pokrytí definovaných UseCase, kvalita a designové zpracování návrhů obrazovek a přívětivosti uživ. Prostředí.	Výstupem milníku je komplexní analýza systému zahrnující především: dokumentaci business požadavků a procesní analýza, wireframe a prototypy hlavních obrazovek systému, technický návrh systému včetně architektury a databázového modelu, bezpečnostní analýza a návrh řízení přístupu.	**Do 45 dnů od uveřejnění v registru smluv**	**10 %**

	3. Technický návrh systému - Definice technologické architektury – výběr vhodných technologií, návrh databázového modelu, API, integrace s externími registry (RŽP, ISZR, NIA, MPO), Bezpečnostní analýza – návrh řízení přístupu (RBAC, certifikáty, OTP), auditních logů a souladu s NIS2, Výkonová analýza a škálovatelnost – návrh infrastruktury umožňující budoucí rozšíření systému. **4. Testování konceptu a validace návrhu** - Ověření navržené architektury z hlediska výkonu a bezpečnosti, Validace UI/UX návrhu s vybranými uživateli a zapracování zpětné vazby, Schválení specifikace systému a technologického návrhu MPO a klíčovými stakeholdery.				

<u>Klíčový milník B</u> - 1. Funkční verze Aplikace AIS JePEK	V rámci tohoto milníku je očekáváno dodání první funkční verze JePEK umožňující realizovat základní činnosti určené jednotlivým uživatelským rolím systému.	Akceptační test, kvalitativní posouzení dodané dokumentace	Výstupem je funkční prototyp aplikace zpřístupněný vybraným uživatelům objednatele pro rutinní UAT testování, základní uživatelská příručka pro zainteresované uživatele a seznam testovacích scénářů pro testování na straně objednatele.	**Do 150 dnů od uveřejnění v registru smluv**	**30 %**
<u>Klíčový milník C</u> - 1. Funkční verze Aplikace AIS JePEK v 1. fázi integrace	Nad rámec 1. funkčního prototypu (MVP) jsou dále implementovány funkce umožňující integrace na interní systémy dotčených kontrolních úřadů -> provedena základní integrace dat z následujících kontrolních orgánů: **- Český metrologický institut,** **- Český úřad pro zkoušení zbraní a střeliva,** **- Úřad pro technickou normalizaci, metrologii a státní zkušebnictví,** **- Puncovní úřad,** **- Státní energetická inspekce,** **- 1x útvar Ministerstva průmyslu a obchodu, který provádí kontroly.** Výše uvedené kontrolní orgány realizují ročně přibližně **3 000 až 5 000 kontrol.**	Akceptační test, kvalitativní posouzení dodané dokumentace	Výstupem tohoto milníku je portál JePEK funkčně připravený pro využití ze strany interních uživatelů MPO stejně tak pro uživatele na straně kontrolních úřadů v produkčním prostředí. Je provedena integrace na vyjmenované kontrolní úřady a je možné spravovat a zobrazovat plány kontrol, provádět kontroly kolizí termínů, reportovat data z portálu JePEK. Uživatelská dokumentace v potřebném rozsahu pro školení uživatelů ve	**Do 180 dnů od uveřejnění v registru smluv**	**30 %**

			všech rolích, testovací scénáře pro realizaci akceptačních testů.		
<u>Klíčový milník D</u> - Funkční verze AIS JePEK (plná verze)	V rámci tohoto milníku bude po vybraném Poskytovateli požadováno v rámci akceptačního řízení, aby AIS JePEK byl: **a)** Finálně vyvinut, tzn. **byly dokončeny vývojové práce** z předchozího milníku, byl hotov UI/UX Design a byl dokončen Frontend a Backend vývoj. **b)** Byla provedena **další integrace dat** z následujících kontrolních orgánů: **- Krajské živnostenské úřady, Obecní živnostenské úřady,** nebo **- Česká obchodní inspekce.** Výše uvedené subjekty jsou připraveny data dle potřeby na straně svých systémů poskytnout k integraci. Uvedené kontrolní orgány realizují ročně přibližně **20 000 kontrol.**	Akceptační test, kvalitativní posouzení dodané Dokumentace	Výstupem milníku je plná funkční verze portálu JePEK v celé zamýšlené funkcionalitě – dle analýzy. Kompletní Dokumentace systému.	**Do 31. 3. 2026 (Termín vyplývající z Národního plánu obnovy – NPO)**	**30 %**
					100 %

Akceptační testy, vady, kritéria	
Vady Díla budou hodnoceny podle závažnosti – klasifikace specifikované v této Příloze, zohledňující závažnost vad z hlediska Objednatele. "Vada" znamená (i) rozpor mezi skutečnými vlastnostmi Díla a vlastnostmi, které jsou stanoveny touto Smlouvou nebo (ii) jakékoli funkční odchýlení Díla od standardních funkčních vlastností popsaných ve Smlouvě, které negativně postihuje jeho činnost nebo funkčnost. Výstupy typu „Aplikace“ se rozumí výstupy příslušných částí, které jsou předmětem dodávky a jsou akceptovány během příslušných akceptačních testů Objednatelem. Níže v této Příloze jsou uvedena příslušná akceptační kritéria.	
Kategorie	**Dopad na užívání systému**
Kategorie A	Znamená vadu, která se projevuje tím, že Dílo nebo jakákoliv jeho část nemá vlastnosti výslovně vymíněné Smlouvou, nebo Dílo nebo jeho podstatná část je zcela nefunkční nebo Objednatel nemůže Dílo nebo jakoukoliv jeho podstatnou část užívat.
Kategorie B	Znamená vadu, která se projevuje tím, že užívání nebo funkčnost Díla nebo jakékoliv jeho části je vadou významně omezeno a dochází tak k významnému zpomalení užívání Díla ze strany Objednatele.
Kategorie C	Znamená vadu, která nespadá do vady kategorie A nebo vadu kategorie B a která nebrání nebo má zcela minimální vliv na řádné užívání nebo funkčnost Díla nebo jakékoliv jeho části ze strany Objednatele (uživatele)

Klíčový milník B - 1. Funkční verze Aplikace AIS JePEK	
Pravidla	1. Za Vadu je považována každá Vada, která není odstraněna, nebo jejíž odstranění nebylo Objednatelem akceptováno.

	2. Kategorizaci Vady provádí pověřený pracovník Objednatele s následným potvrzením pověřeného pracovníka **Poskytovatele** s cílem dosáhnout shody v kategorizaci Vad; v případě neshody v kategorizaci Vad musí být toto uvedeno v Akceptačním protokolu. O kategorizaci Vady následně rozhodnou kontaktní osoby Smluvních stran.	
	3. V průběhu Akceptačního testu nelze provádět změny testovaného aplikačního systému bez souhlasu Objednatele.	
	Výše uvedená pravidla musí být splněna všechna zároveň.	
Akceptační kritéria	Max. počet Vad priority Kategorie A	**0**
	Max. počet Vad priority Kategorie B	**10**
	Max. počet Vad priority Kategorie C	**30**

Klíčový milník C - 1. Funkční verze Aplikace AIS JePEK v 1. fázi integrace	
Pravidla	1. Za Vadu je považována každá Vada, která není odstraněna, nebo jejíž odstranění nebylo Objednatelem akceptováno.
	2. Kategorizaci Vady provádí pověřený pracovník Objednatele s následným potvrzením pověřeného pracovníka **Poskytovatele** s cílem dosáhnout shody v kategorizaci Vad; v případě neshody v kategorizaci Vad musí být toto uvedeno v Akceptačním protokolu. O kategorizaci Vady následně rozhodnou kontaktní osoby Smluvních stran.
	3. V průběhu Akceptačního testu nelze provádět změny testovaného aplikačního systému bez souhlasu Objednatele.

	Výše uvedená pravidla musí být splněna všechna zároveň.	
Akceptační kritéria	Max. počet Vad priority Kategorie A	**0**
	Max. počet Vad priority Kategorie B	**2**
	Max. počet Vad priority Kategorie C	**20**

Klíčový milník D - Funkční verze AIS JePEK (plná verze)		
Pravidla	1. Za Vadu je považována každá Vada, která není odstraněna, nebo jejíž odstranění nebylo Objednatelem akceptováno.	
	2. Kategorizaci Vady provádí pověřený pracovník Objednatele s následným potvrzením pověřeného pracovníka **Poskytovatele** s cílem dosáhnout shody v kategorizaci Vad; v případě neshody v kategorizaci Vad musí být toto uvedeno v Akceptačním protokolu. O kategorizaci Vady následně rozhodnou kontaktní osoby Smluvních stran.	
	3. V průběhu Akceptačního testu nelze provádět změny testovaného aplikačního systému bez souhlasu Objednatele.	
	Výše uvedená pravidla musí být splněna všechna zároveň.	
Akceptační kritéria	Max. počet Vad priority Kategorie A	**0**
	Max. počet Vad priority Kategorie B	**0**
	Max. počet Vad priority Kategorie C	**0**

Po dodání výše uvedených milníků bude následovat provoz a průběžný rozvoj AIS JePEK v období od 1. 4. 2026 do 31. 3. 2032, tj. 6 let, kdy budou v rámci rozvojových požadavků postupně připojovány kontrolní orgány mimo gesci Ministerstva průmyslu a obchodu. Těchto kontrolních orgánů může být až 43.

Současně zadavatel deklaruje, že na tyto rozvojové požadavky je alokováno maximálně 1 300 člověkodní, které budou po vzájemné dohodě zadavatele a objednatel, v předem odsouhlaseném rozsahu, postupně čerpány.

Zamýšlené základní oblasti rozvoje: další rozvoj a zlepšení uživatelského rozhraní, integrace s dalšími systémy, rozšíření funkcionality, aplikace umělé inteligence (AI), školení a podpora uživatelů v souvislosti s rozvojem, konzultační služby ve vztahu k rozvoji a kybernetické bezpečnosti.

Konzultace s uživateli: Poskytovatel se zapojí do pravidelných konzultací s klíčovými uživateli (úředníky i veřejností) za účelem pochopení jejich potřeb a požadavků. Na základě těchto konzultací poskytne návrhy na úpravy a rozvoj systému.

Zajištění kontinuálního vývoje: Poskytovatel zajistí průběžnou údržbu a rozvoj systému v souladu s novými legislativními a technologickými požadavky. Bude sledovat změny relevantní pro systém a navrhovat jejich implementaci tak, aby bylo zajištěno dlouhodobé fungování a efektivita řešení.

Zajištění kontinuálního souladu s požadavky na kybernetikou bezpečnost z důvodu změny legislativy v oblasti kybernetické bezpečnosti.

Položka	Období	Časová dotace
Provoz	od **1. 4. 2026** do **31. 3. 2032**	tj. **72** měsíců (6 let)
Rozvoj	od **1. 4. 2026** do **31. 3. 2032**	**1 300** člověkodnů

Příloha č. 7 – Realizační tým Poskytovatele

Kontaktní údaje	Role v realizačním týmu	Minimální kvalifikace
[redacted]	Projektový manažer	Min. 3 roky praxe v pozici vedoucího týmu, kde se spolupodílel na min. 2 zakázkách obdobného charakteru s fakturovanou celkovou cenou min. 10 000 000 Kč bez DPH. Znalost českého jazyka na úrovni nezbytné pro ústní i písemnou komunikaci v rámci plnění veřejné zakázky.
[redacted]	IT Analytik	Min. 3 roky praxe v pozici vedoucího týmu, kde se spolupodílel na min. 2 zakázkách obdobného charakteru s fakturovanou celkovou cenou min. 10 000 000 Kč bez DPH. Znalost UML a Archimate notací a zkušenosti s modelovacími CASE nástroji (např. Archi, Enterprise architect).
[redacted]	Specialista kybernetické bezpečnosti	Praxe alespoň 5 let a účast na minimálně 2 zakázkách s návrhem bezpečnostní architektury velkých informačních systémů. Praxe v oblasti poskytování konzultačních služeb v oblasti informační a kybernetické bezpečnosti v návaznosti na ZoKB a vyhlášky č. 82/2018, o kybernetické bezpečnosti („**VyKB**“). Praxe v provádění analýz rizik dle schválené metodiky (Identifikace klíčových aktiv organizace; Identifikace hrozeb a zranitelností; Identifikace, stanovení a hodnocení rizik).

		Zkušenosti s tvorbou Dokumentace dle ZoKB nebo ISO 270001 k jednotlivým systémům. Prokazatelné zkušenosti s definicí a implementací nápravných opatření. Praxe v oblasti provádění kontrol účinnosti realizovaných opatření v oblasti kybernetické a informační bezpečnosti.
[redacted]	IT Architekt	Min. 3 roky praxe v postavení solution architekta, kde se spolupodílel na min. 2 zakázkách obdobného charakteru s fakturovanou celkovou cenou min. 10 000 000 Kč bez DPH. Znalost UML a Archimate notací a zkušenosti s modelovacími CASE nástroji (např. Archi, Enterprise architect). Znalost a zkušenost s uplatněním návrhových integračních vzorů, integračních technik a protokolů (Synchronní/Asynchronní, REST, SOAP).
[redacted]	IT Senior vývojář	Min. 3 roky praxe v oboru shodném s předmětem plnění (zhotovení informačního systému) na pracovní pozici shodné/obdobné s pozicí, jakou bude zastávat v realizačním týmu, a současně se spolupodílel na min. 2 zakázkách obdobného charakteru s fakturovanou celkovou cenou min. 10 000 000 Kč bez DPH.
[redacted]	IT Junior vývojář	Min. 1,5 roku praxe v oboru shodném s předmětem plnění (zhotovení informačního systému) na pracovní pozici shodné/obdobné s pozicí, jakou bude zastávat v realizačním týmu, a současně se spolupodílel na min. 1 zakázce obdobného

		charakteru s fakturovanou celkovou cenou min. 10 000 000 Kč bez DPH.
[redacted]	IT Specialista uživatelské podpory	Min. 3 roky praxe v oboru shodném s předmětem plnění (zhotovení informačního systému) na pracovní pozici shodné/obdobné s pozicí, jakou bude zastávat v realizačním týmu tzn. specialisty uživatelské podpory s platnou certifikací v oblasti řízení a správy IT služeb a současně se spolupodílel na min. 2 zakázkách obdobného charakteru s fakturovanou celkovou cenou min. 10 000 000 Kč bez DPH.
[redacted]	IT Specialista uživatelské podpory	Min. 3 roky praxe v oboru shodném s předmětem plnění (zhotovení informačního systému) na pracovní pozici shodné/obdobné s pozicí, jakou bude zastávat v realizačním týmu tzn. specialisty uživatelské podpory s platnou certifikací v oblasti řízení a správy IT služeb a současně se spolupodílel na min. 2 zakázkách obdobného charakteru s fakturovanou celkovou cenou min. 10 000 000 Kč bez DPH.

Příloha č. 8 – Seznam subPoskytovatelů

Popis části Díla zajišťované subPoskytovatelem	SubPoskytovatel
----------	----------

Příloha č. 9 – Oprávněné osoby a kontaktní údaje

Za Objednatele:

ve věcech smluvních:

Jméno a Příjmení:	Ing. Pavel Vinkler, Ph.D.	Ing. Jiří Vondrák
E-mail:	[redacted]	[redacted]
Telefon:	[redacted]	[redacted]

ve věcech obchodních:

Jméno a Příjmení:	Ing. Jiří Vondrák
E-mail:	[redacted]
Telefon:	[redacted]

ve věcech technických:

Jméno a Příjmení:	Ing. Hana Staňková
E-mail:	[redacted]
Telefon:	[redacted]

Příloha č. 9 – Oprávněné osoby a kontaktní údaje

Za Poskytovatele:

ve věcech smluvních:

Jméno a Příjmení:	Ing. Petr Polách
E-mail:	[redacted]
Telefon:	[redacted]

ve věcech obchodních:

Jméno a Příjmení:	Ing. Pavel Hrdlička
E-mail:	[redacted]
Telefon:	[redacted]

ve věcech technických:

Jméno a Příjmení:	Ing. Martin Prem
E-mail:	[redacted]
Telefon:	[redacted]

Příloha č. 10 – Typy vad Díla

Klasifikace poruchových stavů (vad a poruch)

Kategorie vad a poruch

- Vada kategorie I. znamená kritickou vadu, která má zásadní dopad na základní funkce AIS, kdy se například nejde do AIS přihlásit. Dále je ohrožena bezpečnost dat a výsledky zpracování dat vykazují zjevné faktické chyby/vady. Dochází k poruchám v databázi a souvisejících aplikačních služeb, které způsobují výpadky AIS. Nedochází k přenosu dat mezi AIS a externími systémy mimo perimetr Objednatele.
- Vada kategorie II. znamená vadu umožňující provoz základních funkcí AIS, kdy dochází k bezvadnému přenosu dat mezi cílovým AIS a externími systémy mimo perimetr Objednatele. Zároveň tento druh vady nemá vliv na kvalitu ani na bezpečnost dat a výsledky zpracování výsledných dat. Nejsou například funkční nadstavbové reportovací nástroje nebo filtrování dat je nedostupné.
- Vada kategorie III. znamená vadu, která není vadou kategorie I. anebo II. (např. špatná grafická úprava aplikace, špatný pravopis u nápovědy apod.).

Příloha č. 11 - Pojistný certifikát

V142

TC9940610102 6

O221559191910 2

GENERALI ČESKÁ POJIŠŤOVNA

Generali Česká pojišťovna a.s., Spálená 75/16, Nové Město, 110 00 Praha 1, IČO: 452 72 956, DIČ: CZ699001273, je zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, spis. zn. B 1464, člen skupiny Generali, zapsané v italském registru pojišťovacích skupin, vedeném IVASS, pod číslem 026

POJISTKA

Pojištění majetku a odpovědnosti podnikatele a právnických osob **ProfiPlán**

potvrzení o uzavření pojistné smlouvy č. 4580904288

Pojistník

Název	ASD Software, s.r.o.
Adresa	Žerotínova 2981/55A, Šumperk, 787 01
Stát	ČESKÁ REPUBLIKA
IČO	62363930

Pojištění profesní odpovědnosti poskytovatele software, hardware, zpracovaní dat a správy sítí

Pojistná událost
Pojistnou událostí je vznik povinnosti pojištěného nahradit škodu nebo újmu uvedenou v pojistné smlouvě či pojistných podmínkách, se kterou je spojena povinnost pojistitele poskytnout pojistné plnění.

Pojistná nebezpečí
Pojistným nebezpečím jsou skutečnosti a události vymezené v pojistné smlouvě jako možná příčina vzniku pojistné události.

Oprávněnou osobou z tohoto pojištění je pojistník.

Podmínky, rozsah pojištění a pojistných nebezpečí stanoví pojistná smlouva a Všeobecné pojistné podmínky pro pojištění profesní odpovědnosti VPPPI-P-01/2020.

Pojištění v základním rozsahu se sjednává s limitem pojistného plnění	50 000 000 Kč
Pojištění v základním rozsahu se sjednává s územním rozsahem	Česká republika
Pojištění v základním rozsahu se sjednává se spoluúčastí	5 000 Kč

Počátek a doba pojištění

Sjednané pojištění je účinné od 0:00 hod dne 4. 7. 2024.
Pojištění se sjednává na dobu neurčitou.

Pojistitel potvrzuje, že údaje obsažené v pojistce jsou platné ke dni jejího vydání.

Platnost pojistky od: 4. 7. 2021

S pozdravem

Generali Česká pojišťovna a.s.

[redacted]

Eva Skalníková
senior manažer správy neživotního pojištění

Příloha č. 12

ke Smlouvě o vytvoření, rozvoji informačního systému JePEK,

službách provozu a službách podpory

(dále jen „**Smlouva**“)

Smluvní ujednání v rámci zákona o kybernetické bezpečnosti

uzavřená dle § 4 zákona č. 181/2014 Sb., o kybernetické bezpečnosti, (dále jen „**Příloha**“)

Česká republika – Ministerstvo průmyslu a obchodu dále také jako „**Objednatel**“

a

ASD Software, s.r.o. dále také jako „**Poskytovatel**“

1. Obecná ustanovení

1.1. Tato Příloha tvoří nedílnou součást Smlouvy.

1.2. Není-li dále stanoveno jinak nebo nevyplývá-li jinak z kontextu, mají pojmy počínající velkým písmenem v této Příloze shodný význam, jaký mají ve Smlouvě.

1.3. Smluvní strany dále vymezují následující pojmy:

a. zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „**ZoKB**“); a

b. vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „**VoKB**“).

1.4. Poskytovatel bere na vědomí, že předmět plnění Smlouvy bude po svém uvedení do provozu významným informačním systémem dle § 3 písm. e) ZoKB.

1.5. Objednatel tímto informuje Poskytovatele, že plnění Poskytovatele dle této Smlouvy se považuje za plnění významného dodavatele dle § 2 písm. n) VoKB a že jej Objednatel eviduje v souladu s § 8 odst. 1 písm. b) VoKB jako významného dodavatele.

1.6. Poskytovatel bere na vědomí, že jej Objednatel současně považuje za provozovatele dle § 2 písm. g) ZoKB ve vztahu k systému specifikovanému v odst. 1.4 této Přílohy a že jej Objednatel eviduje jako provozovatele v souladu s § 8 odst. 1 písm. b) VoKB.

1.7. Poskytovatel určí odpovědnou osobu ve věcech kybernetické bezpečnosti, která odpovídá za:

a. informování statutárního orgánu Poskytovatele o požadavcích na kybernetickou bezpečnost, které vyplývají ze smluvního vztahu se Objednatelem, z VoKB a z této Přílohy;

b. každoroční přezkoumání stavu plnění povinností Poskytovatele dle této Přílohy a podání písemné zprávy o stavu jejich plnění Objednateli; a

c. komunikaci s manažerem kybernetické bezpečnosti Objednatele ve věcech spojených s plněním dle této Přílohy nebo vyplývajících ze ZoKB a VoKB.

1.8. Poskytovatel informuje Objednatele o jmenování odpovědné osoby ve věcech kybernetické bezpečnosti a předá Objednateli kontaktní údaje odpovědné osoby do deseti dnů od nabytí účinnosti této přílohy.

2. Rozsah zapojení Poskytovatele a poddodavatelé Poskytovatele

2.1. Rozsah zapojení Poskytovatele na rozvoji, provozu a zajištění kybernetické bezpečnosti primárních a podpůrných aktiv dle VoKB je určen předmětem plnění Smlouvy včetně jejích příloh.

2.2. Poskytovatel je oprávněn využít k plnění dle Smlouvy poddodavatele jen v případě, že to Smlouva včetně jejích příloh výslovně připouští, a to za podmínek v ní uvedených. Nestanoví-li Smlouva včetně příloh jinak, podléhají jednotliví poddodavatelé předchozímu písemnému schválení ze strany Objednatele.

2.3. Poskytovatel je povinen zavázat případné poddodavatele k plnění shodných povinností, které plní Poskytovatel vůči Objednateli dle této Přílohy. Poskytovatel Objednateli doloží, že u poddodavatelů smluvně vyžaduje dodržování pravidel dle této Přílohy, a to poskytnutím příslušné smlouvy do 10 dnů od jejího uzavření.

2.4. Poskytovatel se zavazuje, že pravidla dle této Přílohy budou dodržovat i pracovníci Poskytovatele, poddodavatelé Poskytovatele a jejich pracovníci. Za porušení pravidel dle této Přílohy poddodavatelem odpovídá Poskytovatel Objednateli tak, jako by pravidel dle této Přílohy porušil sám.

2.5. Poskytovatel se zavazuje soustavně (případně pravidelně dle povahy) dohlížet na plnění této Přílohy ze strany jeho poddodavatelů a jejich zaměstnanců. Poskytovatel odpovídá za zajištění dostatečné znalosti pravidel dle této Přílohy, ze strany svých dodavatelů a jejich zaměstnanců.

2.6. Objednatel je oprávněn provést školení pravidel dle této Přílohy pro pracovníky Poskytovatele a jeho poddodavatelů, kteří mají přístup k aktivům Objednatele. Objednatel oznámí Poskytovateli předpokládaný termín konání školení alespoň s předstihem 30 dnů a určí pracovníky Poskytovatele, kteří jsou povinni se školení zúčastnit. Objednatel současně zvolí formu a technické prostředky, prostřednictvím kterých bude školení probíhat. Školení ze strany Objednatele nezbavuje Poskytovatele povinnosti provádět vlastní školení svých školení pracovníků a odpovědnosti za zajištění dostatečné znalosti pravidel dle této Přílohy ze strany těchto pracovníků. Poskytovatel je povinen poskytnout k tomu veškerou součinnost, zejména zajistit účast svých pracovníků a poddodavatelů na školení a zajistit odpovídající prostory a technické prostředky dle pokynů Objednatele.

3. Povinnosti provozovatele

3.1. Poskytovatel bere na vědomí, že nad rámec povinností stanovených touto Přílohou je jakožto provozovatel dle § 2 písm. g) ZoKB povinen:

a. oznámit své kontaktní údaje příslušnému orgánu v souladu s § 16 ZoKB;

b. zavádět bezpečnostní opatření dle potřeb Objednatele v souladu s § 4 ZoKB;

c. hlásit kybernetické bezpečnostní incidenty v souladu s § 8 ZoKB;

d. provádět opatření v souladu s § 11 ZoKB; a

e. předložit Objednateli výsledky auditu kybernetické bezpečnosti, pokud je proveden, v souladu s § 16 odst. 5 VoKB.

4. Data, využití Dat Poskytovatelem a likvidace Dat

4.1. Poskytovatel je při poskytování plnění dle Smlouvy oprávněn užívat nebo sdílet data předaná mu Objednatelem či jiným způsobem získaná nebo vytvořená při plnění této Smlouvy (dále jen „**Data**“) pouze v rozsahu nezbytném ke splnění Smlouvy a pouze v souladu se Smlouvou a příslušnými právními předpisy, tj. zejména ZoKB a VoKB.

4.2. Poskytovatel se zavazuje dodržovat parametry plnění definující časy odezvy a odstranění vad v případě omezení dostupnosti, důvěrnosti či integrity Dat, jak jsou stanoveny Smlouvou.

4.3. Poskytovatel bere na vědomí a souhlasí, že veškerá Data zůstávají předmětem výhradních práv Objednatele, který je jediným vlastníkem Dat a pořizovatelem databází, ve kterých jsou Data uložena.

4.4. Poskytovatel se zavazuje šifrovat datové nosiče, která obsahují Data, v souladu s předepsanými pravidly v rámci klasifikace informací.

4.5. Poskytovatel se zavazuje zachovávat mlčenlivost a důvěrnost Dat a zavazuje se, že tato Data nebudou Poskytovatelem zneužita, využita a poskytnuta třetím osobám.

4.6. Poskytovatel je povinen omezit přístup k Datům Objednatele pouze na ty zaměstnance a třetí strany, u kterých přístup vyžaduje plnění Smlouvy nebo plnění zákonných povinností. Poskytovatel nesmí umožnit přístup k Datům Objednatele jiným organizacím, jako například poddodavatelům nebo partnerům, bez předcházejícího prokazatelného souhlasu Objednatele. Vysloví-li Objednatel ve Smlouvě nebo jinak písemně souhlas se zapojením konkrétního poddodavatele do plnění Smlouvy, uděluje tím souhlas se zpřístupněním Dat Objednatele poddodavateli v rozsahu nezbytném pro plnění Smlouvy.

4.7. Učiní-li orgány činné v trestním řízení nebo jiné orgány státní správy jakoukoli právně závaznou žádost o poskytnutí Dat Objednatele, je Poskytovatel povinen tuto skutečnost oznámit Objednateli neprodleně a s předstihem před poskytnutím takových informací, pokud mu to právní předpisy nezakazují.

4.8. V případě, že cizozemský orgán požádá o zpřístupnění nebo předání Dat zpracovávaných na území cizího státu, Poskytovatel takové žádosti vyhoví

a. až po provedení přezkoumání zákonnosti žádosti,

b. až po vynaložení úsilí o zabránění zpřístupnění nebo předání dat v rámci možností daných právním řádem, v jehož působnosti dochází ke zpracování dat nebo podle kterého byla žádost podána,

c. pouze v nezbytném rozsahu.

4.9. Poskytovatel se zavazuje na základě výzvy Objednatele bez zbytečného odkladu předat bezpečným způsobem ve strojově čitelné podobě a obvyklém formátu jakákoli Data v dispoziční sféře Poskytovatele. Poskytovatel se k výzvě Objednatele zavazuje poskytnout nezbytnou součinnost, přičemž si smluvní strany mohou písemně dohodnout jiný způsob předání Dat.

4.10. Poskytovatel se zavazuje odstranit veškerá Data pokud dojde k ukončení Smlouvy nebo pokud Objednatel podá písemnou žádost, a to nejpozději do 14 dní od ukončení Smlouvy a za možného dozoru zástupce Objednatele. V případě, že Poskytovatel bude mít na svých nosičích Data vysoké či kritické úrovně důležitosti určené v souladu s přílohou č. 1 VoKB, má povinnost tyto nosiče fyzicky protokolárně zlikvidovat, případně je předat k likvidaci Objednateli.

5. Řízení aktiv a rizik

5.1. Před zahájením poskytování plnění a dále průběžně po celou dobu trvání Smlouvy Poskytovatel [zajistí / poskytne Objednateli součinnost pro zajištění]:

a. identifikaci aktiv v rámci předmětu plnění Smlouvy a jejich kategorizaci a hodnocení, a zařazení do bezpečnostních úrovní dle stupnic pro hodnocení důvěrnosti, integrity a dostupnosti v souladu s § 4 VoKB a přílohou č. 1 VoKB;

b. určení vazeb mezi primárními a podpůrnými aktivy a případně určení vazeb na současná aktiva Objednatele;

c. pravidelnou aktualizaci tohoto seznamu aktiv a jejich vazeb;

d. řízení bezpečnostních rizik, která mohou ovlivnit poskytování předmětu plnění Smlouvy, v souladu s minimálními požadavky na řízení rizik upravenými v ZoKB a VoKB;

e. informování Objednatele o způsobu řízení rizik a předložení zprávy o hodnocení aktiv a rizik, která jsou využívána pro plnění Smlouvy a o zbytkových rizicích souvisejících s aktivy využívanými pro plnění Smlouvy;

f. identifikaci a hodnocení relevantních hrozeb a zranitelností pro aktiva dle čl. 5.1 písm. a) této Přílohy se zohledněním kategorie hrozeb a zranitelností uvedených v příloze č. 3 VoKB a v rozsahu dle přílohy č. 2 VoKB;

g. přepočet dopadu aktuálních kybernetických rizik v souvislosti s novými hrozbami spojenými s předmětem plnění dle Smlouvy;

h. hodnocení rizik, které bude zohledňovat přepočet dle předchozího odstavce této Přílohy, toto hodnocení strukturovaně popsat a Objednateli předložit;

i. zpracování prohlášení o aplikovatelnosti pro aktiva dle čl. 5.1 písm. a) této Přílohy podle § 5 odst. 1 písm. f) VoKB;

zpracování plánu zvládání rizik pro aktiva dle čl. 5.1 písm. a) podle § 5 odst. 1 písm. g) a h) VoKB.

5.2. Při provádění úkonů podle odst. 5.1 této Přílohy je Poskytovatel povinen postupovat podle bezpečnostní best practice, metodik a postupů a se zohledněním podkladů jemu poskytnutých za tímto účelem.

5.3. [Úkony / Součinnost] podle odst. 5.1 této Přílohy zajistí Poskytovatel nejméně jednou ročně v rozsahu dvou pracovních dnů a dále pokud nastanou okolnosti podle § 5 odst. 1 písm. h) VoKB.

5.4. [Objednatel a Poskytovatel se zavazují podrobit předání a převzetí dokumentace podle odst. 5.1 této Přílohy akceptačnímu řízení, přičemž lhůta pro připomínkování dokumentů se stanoví na 10 pracovních dnů od obdržení příslušného dokumentu a lhůta k odstranění vad dokumentů se stanoví na 10 pracovních dnů od obdržení připomínek k tomuto dokumentu. Nestanoví-li Smlouva pravidla akceptačního řízení, má Objednatel ve lhůtě pro připomínkování dokumentů právo vytknout zhotoviteli vady dokumentů. Dokument má vadu, je-li v rozporu s požadavky ZoKB, VoKB nebo Smlouvy (vč. této Přílohy). Poskytovatel je povinen ve lhůtě k odstranění vad dokumentů předat Objednateli dokumenty bez vad vytčených Objednatelem. Tato procedura se může opakovat, nejsou-li vady dokumentů odstraněny řádně. / S dokumentací podle odst. 5.1 této Přílohy se Objednatel zavazuje Poskytovatele seznámit bez zbytečného odkladu po jejím zpracování, nejpozději však do 15 dnů po tomto zpracování. Poskytovatel je oprávněn vznést k dokumentaci připomínky, přičemž Objednatel je povinen připomínky zohlednit, pokud z dokumentace vyplývají Poskytovateli povinnosti nad rámec požadavků ZoKB, VoKB a Smlouvy (vč. této Přílohy).]

5.5. Poskytovatel je povinen zavést a po celou dobu trvání Smlouvy udržovat opatření dle aktuálního plánu zvládání rizik podle odst. 0) této Přílohy. Opatření je Poskytovatel povinen zavést před zahájením poskytování plnění dle Smlouvy. Zejména je Poskytovatel povinen zavést a udržovat opatření zejména v následujících oblastech:

a. klasifikace informací,
b. nakládání s informacemi,
c. školení pracovníků Poskytovatele v IT bezpečnosti,
d. přístupu k logům a auditním stopám,
e. mobilních zařízení a práce na dálku,
f. řízení přístupů,
g. centrálního řízení bezpečnostních nastavení,
h. kryptografických bezpečnostní opatření,
i. fyzického bezpečnosti,
j. ukládání dat,
k. dostupnosti dat,
l. zálohování,
m. správy zranitelností a záplat,
n. ochrany před škodlivým softwarem a
o. vývoje a údržby systémů,

které jsou dále rozvedeny v čl. 6 až 9 této Přílohy.

6. Klasifikace informací a ochrana informačních aktiv

6.1. Poskytovatel se zavazuje pro klasifikaci informací užívat stupně klasifikace Objednatele, nebo je povinen zavést vlastní mapování či překlad rizik mezi klasifikačním schématem a klasifikací Objednatele.

6.2. Objednatel klasifikuje informace následujícím způsobem:

Klasifikace	Popis	Označování dokumentů	Hodnocení aktiva
Veřejné	Informace jsou veřejně přístupné nebo byly určeny ke zveřejnění (např. na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů). Narušení důvěrnosti informací neohrožuje oprávněné zájmy MPO.	Není povinné dokumenty označovat jako veřejné	Kritičnost: nízká
Interní	Informace pro vnitřní potřebu nezařazené do některé z vyšších kategorií, jejichž zveřejnění nebo neoprávněný přístup k nim může mít vliv na bezpečnost provozu IS nebo MPO. Do této kategorie jsou zařazeny informace, jejichž zveřejnění je omezeno na základě ustanovení § 11 odst. 1 zákona č. 106/1999 Sb., o svobodném přístupu k informacím.	Označení: „pro vnitřní potřebu“	Kritičnost: střední
Citlivá	Informace nejsou veřejně přístupné a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními.	Označení: „citlivé“	Kritičnost: vysoká
Velmi citlivá	Informace nejsou veřejně přístupné a vyžadují nadstandardní míru ochrany and rámec předchozí kategorie (např. strategické obchodní tajemství, citlivé osobní údaje).	Označení: „velmi citlivé“	Kritičnost: velmi vysoká

6.3. Poskytovatel je povinen zavést vhodná opatření pro ochranu informací přiměřená úrovni jejich klasifikace, která budou vyžadovat minimálně stejná bezpečnostní pravidla pro zacházení s aktivy Objednatele, která jsou uvedena v následujících tabulkách. S výjimkou aktiv klasifikovaných jako Veřejné je při jakémkoliv předávání aktiv vně organizaci Poskytovatele nutno dodržet čl. 4.5 této Přílohy.

Komunikační kanál	**Klasifikace aktiv: Veřejné**
Poskytování aktiv v rámci organizace	Žádná omezení.
Poskytování informací třetím stranám	
Nepřenosná datová média (pevné disky, stolní počítače, servery apod.)	
Přenosná datová média (CD, DVD, flash disky apod.)	
Přenosná výpočetní technika (notebooky, chytré telefony apod.)	
Internet – ukládání a publikace (cloudová úložiště, sociální sítě)	
Přenos po internetu (mezi systémy)	
Intranet	
Papírové dokumenty	
E-mail	
FAX	
Telefonní hovory (včetně VOIP)	
Způsob likvidace	**Informace na lidsky čitelném nosiči** (tištěné dokumenty, poznámky a podobně): Odstranění: Vyhození do odpadu. **Mobilní zařízení** (mobilní telefony, tablety): Odstranění: Vymazání informací, reset zařízení do továrního nastavení.

	Síťová zařízení (router, switch, modem a podobně), **Kancelářské vybavení** (scanery, tiskárny, fax): Odstranění: Vymazání informací, reset do továrního nastavení. **Magnetická média** (magnetické pásky, disky, HDD [Hard Disk Drive]), **Optická média** (CD, DVD, HD-DVD, BLU-RAY), **Elektronická média** (flash paměti): Odstranění: Smazání dat na úrovni souborového systému. **Outsourcing a cloud**: Přípustný způsob likvidace dat by měl být stanoven smluvním ujednáním. Odstranění: Odstranění všech souborů včetně předchozích verzí.

Komunikační kanál	**Klasifikace aktiv: Interní**
Poskytování aktiv v rámci organizace	Informace mohou být poskytnuty zaměstnancům Poskytovatele, pokud jsou relevantní pro výkon jejich činnosti.
Poskytování informací třetím stranám	Informace mohou být třetím stranám poskytovány pouze na základě dohody o mlčenlivosti.
Nepřenosná datová média (pevné disky, stolní počítače, servery apod.)	Žádné další požadavky.
Přenosná datová média (CD, DVD, flash disky apod.)	Médium musí být označeno „PRO VNITŘNÍ POTŘEBU“.
Přenosná výpočetní technika (notebooky, chytré telefony apod.)	Žádné další požadavky.
Internet – ukládání a publikace (cloudová úložiště, sociální sítě)	Data nesmí být ukládána v rámci internetových úložišť nebo veřejně přístupných webech a sociálních sítích.
Přenos po internetu (mezi systémy)	Žádné další požadavky.
Intranet	Žádné další požadavky.
Papírové dokumenty	Dokumenty musí být označeny jako „PRO VNITŘNÍ POTŘEBU“.
E-mail	Žádné další požadavky.

FAX	Dokumenty musí být označeny jako „PRO VNITŘNÍ POTŘEBU“.
Telefonní hovory (včetně VOIP)	Žádné další požadavky.
Způsob likvidace	**Informace na lidsky čitelném nosiči** (tištěné dokumenty, poznámky a podobně): Přepsání: Začernění. Fyzická likvidace: Znehodnocení nosiče informací použitím skartovacího stroje. **Mobilní zařízení** (mobilní telefony, tablety): Přepsání: Pro zařízení s šifrovaným úložištěm - odstranění informací a reset do továrního nastavení. **Síťová zařízení** (router, switch, modem a podobně), **Kancelářské vybavení** (scanery, tiskárny, fax): Přepsání: Odstranění a zahlcení umělými událostmi (umělý síťový provoz, testovací tiskové úlohy a podobně.). **Magnetická média** (magnetické pásky, disky, HDD [Hard Disk Drive]), **Optická média** (CD, DVD, HD-DVD, BLU-RAY): Přepsání: Přepsání dat. V případě šifrovaného média je alternativou bezpečná likvidace kryptografických klíčů. **Elektronická média** (flash paměti): Fyzická likvidace. **Outsourcing a cloud**: Přípustný způsob likvidace dat by měl být stanoven smluvním ujednáním. Přepsání: Použití šifrování datových úložišť na úrovni paměťového média a bezpečná likvidace kryptografických klíčů. Alternativně v případě dedikovaného paměťového média je možné data po ukončení služby přepsat.

Komunikační kanál	**Klasifikace aktiv: Citlivé**
Poskytování aktiv v rámci organizace	Pouze se souhlasem garanta daného primárního aktiva.
Poskytování informací třetím stranám	Informace mohou být třetím stranám poskytovány pouze se souhlasem garanta daného primárního aktiva a na základě dohody o mlčenlivosti.

Nepřenosná datová média (pevné disky, stolní počítače, servery apod.)	Data musí být zašifrována s použitím nasazeného šifrovacího řešení.
Přenosná datová média (CD, DVD, flash disky apod.)	Data musí být zašifrována s použitím nasazeného šifrovacího řešení. Po použití je nutná likvidace. Médium musí být označeno „CITLIVÉ“.
Přenosná výpočetní technika (notebooky, chytré telefony apod.)	Data musí být zašifrována s použitím nasazeného šifrovacího řešení. Přenosná technika musí být chráněna proti ztrátě či krádeži.
Internet – ukládání a publikace (cloudová úložiště, sociální sítě)	Data nesmí být ukládána v rámci internetových úložišť nebo veřejně přístupných webech a sociálních sítích.
Přenos po internetu (mezi systémy)	Data je nutno přenášet pouze prostřednictvím šifrovaného kanálu.
Intranet	Přístup k datům musí být omezen pouze na určenou skupinu uživatelů. Data musí být zašifrována s použitím nasazeného šifrovacího řešení.
Papírové dokumenty	Interně musí být dokumenty označeny jako „CITLIVÉ“ a bezpečně uloženy. Po použití musí být skartovány. Mimo organizaci je třeba převážet v zapečetěné obálce a pouze adresátům, kteří byli schváleni garantem daného primárního aktiva.
E-mail	Data musí být zašifrována s použitím nasazeného šifrovacího řešení.
FAX	Dokumenty musí být označeny jako „CITLIVÉ“. Musí být potvrzeno akceptování příjemcem zprávy (zasláním testovací stránky a obdržením potvrzení od příjemce).
Telefonní hovory (včetně VOIP)	Informace by měly být sdělovány pouze po identifikaci osoby jako oprávněné pro přístup k těmto informacím.
Způsob likvidace	**Informace na lidsky čitelném nosiči** (tištěné dokumenty, poznámky a podobně): Fyzická likvidace: Znehodnocení nosiče informací použitím skartovacího stroje s podélným i příčným řezem, spálením nebo rozložením.

	Mobilní zařízení (mobilní telefony, tablety), **Síťová zařízení** (router, switch, modem a podobně), **Kancelářské vybavení** (scanery, tiskárny, fax), **Magnetická média** (magnetické pásky, disky, HDD [Hard Disk Drive]): Fyzická likvidace: Rozebrání zařízení a zničení nosiče informací. **Optická média** (CD, DVD, HD-DVD, BLU-RAY), **Elektronická média** (flash paměti): Fyzická likvidace: Zničení nosiče informací. **Outsourcing a cloud**: Přípustný způsob likvidace dat by měl být stanoven smluvním ujednáním. Přepsání: Použití šifrování datových úložišť na úrovni paměťového média a bezpečná likvidace kryptografických klíčů uložených v certifikovaném hardware security modulu (HSM) řízená zákazníkem (například podle standardu FIPS 140-2 Level 2). Při ukončení služby bude zlikvidován vrchní přístupový klíč a data jsou přepsána.

Komunikační kanál	**Klasifikace aktiv: Velmi citlivé**
Poskytování aktiv v rámci organizace	Pouze se souhlasem garanta daného primárního aktiva.
Poskytování informací třetím stranám	Informace mohou být třetím stranám poskytovány pouze se souhlasem garanta daného primárního aktiva a na základě dohody o mlčenlivosti.
Nepřenosná datová média (pevné disky, stolní počítače, servery apod.)	Data musí být zašifrována s použitím nasazeného šifrovacího řešení.
Přenosná datová média (CD, DVD, flash disky apod.)	Data musí být zašifrována s použitím nasazeného šifrovacího řešení a bezpečným způsobem fyzicky uložena. Po použití je nutná likvidace. Médium musí být označeno „VELMI CITLIVÉ“.
Přenosná výpočetní technika (notebooky, chytré telefony apod.)	Data musí být zašifrována s použitím nasazeného šifrovacího řešení. Přenosná technika musí být chráněna proti ztrátě či krádeži.

Internet – ukládání a publikace (cloudová úložiště, sociální sítě)	Data nesmí být ukládána v rámci internetových úložišť nebo veřejně přístupných webech a sociálních sítích.
Přenos po internetu (mezi systémy)	Data je nutno přenášet pouze prostřednictvím šifrovaného kanálu.
Intranet	Přístup k datům musí být omezen pouze na určenou skupinu uživatelů a monitorován. Data musí být zašifrována s použitím nasazeného šifrovacího řešení.
Papírové dokumenty	Interně musí být dokumenty označeny jako „VELMI CITLIVÉ“ a bezpečně uloženy v trezoru. Po použití je nutná likvidace. Mimo organizaci je třeba převážet pouze osobně, v zapečetěné obálce a pouze adresátům, kteří byli schváleni garantem daného primárního aktiva.
E-mail	Data musí být zašifrována s použitím nasazeného šifrovacího řešení.
FAX	Dokumenty musí být označeny jako „VELMI CITLIVÉ“. Povoleno pouze v případě, že je použita šifrovací technologie pro přenos pomocí FAXu.
Telefonní hovory (včetně VOIP)	Informace by měly být sdělovány pouze po identifikaci osoby jako oprávněné pro přístup k těmto informacím a pouze pokud je telefonní hovor šifrován.
Způsob likvidace	**Informace na lidsky čitelném nosiči** (tištěné dokumenty, poznámky a podobně): Fyzická likvidace: Znehodnocení nosiče informací použitím skartovacího stroje s podélným i příčným řezem, spálením nebo rozložením. **Mobilní zařízení** (mobilní telefony, tablety), **Síťová zařízení** (router, switch, modem a podobně), **Kancelářské vybavení** (scanery, tiskárny, fax), **Magnetická média** (magnetické pásky, disky, HDD [Hard Disk Drive]): Fyzická likvidace: Rozebrání zařízení a zničení nosiče informací. **Optická média** (CD, DVD, HD-DVD, BLU-RAY), **Elektronická média** (flash paměti): Fyzická likvidace: Zničení nosiče informací. **Outsourcing a cloud**: Přípustný způsob likvidace dat by měl být stanoven smluvním ujednáním.

	Přepsání/fyzická likvidace: Použit způsob viz klasifikace aktiv „Citlivá“ nebo použita dedikovaná paměťová kapacita úložiště. Při ukončení služby provedena celková sanitizace všech použitých paměťových médií podle výše uvedených řádků pro úroveň kritická.

7. Bezpečnost lidských zdrojů

7.1. Poskytovatel se zavazuje prověřit každého pracovníka před umožněním přístupu k Datům nebo před jeho zapojením do činností, které by mohly ovlivnit předmět plnění Smlouvy, a to alespoň z hlediska:

a. kontroly dosaženého vzdělání a odborné kvalifikace;

b. ověření bezpečnostní způsobilosti dle výpisu z rejstříku trestů;

c. profesních zkušeností, jde-li o pracovníky, kteří mají zastávat bezpečnostní nebo administrátorské role.

7.2. Poskytovatel zavede pravidelné školení svých pracovníků v oblasti kybernetické bezpečnosti a základní kybernetické hygieny, realizuje alespoň 1x ročně další doplňující aktivity rozvoje povědomí v oblasti kybernetické bezpečnosti a vede o tomto školení a realizovaných aktivitách spolehlivou evidenci.

7.3. Poskytovatel poučí své pracovníky o požadavcích dle této Přílohy před umožněním jejich přístupu k Datům nebo před jejich zapojením do činností, které by mohly ovlivnit bezpečnost v souvislosti s předmětem plnění Smlouvy.

7.4. Poskytovatel zajistí, aby pracovníci před umožněním jejich přístupu k Datům nebo před zapojením do činností, které by mohly ovlivnit bezpečnost předmětu plnění Smlouvy, měli uzavřenou dohodu o zachování mlčenlivosti (důvěrnosti) Dat s adekvátní dobou trvání povinnosti mlčenlivosti.

7.5. Poskytovatel zajistí procesy a pravidla vedení disciplinárního řízení (zejména odstupňované reakce) a v případě potřeby provádí disciplinární řízení k přijetí opatření vůči pracovníkům, kteří porušili povinnosti v oblasti kybernetické bezpečnosti.

7.6. Poskytovatel zajistí dostatečnou míru zastupitelnosti pro technické bezpečnostní aspekty plnění smlouvy.

8. Řízení provozu

8.1. Poskytovatel stanoví práva a povinnosti administrátorů, uživatelů a osob zastávajících bezpečnostní role.

8.2. Poskytovatel stanoví pravidla a postupy pro ochranu před škodlivým kódem a pravidla a postupy pro řízení technických zranitelností.

8.3. Poskytovatel stanoví pravidla a postupy k provádění pravidelného zálohování a kontroly použitelnosti prováděných záloh.

8.4. Poskytovatel stanoví pravidla pro zajištění oddělení vývojového, testovacího a provozního prostředí.

9. Řízení přístupu

9.1. Zásady řízení přístupu k Datům Objednatele:

a. Politika řízení přístupu Poskytovatele by měla být nastavena, dokumentována, a revidována na základě business požadavků a požadavků informační bezpečnosti tak, aby efektivně chránila důvěrnost, dostupnost a integritu Dat dle jejich kritičnosti/citlivosti.

b. Mohou být provozována pouze taková aktiva, která umožňují správu rolí a uživatelů a která neumožní činnost uživatelů bez autentizace a zároveň umožňují ochranu autentizačního mechanismu před neoprávněným přístupem a prolomením autentizačních parametrů.

c. Poskytovatel je povinen zajistit, že součástí každé aplikace je funkce řízení přístupu odpovídající kritičnosti zpracovávaných informací.

d. Uživatelské účty musí být adekvátně chráněny prostřednictvím autentizačních mechanismů;

e. Účty musí být vytvářeny výhradně pro fyzické osoby a výhradně fyzickými osobami využívány. Jedinou výjimkou jsou technické účty.

f. Sdílené uživatelské účty, tedy účty, které má používat skupina lidí, by neměly být vytvářeny, protože neumožňují přiřazení individuální odpovědnosti. Nemělo by být k dispozici anonymní používání systémů a služeb nebo používání sdílených účtů.

g. Uživatelé musí chránit své uživatelské účty, zejména své autentizační údaje a nástroje a nesmí poskytnout tyto údaje třetí straně.

h. Výchozí nebo dočasná hesla musí být změněna při prvním použití uživatelem. Individuální heslo uživatele musí být uchováno v tajnosti.

i. Hesla, uživatelské účty a šifrovací klíče nesmí být nijak a s nikým sdíleny, např. telefonicky, e-mailem nebo jakýmkoliv jiným způsobem.

j. Poskytovatel musí monitorovat užívání sítí, služeb, aplikací a dat, aby byl schopen zjistit neoprávněný přístup a zamezit mu. Aktivity administrátorů musí být logovány a logy musí být chráněny před změnou nebo neoprávněným přístupem.

k. Používání nepersonifikovaných účtů (např. “root” nebo “správce”) je dovoleno pouze v případě, že není z technických důvodů jiná možnost. V tomto případě musí být přístup k takovým účtům monitorován a logován.

9.2. Role řízení přístupů:

a. Poskytovatel je povinen implementovat oddělení povinností u rolí nejméně na:

- podávání žádostí o přístup,
- udílení přístupů a
- správu přístupů.

b. Řízení přístupů by mělo být řešeno na základě rolí.

9.3. Politika řízení přístupu:

a. Politika řízení přístupů musí být pravidelně revidována a aktualizována. Politika musí odpovídat legislativním a smluvním požadavkům.

b. Politika řízení přístupů musí požadovat:

- Schvalování žádostí uživatelů o přístup vlastníkem aktiva.
- Oddělení neslučitelných povinností.
- Přístup na základě principu “need to know”.
- Zachování principu “deny by default”.
- Privilegovaná přístupová oprávnění.
- Sdílené uživatelské účty.
- Revize přístupových oprávnění.
- Odebírání přístupových oprávnění.
- Vícefaktorovou autentizaci při přístupu k citlivým IT komponentám nebo vzdáleném přístupu k datům Objednatele.

9.4. Přihlašování a pravidla přístupů:

a. Hesla defaultních účtů musí být změněna během úvodního nastavení systému. Přiřazená hesla musí splňovat minimální bezpečnostní požadavky tak, aby efektivně chránila důvěrnost,

dostupnost a integritu informací, ke kterým má Poskytovatel přístup, dle jejich kritičnosti/citlivosti.

b. Zamykání obrazovky a klávesnice (např. spořič obrazovky zamčený heslem) musí být používáno, umožňuje-li to operační systém používaných IT komponent.

c. Musí být zavedeny postupy pro odebírání nebo blokování přístupových oprávnění uživatelů v případě potřeby, zejména pokud:

- zaměstnanec již nepotřebuje přístup k plnění svých pracovních povinností (např. pokud došlo ke změně pozice zaměstnance),
- zaměstnanec se dopustil závažného porušení povinností v oblasti kybernetické bezpečnosti nebo existují důvodné obavy, že se takového porušení dopustí,
- zaměstnanec nesplňuje požadavky na přístup k Datům nebo požadavky na zapojení do činností, které by mohly ovlivnit bezpečnost předmětu plnění Smlouvy,
- se ukáže potřeba přijmout mimořádné bezpečností opatření spočívající v odebrání přístupu (zejména pokud Poskytovatel dal zaměstnanci výpověď z výpovědního důvodu podle § 52 písm. f), g) a h) zákoníku práce),
- dojde k ukončen pracovní poměr nebo jiné formy spolupráce,
- došlo k úniku autentizačních údajů (hesla),

aby bylo zajištěno, že [účty ve všech systémech, ke kterým měl uživatel přístup, jsou bezodkladně zablokovány, přístupová oprávnění k vybavení a službám zpracování dat jsou bezodkladně odebírána a / nebo přihlašovací údaje (např. ID uživatele, heslo, token nebo digitální certifikát) jsou bezodkladně zablokované a / nebo komponenty, které umožňují přístup, jako jsou tokeny nebo identifikační karty zaměstnanců, jsou bezodkladně zablokovány nebo deaktivovány v systému].

d. Musí být vedena evidence o udělených a odebraných přístupových oprávněních.

e. Všechny IT komponenty musí být před předáním uživatelům konfigurovány tak, aby citlivé bezpečnostní operace mohly vykonávat pouze osoby s příslušným oprávněním (správci). O výjimkách musí být informována příslušná osoba Objednatele. Výjimky musí být předem schváleny a zdokumentovány.

f. Poskytovatel může být Objednatelem požádán, aby mu poskytnul podporu při provádění auditu uživatelských oprávnění v systémech pod kontrolou Poskytovatele. Poskytovatel musí poskytnut podporu, která bude pro tento účel potřebná.

10. Akvizice, vývoj a údržba

10.1. Poskytovatel zajistí, aby požadavky na zajištění bezpečnosti Dat byly zahrnuty do všech vývojových, implementačních či akvizičních projektů, kde je reálné narušení informační bezpečnosti Dat a ochrany soukromí, a vyčlení pro tento účel potřebné zdroje.

10.2. Poskytovatel zajistí oddělení vývojového, testovacího a provozního prostředí.

11. Zvládání kybernetických bezpečnostních událostí a incidentů

11.1. Poskytovatel zajistí, aby jeho pracovníci a dodavatelé oznamovali neobvyklé chování technických aktiv a podezření na jakékoliv zranitelnosti a hrozby.

11.2. Poskytovatel vede a uchovává záznamy o kybernetických bezpečnostních incidentech a o jejich zvládání.

11.3. Poskytovatel prošetří a určí příčiny kybernetického bezpečnostního incidentu. Poskytovatel poskytne Objednateli aktivní součinnost a relevantní informace o příčinách, podezřelém zařízení či osobě na straně Poskytovatele v případě kybernetického bezpečnostního incidentu souvisejícího s Daty.

12. Fyzická bezpečnost

12.1. Poskytovatel se zavazuje zajistit:

a. dodržování politiky čistého stolu;

b. kanceláře, pracovní místnosti a prostory v případě jejich opuštění tak, aby nemohlo dojít k nedovolenému vstupu neoprávněných osob;

c. uzamykání pracovních stolů, skříní, kontrolovat uzavření oken;

d. dodržování režimových opatřeních v případě režimových pracovišť (perimetr s řízeným vstupem).

12.2. Poskytovatel bere na vědomí, že Objednatel vede evidenci osob, které vstupují do neveřejných částí objektů Objednatele, a evidenci vozidel, která vjíždějí do objektů Objednatele.

13. Bezpečnost komunikačních sítí

13.1. Poskytovatel se zavazuje zajistit:

a. vhodnou segmentaci komunikační sítě,

b. ochranu komunikační sítě bezpečným rozhraním, přičemž bude povolena pouze nutná komunikace;

c. aby na síťových zařízeních byly spuštěny pouze nutné služby;

d. sledování zranitelností nasazených síťových zařízení a odstraňování zjištěných zranitelností v dostatečných intervalech;

e. šifrování přenosu informací a dat v rámci komunikační sítě.

14. Správa a ověřování identit

14.1. Poskytovatel se zavazuje:

a. používat nástroj pro správu a ověření identity (autentizační mechanismus), který přenáší a ukládá autentizační parametry v šifrované podobě;

b. používat autentizační mechanismus, který je založený na více faktorové autentizaci s nejméně dvěma různými typy faktorů, pokud je to možné;

c. v případě ztráty, vyzrazení nebo podezření na kompromitaci autentizačních nástrojů nebo parametrů je třeba okamžitě změnit parametry autentizace;

d. aktiva, která nepodporují více faktorovou autentizaci, mohou dočasně zajistit autentizaci pomocí podobně silných kryptografických klíčů nebo hesel.

e. pokud je autentizace založena na heslech a nevyužívá se více faktorové autentizace, musí systém vynucovat hesla s vlastnostmi podle aktuální best practice.

15. Ochrana před škodlivým kódem

15.1. Poskytovatel zajistí použití nástroje pro nepřetržitou automatickou ochranu koncových zařízení.

15.2. Poskytovatel monitoruje a řídí používání výměnných zařízení a datových nosičů a jejich automatické spouštění.

15.3. Poskytovatel provádí pravidelnou a účinnou aktualizaci nástroje pro ochranu před škodlivým kódem.

16. Detekce, zaznamenávání a vyhodnocování kybernetických bezpečnostních událostí

16.1. Poskytovatel se zavazuje zajistit:

a. aby všechny klíčové prvky propojující významné uzly interních komunikačních sítí, bezpečnostní síťové prvky a všechny prvky na vnějším perimetru měly aktivní monitorování kybernetických bezpečnostních událostí;

b. aby monitorování sítě zajišťovalo ověření a kontrolu přenášených dat v rámci komunikační sítě a mezi komunikačními sítěmi, ověření a kontrolu přenášených dat na perimetru komunikační sítě;

c. aby v interních sítích byl provozován IDS/IPS.

d. aby detekovaná nežádoucí komunikace byla automaticky blokována;

e. aby byly zaznamenávány kybernetické bezpečnostní události narušující integritu síťových prvků nebo síťové komunikace, aby tyto záznamy byly uchovány a poskytnuty Objednateli na vyžádání;

16.2. Poskytovatel nasadí nástroje typu SIEM pro počáteční posouzení, zda zachycené události představují bezpečnostní událost nebo incident, přičemž tyto nástroje budou schopné rozdělit a zpracovat událost nebo řetězec událostí alespoň do 3 kategorií:

a. pozitivní – událost nebo sled událostí jednoznačně představuje bezpečnostní událost nebo bezpečnostní incident;

b. negativní – událost nebo sled událostí jednoznačně nepředstavuje bezpečnostní událost;

c. nejasný (falešně pozitivní / falešně negativní) – událost nebo sled událostí může v určitém kontextu představovat bezpečnostní událost nebo incident, ale v době hodnocení není možné událost jednoznačně klasifikovat, přičemž tyto události jsou dále hlášeny a hodnoceny pomocí jiných technik a nástrojů, případně ručně.

16.3. Poskytovatel zajistí, aby primární reakcí byla eskalace bezpečnostní události nebo incidentu do příslušných hlášení, případně přímá eskalace na příslušné odpovědné pracovníky.

17. Aplikační bezpečnost

17.1. Poskytovatel se zavazuje užívat technická aktiva, která jsou podporována, sledovat dostupnost opravných balíčků nebo záplat a zajistit bezodkladnou bezpečnostní aktualizaci. Pokud není bezpečnostní aktualizace dostupná, Poskytovatel zajistí jiné kompenzační řešení, případně zranitelnost může být akceptována.

18. Kryptografické algoritmy

18.1. Poskytovatel se zavazuje používat pouze aktuálně doporučované a odolné kryptografické algoritmy a kryptografické klíče.

19. Dodatečná bezpečnostní opatření

19.1. V případě, že Objednatel při hodnocení rizik spojených s touto Smlouvou identifikuje skutečnosti, jejichž existence tvoří podstatnou kybernetickou hrozbu a/nebo riziko pro předmět Smlouvy, a tyto dosahují kritické úrovně dle přílohy č. 2 VoKB, nebo v případě, že vyjde najevo, že Poskytovatel porušuje tuto Přílohu či takové porušení hrozí, porušuje Smlouvu včetně jejích dalších příloh podstatným způsobem či takové podstatné porušení hrozí, může Objednatel Poskytovateli uložit přijetí dalších bezpečnostních opatření ve smyslu § 5 ZoKB bez nutnosti přijetí dodatku Smlouvy ve smyslu § 100 odst. 1 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů. Objednatel při naplnění podmínek výše předá Poskytovateli seznam vybraných bezpečnostních opatření, která navrhuje ke snížení identifikovaného rizika zavést, a to včetně konkrétní specifikace formy bezpečnostního opatření. Poskytovatel je povinen bez zbytečného prodlení zavést požadovaná bezpečnostní opatření a jejich zavedení oznámit Objednateli. Poskytovatel je oprávněn do 5 pracovních dní podat připomínky k formě zvolených bezpečnostních opatření a navrhnout jinou formu zvolených bezpečnostních opatření, kterou je povinen zavést bez zbytečného prodlení, po jejich schválení Objednatelem, a jejich zavedení Objednateli oznámit.

19.2. Další bezpečnostní opatření přijatá dle tohoto článku Přílohy musí být přiměřená, přičemž součást ceny za plnění dle Smlouvy tvoří také náklady na implementaci bezpečnostních opatření, není-li určeno ve Smlouvě jinak.

20. Dokumentace

20.1. Poskytovatel je povinen zpracovat a do 30 pracovních dnů od zahájení poskytování plnění dle Smlouvy Objednateli předat dokumentaci, která bude ve smyslu přílohy č. 5 VoKB zahrnovat:

a. postupy pro řízení provozu a komunikací;

b. postupy pro řízení přístupů (konkrétní postupy pro pracovníky Poskytovatele a jeho poddodavatele podílející se na poskytování plnění dle Smlouvy);

c. postupy pro bezpečné chování uživatelů (konkrétní postupy pro pracovníky Poskytovatele a jeho poddodavatelů podílející se na poskytování plnění dle Smlouvy);

d. postupy pro zálohování a obnovu a dlouhodobé ukládání;

e. postupy pro řízení technických zranitelností;

f. postupy pro zajištění bezpečnosti komunikační sítě;

g. postupy pro ochranu před škodlivým kódem;

h. postupy pro nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí

i. postupy pro bezpečné používání kryptografické ochrany

j. postupy pro řízení změn;

k. postupy pro zvládání incidentů;

l. pro řízení kontinuity činnosti;

m. datový model a modely architektonické modely v grafickém jazyce ArchiMate;

n. přehled jednotlivých zařízení pro poskytovanou službu (v rozsahu konfiguračních údajů CMDB aktualizovaných na denní bázi: obecný název, typ zařízení, označení výrobce, sériové číslo, ID/tag, typ HW včetně verze, typ SW včetně verze, typ a počet CPU, velikost RAM, výrobcem udávaný příkon, řešitelská skupina odpovědná za zařízení, emailový a telefonický kontakt na řešitelskou skupinu odpovědnou za zařízení);

o. další dokumentaci relevantní pro poskytování služby (přehled topologie infrastruktury pro poskytovanou službu; konfigurační standard včetně nastavení zabezpečení pro jednotlivá zařízení minimálně v takovém rozsahu, aby dle něj bylo možné nastavit nové zařízení v případě havárie).

20.2. Nejsou-li požadavky na obsah konkrétní části dokumentace podle odst. 20.1 této Přílohy stanoveny VoKB, ZoKB, Smlouvě (vč. této Přílohy) ani výkladovém dokumentu Národního úřadu pro kybernetickou a informační bezpečnost, uplatní se pro zpracování dokumentace příměřně požadavky mezinárodně platných technických norem, zejména ISO/IEC/IEEE 15289, ISO/IEC/IEEE 26511, ISO/IEC/IEEE 26512, ISO/IEC 26513 a ISO/IEC/IEEE 26515.

20.3. Dokumentaci podle odst. 20.1 této Přílohy je Poskytovatel povinen revidovat a případně aktualizovat nejméně jednou ročně a dále kdykoli při změně skutečností zachycených v dokumentaci. Poskytovatel je povinen výsledek provedené revize a případné aktualizace oznámit Objednateli bez zbytečného odkladu od jejich provedení.

20.4. Objednatel a Poskytovatel se zavazují podrobit předání a převzetí dokumentace podle odst. 20.1 této Přílohy akceptačnímu řízení, přičemž lhůta pro připomínkování dokumentů se stanoví na 10 pracovních dnů od obdržení příslušného dokumentu a lhůta k odstranění vad dokumentů se stanoví na 10 pracovních dnů od obdržení připomínek k tomuto dokumentu. Nestanoví-li Smlouva pravidla akceptačního řízení, má Objednatel ve lhůtě pro připomínkování dokumentů právo vytknout zhotoviteli vady dokumentů. Dokument má vadu, je-li v rozporu s požadavky ZoKB, VoKB

nebo Smlouvy (vč. této Přílohy). Poskytovatel je povinen ve lhůtě k odstranění vad dokumentů předat Objednateli dokumenty bez vad vytčených Objednatelem. Tato procedura se může opakovat, nejsou-li vady dokumentů odstraněny řádně.

21. Autorství a licence

21.1. Není-li ve Smlouvě stanoveno jinak uplatní se na autorství a licence čl. 21 této Přílohy.

21.2. Pokud bude výsledkem činnosti Poskytovatele a součástí plnění Poskytovatele dle Smlouvy dílo, které naplňuje znaky díla dle zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „**autorské dílo**“), a také v případě že bude jakékoli dílo naplňující tyto znaky autorského díla při plnění Poskytovatele použito, prohlašuje Poskytovatel, že Objednatel na základě Smlouvy a v souladu s ní získal veškerá oprávnění k takovému autorskému dílu, aby byl splněn účel Smlouvy.

21.3. Odměna za poskytnutí, zprostředkování nebo postoupení licence k autorskému dílu je zahrnuta v ceně dle Smlouvy.

22. Provádění auditů

22.1. Není-li ve Smlouvě stanoveno jinak uplatní se na provádění auditů čl. 22 této Přílohy.

22.2. Poskytovatel umožní, na základě předchozí výzvy ze strany Objednatele doručené v přiměřeném časovém předstihu a pouze v nezbytném rozsahu, přístup k údajům, účtům, záznamům, pracovním postupům, technické dokumentaci a jiným dokladům či podkladům, do prostor a k technickým prostředkům vztahujícím se k plnění této Smlouvy (dále jen "**Auditované materiály**"), a to za účelem uskutečnění auditu provozních a technologických procesů a/nebo bezpečnostních opatření používaných Poskytovatelem při plnění povinností vyplývajících z této Přílohy a Smlouvy (dále jen "**Audit**").

22.3. Audit bude prováděn dle potřeb Objednatele, a to v pravidelných intervalech a v případě bezpečnostních událostí, důvodného podezření na nedostatečnou úroveň ochrany Dat či aktiv Objednatele či důvodného podezření na nakládání s Daty či aktivy Objednatele v rozporu s relevantními ustanoveními Smlouvy a důvodného podezření na nedodržení bezpečnostních opatření podle této Přílohy.

22.4. Audit bude prováděn Objednatelem nebo jím pověřeným externím auditorem, smluvně zavázaným k mlčenlivosti minimálně v rozsahu odpovídajícím povinnostem mlčenlivosti Objednatele dle Smlouvy, a která není k Poskytovateli v soutěžním nebo jiném konkurenčním postavení.

22.5. Poskytovatel poskytne veškerou nezbytnou součinnost k řádnému provádění a dokončení Auditu a pro tuto činnost zajistí účast kvalifikovaných pracovníků.

22.6. Jakákoliv data, informace nebo jiná aktiva získaná při Auditu mohou být použita výhradně pro účely Auditu, vyhodnocení jeho výsledků a přijetí navazujících opatření a pro další potřeby Objednatele při řízení vztahu s Poskytovatelem.

22.7. Poskytovatel je povinen bez zbytečného odkladu, nejpozději však do 1 měsíce od ukončení auditu, předložit Objednateli návrhy opatření napravujících nedostatky zjištěné při Auditu. Jednotlivá opatření navržená v návaznosti na výsledky Auditu podléhají před jejich přijetím Poskytovatelem předchozímu schválení ze strany Objednatele. Návrhy zřejmě nevhodných či neúčinných opatření Objednatel odmítne a Poskytovatel je povinen v přiměřené lhůtě stanovené Objednatelem navrhnout jiná vhodná opatření. Poskytovatel je taktéž povinen se na výzvu Objednatele podrobit dodatečné kontrole ze strany Objednatele nebo osoby, která Audit provedla, za účelem ověření nápravy nedostatků zjištěných při Auditu a kontroly přijatých opatření.

22.8. Součást ceny za plnění dle Smlouvy tvoří také náklady na provedení jednoho Auditu za kalendářní rok. Pokud Audit odhalí jakékoliv podstatné porušení Smlouvy nebo hrozbu takového podstatného porušení, uhradí Poskytovatel Objednateli veškeré důvodně vynaložené náklady vzniklé v důsledku Auditu a porušení bezodkladně napraví vč. případné implementace dodatečných bezpečnostních opatření.

23. Řízení změn

23.1. Poskytovatel se zavazuje sledovat a identifikovat změny, které mají nebo mohou mít vliv na zajištění kybernetické bezpečnosti Dat Objednatele a informovat Objednatele o této skutečnosti.

23.2. Poskytovatel se zavazuje, vyjeví-li se skutečnost, že by změna mohla být významnou změnou nebo dá-li Objednatel Poskytovateli takový pokyn, zejména před nasazením nové technologie (hardware a software) nebo při změně stávající technologie nebo při změně postupu správy technologie, která je předmětem plnění smluvního vztahu se Objednatelem, zajistit:

a. identifikaci a vyhodnocení možných dopadů změny na kybernetickou bezpečnost;

b. vyhodnocení, zda změna je významnou změnou dle § 11 VoKB, a při tomto vyhodnocení zohlednit politiku řízení změn Objednatele;

c. předání dokumentace vyhodnocení změny dle předchozích písmen Objednateli k určení změny jako významné změny dle § 11 VoKB;

d. posouzení rizik související s významnou změnou ve vztahu k plnění dle Smlouvy a dokumentovat toto posouzení.

23.3. Poskytovatel se zavazuje při provádění významných změn zajistit:

a. dokumentované řízení realizace významné změny;

b. bezpečnostní testování významné změny před jejím zavedením do provozu v souladu s požadavky § 13 písm. f) VoKB o posouzení možnosti případného navrácení do původního stavu; a

c. zpracování dokumentace skutečného provedení významné změny (popis konfigurace a bezpečnostních nastavení, způsob řízení přístupu včetně vytvořených účtů a přidělených oprávnění, postupy zálohování a obnovy dat, postupy pro zajištění kontinuity provozu a obnovy po havárii) a související aktualizaci dokumentace dle článku 10 této Přílohy a provedení dalších činností.

23.4. Poskytovatel se zavazuje reagovat na změny, zejména aktualizovat hodnocení rizik, bezpečnostní a provozní dokumentaci a upravit na své straně bezpečnostní opatření tak, aby odpovídala novému stavu po provedení změny.

23.5. Poskytovatel se zavazuje při plnění Smlouvy přiměřeně postupovat dle systému řízení změn Objednatele vymezeným v souladu s § 11 a § 13 VoKB.

24. Informační povinnost Poskytovatele

24.1. Poskytovatel je povinen Objednatele bez zbytečného odkladu informovat o:

a. identifikovaných kybernetických bezpečnostních incidentech a hrozbách souvisejících s plněním Smlouvy, nejpozději však do 48 hodin od výskytu;

b. způsobu řízení rizik na straně Poskytovatele a o zbytkových rizicích souvisejících s plněním Smlouvy;

c. významné změně ovládání Poskytovatele, přičemž ovládáním se rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů, či ekvivalentní postavení, a to do 5 pracovních dnů od uskutečnění této změny; a

d. změně vlastnictví či oprávnění nakládat se zásadními aktivy využívanými Poskytovatelem k plnění Smlouvy, a to do 5 pracovních dnů od uskutečnění této změny;

e. změnách v rámci poddodavatelského řetězce Poskytovatele souvisejících s plněním Smlouvy.

24.2. Poskytovatel je povinen poskytnout Objednateli a příslušným dozorovým orgánům veškerou nutnou součinnost v případě dozorového auditu za účelem ověření řízení kybernetické bezpečnosti.

25. Proces ukončení Smlouvy a řízení kontinuity

25.1. Není-li ve Smlouvě stanoveno jinak uplatní se na pravidla pro ukončení Smlouvy a řízení kontinuity čl. 25 této Přílohy.

25.2. Smluvní strany se dohodly, že při ukončení Smlouvy z jakéhokoli důvodu vyvinou veškeré úsilí k tomu, aby do doby dokončení migrace Dat či převodu plnění dle Smlouvy k Objednateli nebo jinému provozovateli, nedošlo k narušení parametrů plnění ve Smlouvě do té doby definovaných, a aby případný nový provozovatel dostal veškeré informace o plnění Smlouvy potřebné pro pokračování nebo nahrazení takového plnění.

25.3. Poskytovatel se zavazuje v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 15 VoKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:

a. ve spolupráci se Objednatelem určit aktiva potřebná k poskytování plnění dle Smlouvy, zpracovat a poskytnout Objednateli plány kontinuity a havarijní plány v souvislosti s těmito aktivy, a případně tyto plány upravit dle požadavků Objednatele;

b. zajistit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování předmětu plnění; a pravidelně kontrolovat a testovat, že je schopen kontinuitu aktiv zajistit dle sjednané úrovně služeb.

25.4. Poskytovatel se zavazuje poskytnout nezbytnou součinnost při zpracování plánů obnovy a havarijních plánů a dalších povinností Objednatele.

26. Smluvní pokuta

26.1. V případě porušení jakékoli povinnosti Poskytovatele dle této Přílohy, je Objednatel oprávněn požadovat smluvní pokuty, jak jsou vymezený níže, a to za každé jednotlivé porušení. Objednatel je oprávněn požadovat pokuty v případě, že:

a. došlo k porušení této Přílohy, a to ve výši 250.000,- Kč, a to za každý jednotlivý případ takového porušení; nebo

b. došlo k porušení této Přílohy, přičemž toto porušení vedlo ke kybernetickému bezpečnostnímu incidentu, a to ve výši 500.000,- Kč, a to za každý jednotlivý případ takového porušení.

26.2. Smluvní pokutou není dotčeno Objednatelovo právo požadovat náhradu škody ve výši převyšující zaplacenou smluvní pokutu.

27. Ostatní ujednání

27.1. Poskytovatel se zavazuje provádět veškerá plnění dle Smlouvy v souladu se Smlouvou, příkazy Objednatele, s předanými podklady a dále v souladu s právními předpisy, zejména ZoKB a VoKB. Poskytovatel se zavazuje při výkonu své činnosti včas a prokazatelně upozornit Objednatele na zřejmou nevhodnost jeho příkazů či doporučení vztahujících se k pravidlům bezpečnosti, jejichž následkem může vzniknout újma nebo nesoulad s právními předpisy a zajistit ve spolupráci se Objednatelem náhradní způsob naplnění pravidel bezpečnosti, pokud stávající řešení přestalo být funkční nebo efektivní.

27.2. Pokud není ve Smlouvě nebo v této Příloze uvedeno jinak, odměna za provádění povinností a opatření dle této Přílohy a Kybernetických požadavků je součástí odměny dle Smlouvy.

27.3. Poskytovatel je oprávněn odstoupit od Smlouvy, pokud dojde k významné změně kontroly nad Poskytovatelem, přičemž kontrolou se rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2020 Sb., o obchodních korporacích, ve znění pozdějších předpisů, či ekvivalentní postavení nebo dojde ke změně vlastnictví či oprávnění nakládat se zásadními aktivy využívanými Poskytovatelem k plnění Smlouvy a tato změna bude Objednatelem vyhodnocena jako bezpečnostní riziko ve smyslu ZoKB a/nebo VoKB.