Rámcová dohoda na poskytování integračních a

konfiguračních služeb

Číslo 2022/066 NAKIT

Smluvní strany

### Národní agentura pro komunikační a informační technologie, s. p.

se sídlem Kodaňská 1441/46, Vršovice, 101 00 Praha 10

IČO: 04767543

DIČ: CZ04767543

zastoupen: xxx

zapsán v obchodním rejstříku vedeném Městským soudem v Praze oddíl A vložka 77322 bankovní spojení xxx

č.ú. xxx

(dále jen **„Objednatel“**)

a

### Společnost SEVITECH

vzniklá na základě smlouvy o společnosti uzavřené dne 26. 1. 2022 mezi níže uvedenými společně a nerozdílně zavázanými společníky:

SEVITECH CZ s.r.o.

se sídlem Na strži 2102/61a, Krč, 140 00 Praha 4

IČO: 07081561

DIČ: CZ07081561

zastoupen: xxx

zapsán v obchodním rejstříku vedeném Městským soudem v Praze oddíl C vložka 294361 bankovní spojení xxx

č.ú. xxx

(dále jen „**Vedoucí společník**“)

SYNCHRONIX a.s.

se sídlem Mlynské nivy 71, Bratislava 821 05

IČO: 31 605 052

DIČ: 2020444338

zastoupen: xxx a xxx

zapsán v obchodním rejstříku vedeném Okresním soudem Bratislava I. oddíl: Sa, vložka 4696/B

(dále jen „**Druhý společník**“)

Ve vztahu k Objednateli a této Smlouvě je za Společnost SEVITECH oprávněn jednat její Vedoucí společník, tj. SEVITECH CZ s.r.o.

(dále Společnost SEVITECH jen jako „**Dodavatel**“)

dále jednotlivě jako „**Smluvní strana**“ nebo společně jako „**Smluvní strany**“ uzavírají v souladu s ustanovením § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**občanský zákoník**“), zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „**AZ**“) a ustanoveními zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**“), tuto rámcovou dohodu na poskytování integračních a konfiguračních služeb (dále jen „**Smlouva**“).

### Preambule

Objednatel provedl v souladu s ustanoveními ZZVZ zadávací řízení k veřejné zakázce

### „Dodání komponent a rolí pro zajištění dalších činností v rámci projektu ISSI II.“ (dále jen

„**Zadávací řízení**“) na uzavření této Smlouvy. Tato Smlouva je uzavřena s Dodavatelem na základě výsledku Zadávacího řízení. Objednatel tímto ve smyslu ustanovení § 1740 odst. 3 občanského zákoníku předem vylučuje přijetí nabídky na uzavření této Smlouvy s dodatkem nebo odchylkou.

V souvislosti s touto Smlouvou byly uzavřeny mezi tentýž Smluvními stranami ještě Smlouva na dodávku GIS SW systému pro data INSPIRE, licencí SW a souvisejících služeb a Smlouva o poskytnutí Podpory GIS Systému, kdy tyto tři smlouvy tvoří společně předmět shora uvedené veřejné zakázky a jsou uzavírány se společným účelem. Tyto tři shora uvedené smlouvy na sebe vzájemně navazují a je nezbytné je vykládat ve vzájemné souvislosti.

### Účel a předmět Smlouvy

* 1. Účelem této Smlouvy je zajištění integrace a konfigurace Geografického informačního systému pro data INSPIRE (Infrastruktura pro prostorová data v Evropě) (dále jen „**GIS Systém**“) v rámci ISSI (Informační systém pro veřejné služby a služby veřejné správy INSPIRE), to vše v souladu s požadavky Objednatele definovanými touto Smlouvou a za účelem plnění závazků Objednatele vůči Ministerstvu vnitra České republiky (dále jen „**Koncový zákazník**“ nebo „**MV**“).
  2. Předmětem této Smlouvy je stanovení podmínek, za kterých bude docházet mezi Smluvními stranami k uzavírání Dílčích smluv (jak je tento pojem definován v čl. [2](#_bookmark3) odst.

[2.6](#_bookmark4) této Smlouvy), na jejichž základě a za podmínek sjednaných v Dílčí smlouvě bude Dodavatel na svůj náklad a nebezpečí dodávat Objednateli plnění blíže specifikované touto Smlouvou a Dílčími smlouvami.

* 1. Předmět plnění dle této Smlouvy spočívá v zajištění odborných kapacit, zejména z oblasti ICT technologií a projektového řízení, a to jednak pro interní potřeby Objednatele a dále za účelem plnění závazků Objednatele vůči jeho zákazníkům na základě jeho potřeb a zadání. Zákazníkem se rozumí subjekt v postavení objednatele vůči Objednateli, jemuž Objednatel dodává zboží a poskytuje služby, a to zejména v oblasti ICT technologií. Zákazníkem Objednatele jsou přitom především orgány státní správy, v současnosti zejména Ministerstvo vnitra České republiky (dále tyto subjekty jednotlivě jako „**Koncový zákazník**“).

Objednatel jakožto dodavatel ICT zboží a služeb pro orgány státní správy se podílí na realizaci klíčových ICT projektů. V rámci plnění těchto projektů je pak potřeba zajistit odborné pracovníky, a to jak v oblasti projektového řízení a administrace projektů, tak v oblasti ICT technologií, architektury, odborných konzultací apod. Bližší specifikace předmětu plnění a poskytovaných služeb je uvedena v Příloze č. 1 této Smlouvy (dále jen „**Služby**“), a bude vždy upřesněna v konkrétní Objednávce a Dílčí smlouvě uzavřené postupem uvedeným v čl. [2](#_bookmark3) této Smlouvy.

Předmětem plnění dle této Smlouvy je tedy především zajištění odborných kapacit v rozsahu Objednatelem nadefinovaných rolí uvedených v Příloze č. 4 této Smlouvy.

Plnění poskytované Dodavatelem Objednateli z rámce sjednaného touto Smlouvou na základě konkrétní Dílčí smlouvy bude dále označováno jako „**Plnění**“.

* 1. Dodavatel prohlašuje a potvrzuje, že:
     1. je oprávněn uzavřít Smlouvu a plnit své povinnosti vyplývající ze Smlouvy;
     2. na straně Dodavatele není k uzavření Smlouvy ani ke splnění závazků Dodavatele z ní vyplývajících požadován žádný souhlas, udělení výjimky, schválení, prohlášení ani povolení jakékoliv třetí osoby či orgánu, popřípadě byly získány;
     3. uzavření Smlouvy Dodavatelem není (i) porušením jakékoliv povinnosti vyplývající z platných právních předpisů v jakémkoliv právním řádu, jímž je Dodavatel vázán, a/nebo (ii) porušením jakékoliv povinnosti vyplývající z jakékoliv smlouvy, jíž je Dodavatel stranou, a/nebo (iii) v rozporu s jakýmkoliv požadavkem, rozhodnutím nebo předběžným opatřením správního orgánu nebo soudu nebo rozhodčím nálezem rozhodců, jímž je Dodavatel vázán;
     4. splňuje veškeré požadavky na jeho způsobilost (kvalifikaci) stanovené v Zadávacím řízení;
     5. Dodavatel není v úpadku nebo v hrozícím úpadku ve smyslu § 3 zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), v platném znění. Proti Dodavateli nebyl podán (i) insolvenční návrh, nebo (ii) návrh na nařízení výkonu rozhodnutí, resp. obdobný návrh v příslušné jurisdikci či podle dříve platných českých právních předpisů, a podle nejlepšího vědomí Dodavatele podání takového návrhu ani nehrozí;
     6. nebyl předložen žádný návrh, ani učiněno žádné rozhodnutí příslušných orgánů Dodavatele ani žádného soudu o likvidaci Dodavatele nebo o jakékoliv jeho přeměně ve smyslu zákona č. 125/2008 Sb., o přeměnách obchodních společností a družstev, ve znění pozdějších předpisů;
     7. neprobíhá a podle nejlepšího vědomí a znalostí Dodavatele ani nehrozí žádné soudní, správní, rozhodčí ani jiné řízení či jednání před jakýmkoliv orgánem jakékoliv jurisdikce, které by mohlo, jednotlivě nebo v souhrnu s dalšími okolnostmi, nepříznivým způsobem ovlivnit schopnost Dodavatele splnit jeho závazky podle této Smlouvy;
     8. Dodavatel udržuje v platnosti ve všech zásadních ohledech licence, souhlasy, povolení a další oprávnění požadovaná právními předpisy platnými pro poskytnutí plnění dle Smlouvy a musí předcházet situaci, kdy by platnost takové licence, souhlasu, povolení a oprávnění byla ukončena. Plnění a jeho poskytnutí Objednateli nesmí být v rozporu s jakýmkoli právem třetí osoby na patentovou, známkoprávní, či jinou ochranu duševního vlastnictví, obchodní firmy či hospodářské soutěže;
     9. není si s vynaložením odborné péče vědom žádné překážky, týkající se Plnění, nebo místa či prostředí Objednatele, která by znemožňovala nebo znesnadňovala poskytnout plnění způsobem sjednaným podle Smlouvy;
     10. v okamžiku dodání Plnění na základě Dílčí smlouvy je výlučným vlastníkem hmotných složek Plnění a není jakkoliv smluvně či zákonně omezen v dispozici s hmotnými složkami Plnění, jeho nabývací právní tituly k hmotným složkám Plnění jsou platné, účinné a vymahatelné, a že je oprávněn převést bez dalšího vlastnické právo k hmotným složkám Plnění na Objednatele, že neuzavřel ohledně hmotných složek Plnění žádnou smlouvu, kterou by převáděl na jinou osobu vlastnická nebo jiná práva k hmotným složkám Plnění, ani smlouvu o smlouvě budoucí obsahující závazek k budoucímu převodu hmotných složek Plnění;
     11. hmotné složky Plnění nejsou zatíženy zástavními, předkupními, nájemními či jinými právy třetích osob, jinými věcnými právy ani jinými omezeními;
     12. žádná třetí osoba nevznesla nárok, v jehož důsledku by mohlo dojít k omezení práva Dodavatele hmotné složky Plnění převést na Objednatele;
     13. Smlouva představuje platný a právně závazný závazek Dodavatele, který je vůči Dodavateli vynutitelný v souladu s podmínkami Smlouvy;
     14. Dodavateli není známa žádná skutečnost, okolnost či událost, která by měla za následek nebo by mohla mít za následek absolutní či relativní neplatnost Smlouvy.
  2. Dodavatel se zavazuje zajistit, aby jeho prohlášení dle této Smlouvy zůstala pravdivá a v platnosti po celou dobu účinnosti Smlouvy.
  3. Služby dle této Smlouvy budou poskytovány prostřednictvím členů Realizačního týmu (jak je tento termín definován v čl. [3](#_bookmark7) odst. 3.3 této Smlouvy) v jednotlivých odborných rolích uvedených a specifikovaných v Příloze č. 4 této Smlouvy, kde je uveden i jmenný seznam konkrétních osob (členů Realizačního týmu) zastávajících vybrané role.
  4. Dodavatel se zavazuje při realizaci Předmětu plnění dle této Smlouvy respektovat a dodržovat podmínky uvedené v Příloze č. 6 této Smlouvy.
  5. Hovoří-li se v přílohách této Smlouvy o zadavateli, rozumí se jím Objednatel.

### Dílčí smlouvy a postup jejich uzavření

* 1. Dílčí smlouva představuje dílčí plnění z rámce sjednaného touto Smlouvou. Jednotlivá Plnění dle Smlouvy budou realizována na základě Dílčích smluv uzavíraných postupem specifikovaným v tomto článku Smlouvy, na základě písemných objednávek doručených Objednatelem Dodavateli (dále jednotlivě jen „**Objednávka**“). Na základě jednotlivých Dílčích smluv bude Dodavatel dodávat / poskytovat Objednateli Plnění podle konkrétních potřeb Objednatele, přičemž druh a množství Plnění budou vždy blíže specifikovány v Dílčí smlouvě.
  2. Objednávka musí obsahovat minimálně tyto náležitosti:
     1. identifikační údaje Objednatele a Dodavatele;
     2. číslo a datum vystavení Objednávky;
     3. označení Smlouvy;
     4. rozsah a specifikaci požadovaných Služeb (Plnění), přehled rolí a přehled člověkohodin / MD (jak je tento pojem definován v čl. [4](#_bookmark15) odst. [4.5](#_bookmark17) této Smlouvy) (případně člověkohodin) u jednotlivých rolí;
     5. požadovaný termín či harmonogram poskytnutí Plnění;
     6. místo poskytnutí Plnění;
     7. celkovou cenu Plnění dle příslušné Dílčí smlouvy (tato cena bude stanovena postupem dle čl. [4](#_bookmark15) odst. [4.1](#_bookmark16) této Smlouvy);
     8. lhůtu pro akceptaci Objednávky ze strany Dodavatele;
     9. podpis oprávněné osoby Objednatele.

Dále může Objednatel mj. specifikovat v Objednávce:

* parametry poskytování Plnění včetně sankcí za jejich nedodržení;
* požadavky na osvědčení pro přístup k utajovaným informacím dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „**ZOUI**“);
* kritéria akceptační procedury, jejichž splnění je pro akceptaci Plnění požadováno;
* případně další požadavky vztahující se k poskytování Plnění.
  1. Objednatel je oprávněn, avšak nikoli povinen vystavovat Objednávky ode dne účinnosti této Smlouvy dle svého uvážení. Každá takto vystavená Objednávka se považuje za písemnou výzvu k poskytnutí plnění a současně za návrh na uzavření Dílčí smlouvy za podmínek stanovených touto Smlouvou. Dodavatel je povinen písemně akceptovat Objednávku ve lhůtě pěti (5) pracovních dnů od jejího doručení Objednatelem, pokud nebude Objednatelem stanovena lhůta delší (dále jen „**Potvrzení**“).
  2. Potvrzení – akceptace Objednávky – musí obsahovat minimálně tyto náležitosti:
     1. identifikační údaje Objednatele a Dodavatele;
     2. číslo Objednávky, která je potvrzována;
     3. příslušné dokumenty, pokud budou Objednatelem v Objednávce požadovány;
     4. podpis oprávněné osoby Dodavatele.
  3. V případě, že Objednávka nebude splňovat uvedené minimální náležitosti, má Dodavatel povinnost na tuto skutečnost neprodleně upozornit Objednatele. Objednatel je poté oprávněn vystavit novou Objednávku a Dodavatel je povinen ji ve lhůtě pěti (5) pracovních dnů od jejího doručení písemně potvrdit. Dodací lhůta začíná běžet od okamžiku doručení této nové Objednávky.
  4. Doručením Potvrzení – akceptace Objednávky Dodavatelem – dojde k uzavření Dílčí smlouvy o poskytnutí Plnění (dále jen „**Dílčí smlouva**“), přičemž práva a povinnosti Smluvních stran dle této Dílčí smlouvy odpovídají v celém rozsahu právům a povinnostem Objednatele a Dodavatele stanoveným touto Smlouvou.
  5. Potvrzení, které obsahuje dodatky, výhrady, omezení nebo jiné změny se považuje za odmítnutí Objednávky a tvoří nový návrh Dodavatele na uzavření Dílčí smlouvy, a to i v případě takového dodatku, výhrady, omezení nebo jiné změny, které podstatně nemění podmínky Objednávky ve smyslu § 1740 odst. 3 občanského zákoníku. Dílčí smlouva je v takovém případě uzavřena pouze tehdy, pokud tento nový návrh Objednatel písemně potvrdí a doručí zpět Dodavateli. Výše uvedené dodatky, výhrady,

omezení nebo jiné změny uvedené v Potvrzení nesmí měnit smluvní podmínky tak, že se stanou pro Objednatele méně výhodné v porovnání s touto Smlouvou.

* 1. V případě, že bude Potvrzení obsahovat vady, je Objednatel povinen o tom Dodavatele písemně informovat včetně označení těchto vad a včetně lhůty pro opětovné doručení opraveného/doplněného Potvrzení, a to nejpozději ve lhůtě pěti (5) pracovních dnů od jeho doručení. Dodavatel je povinen odstranit případné vady Potvrzení, které budou řádně specifikované Objednatelem a opravené/doplněné Potvrzení opětovně předložit Objednateli.
  2. Objednatel při uzavírání Smlouvy negarantuje žádný minimální objem plnění, který bude zadán v průběhu její platnosti. Objednatel uzpůsobuje rozsah poptávaného plnění svým aktuálním potřebám, které jsou v čase proměnlivé. Dodavatel se přes výše uvedené zavazuje být připraven poskytnout plnění v rozsahu Služeb poptávaném Objednatelem dle podmínek Smlouvy. Počet Objednávek učiněných Objednatelem není omezený. Současně platí, že Objednatel není povinen učinit, byť jedinou Objednávku a tedy uzavřít, byť jedinou Dílčí smlouvu nebo objednat jakékoliv Plnění.
  3. Objednávka i Potvrzení musí být učiněny elektronickými prostředky a musí být zaslány druhé Smluvní straně prostřednictvím oprávněných osob uvedených v čl. [8](#_bookmark19) této Smlouvy.
  4. Dodavatel se zavazuje poskytovat Objednateli Plnění za podmínek uvedených v této Smlouvě a Dílčí smlouvě, ve sjednané specifikaci, jakosti, čase, množství a sjednaným způsobem. Dodavatel se zavazuje dodat Plnění v co nejlepším provedení a jakosti odpovídající aktuálnímu stavu technologického vývoje a poznání v dané oblasti a kategorii produktů, jakož i požadavkům Objednatele vymezeným v Příloze č. 1 této Smlouvy a příslušných Dílčích smlouvách.
  5. Objednatel se zavazuje Plnění řádně a včas poskytnuté v souladu s touto Smlouvou a příslušnou Dílčí smlouvou převzít a zaplatit za něj dohodnutou Cenu (jak je tento pojem definován v čl. [4](#_bookmark15) odst. [4.1](#_bookmark16) této Smlouvy).
  6. Každá Dílčí smlouva se řídí touto Smlouvou, pokud není v Dílčí smlouvě uvedeno výslovně jinak. Součástí Dílčí smlouvy jsou i podmínky stanovené v této Smlouvě, nestanoví-li Smluvní strany výslovně, že se konkrétní články této Smlouvy na konkrétní Dílčí smlouvu neužijí.
  7. Každá Dílčí smlouva nabývá platnosti dnem uzavření a účinnosti nejdříve uveřejněním příslušné Dílčí smlouvy v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů (dále jen **„zákon o registru smluv“**), není-li výslovně uvedeno pozdější datum.
  8. Objednatel tímto informuje Dodavatele, že vzhledem k předmětu a účelu této Smlouvy předpokládá uzavírání zejména dvou základních typů Dílčích smluv na základě této Smlouvy, a to:
     1. Dílčích smluv tzv. „Ad-hoc“ charakteru, kdy budou členové Realizačního týmu poskytovat pro Objednatele Plnění dle aktuálních a operativních potřeb Objednatele. Tato forma Dílčí smlouvy bude mít stanoven maximální finanční rámec, který nebude možno přesáhnout, a celková Cena dle této Dílčí smlouvy bude placena po částech každý měsíc zpětně na základě společného výkazu práce Realizačního týmu podepsaného zástupcem Objednatele (dále jen „**Výkaz práce**“).
     2. Dílčích smluv, kdy budou členové Realizačního týmu poskytovat pro Objednatele Plnění v podobě předem specifikovaných úkolů a výstupů s jasně definovanými akceptačními kritérii. U těchto Dílčích smluv bude stanoven fixní počet člověkohodin / MD pro jednotlivé role v rámci Realizačního týmu pro Plnění dle konkrétní Dílčí smlouvy, na základě kterého bude vypočtena pevná Cena. Cena bude placena na základě akceptačního protokolu podepsaného Objednatelem (dále jen „**Akceptační protokol**“) buď průběžně, po částech na základě akceptace dílčích částí Plnění, nebo jako celek, po konečné akceptaci celého Plnění. Akceptační procedura a podrobné platební podmínky u tohoto typu Dílčích smluv budou vždy stanoveny v příslušné Objednávce, resp. konkrétní Dílčí smlouvě a mohou se odvíjet od platebních milníků určených Koncovým zákazníkem.

Tím není dotčeno právo Objednatele odchýlit se při tvorbě návrhů Dílčích smluv od výše uvedených konstrukcí dvou základních typů Dílčích smluv, avšak vždy za podmínek stanovených touto Smlouvou.

* 1. Ukončení či splnění jednotlivé Dílčí smlouvy nemá vliv na povinnost plnění dle jiné Dílčí smlouvy nebo této Smlouvy.

### Termín, místo a podmínky plnění, akceptační řízení

* 1. Místem plnění je Česká republika. Konkrétní místo a termín plnění budou stanoveny v Dílčí smlouvě. Termín a místo plnění lze po uzavření Dílčí smlouvy změnit jen s výslovným a předchozím souhlasem Smluvních stran.
  2. Dodavatel se zavazuje realizovat jakékoliv Plnění z rámce sjednaného touto Smlouvou a požadovaného Objednatelem na základě Dílčí smlouvy v souladu s touto Smlouvou, pokud bude odpovídat účelu této Smlouvy a nebudou dány důvody pro odmítnutí poskytnutí takového Plnění. Dodavatel se zavazuje poskytnout Objednateli Plnění v souladu s časovým harmonogramem či ve lhůtě uvedené v Dílčí smlouvě.
  3. Dodavatel se zavazuje alokovat na poskytování Služeb dle této Smlouvy kapacity osob s kompetencemi dostatečnými k poskytování Služeb, a to ve struktuře, rozsahu a s odborností minimálně na úrovni požadované Objednatelem pro realizační tým v zadávací dokumentaci v rámci Zadávacího řízení (dále jen **„Zadávací dokumentace“**) (realizační tým dle této věty dále jako **„Realizační tým“**). Dodavatel je povinen zajistit kontinuitu svých osob podílejících se na plnění dle této Smlouvy dle předchozí věty v celém průběhu plnění předmětu Smlouvy. Složení a požadavky na Realizační tým jsou uvedeny v Příloze č. 4 této Smlouvy.

V případě, kdy některá z osob tvořících Realizační tým Dodavatele pro poskytování plnění dle této Smlouvy není schopna se z jakéhokoliv důvodu podílet na poskytování takového plnění, musí Dodavatel o takové situaci neprodleně písemně informovat Objednatele a zajistit náhradní osobu, která bude splňovat podmínky pro danou roli, kterou bude při poskytování plnění zastávat, stanovené v Zadávací dokumentaci, a to nejpozději do deseti (10) pracovních dnů ode dne, kdy daná osoba není schopna se podílet na poskytování plnění dle této Smlouvy, pokud nebude Objednatelem stanovena jiná lhůta.

Objednatel si vyhrazuje právo písemně požádat Dodavatele o výměnu člena Realizačního týmu pro opakovanou nespokojenost s kvalitou jím odváděné práce nebo pro nedostatečnou komunikaci s Objednatelem. Pokud Objednatel požádá o výměnu člena Realizačního týmu, není Dodavatel oprávněn plnit prostřednictvím osoby, o jejíž výměnu Objednatel požádal, své závazky.

Bude-li ze závažných důvodů vzniklých na straně Dodavatele nutné nahradit kteréhokoliv člena Realizačního týmu nebo využije-li Objednatel svého práva požádat Dodavatele o výměnu člena Realizačního týmu, bude po předchozím schválení Objednatelem nahrazen novým členem Realizačního týmu, a to do deseti

(10) pracovních dnů od oznámení důvodů pro nahrazení Objednateli / doručení žádosti o výměnu člena Realizačního týmu Dodavateli. Tento nový člen Realizačního týmu musí splňovat kvalifikační předpoklady stanovené v Zadávacím řízení a zároveň jeho zkušenosti musí být minimálně v takovém rozsahu, v jakém byly započteny do hodnocení nabídek v Zadávacím řízení u člena Realizačního týmu, kterého nahrazuje, byla-li kvalifikace či některá její část předmětem hodnocení.

Smluvní strany pro vyloučení případných pochybností sjednávají, že v případě nahrazení člena Realizačního týmu novým členem není nutné k této Smlouvě uzavírat dodatek.

Dodavatel je dále povinen zajistit, aby nový člen Realizačního týmu byl řádně a prokazatelně proškolen v oblasti bezpečnosti dat a informací. Dodavatel je povinen splnění povinnosti dle předchozí věty doložit před schválením této změny Objednatelem, a to stejnou formou, jaká byla vyžadována v Zadávacím řízení.

* 1. Dodavatel není oprávněn postoupit ani převést jakákoliv svá práva či povinnosti vyplývající ze Smlouvy bez předchozího písemného souhlasu Objednatele na třetí osoby. Dodavatel je oprávněn pověřit plněním závazků plynoucích ze Smlouvy jiné třetí osoby (poddodavatele), nebo takové třetí osoby (poddodavatele) změnit, uvedl-li je již ve své nabídce v Zadávacím řízení, pouze s předchozím písemným souhlasem Objednatele. Pokud se jedná o takové třetí osoby (poddodavatele), kterými Dodavatel prokazoval kvalifikaci, tak musí tato nová třetí osoba (poddodavatel) splňovat kvalifikační předpoklady minimálně v rozsahu stanoveném v Zadávacím řízení. Pokud byla tato třetí osoba (poddodavatel) taktéž součástí hodnocení nabídek v Zadávacím řízení, tak musí taktéž splňovat kvalifikační předpoklady minimálně v takovém rozsahu, v jakém byly započteny do tohoto hodnocení nabídek v Zadávacím řízení u původní třetí osoby (poddodavatele). Dodavatel je povinen splnění náležitostí dle předchozí věty doložit před odsouhlasením této změny Objednatelem, a to stejnou formou, jaká byla vyžadována v Zadávacím řízení. Udělí-li Objednatel s využitím nebo změnou třetí osoby (poddodavatele) souhlas, je Dodavatel povinen zavázat poddodavatele k zachování důvěrných informací a k ochraně osobních údajů ve smyslu čl. [11](#_bookmark21) této Smlouvy a k zajištění bezpečnostních požadavků zejména ve smyslu čl. [14](#_bookmark28) této Smlouvy ve stejném rozsahu, v jakém je k této povinnosti zavázán sám. Dodavatel odpovídá za své poddodavatele jako za plnění vlastní, včetně odpovědnosti za způsobenou újmu. Dodavatel se zavazuje neprodleně doložit Objednateli na základě jeho výzvy smluvní dokumenty se svými poddodavateli, ze kterých bude vyplývat závazek poddodavatele poskytovat plnění v souladu s požadavky na ochranu důvěrných informací a osobních údajů a bezpečnostními požadavky vyplývajícími z této Smlouvy.
  2. Dodavatel je povinen zajistit, že i jeho poddodavatelé, kteří se budou podílet na plnění této Smlouvy, se zaváží dodržovat v plném rozsahu ujednání mezi Dodavatelem a Objednatelem a nebudou v rozporu s požadavky Objednatele uvedenými v této Smlouvě.
  3. Dodavatel je povinen po celou dobu účinnosti této Smlouvy garantovat, že v každém okamžiku v průběhu účinnosti Smlouvy disponuje minimální kapacitou osob ve vybraných rolích blíže specifikovanou v Příloze č. 5 této Smlouvy.
  4. Objednatel může Dodavatele, resp. členy Realizačního týmu vyzvat k poskytování Plnění dle Dílčí smlouvy prostřednictvím e-mailu nebo telefonicky. Tato výzva k poskytování Plnění dle Dílčí smlouvy musí obsahovat termín či termíny požadované Objednatelem pro poskytování daného Plnění dle Dílčí smlouvy.
  5. Příslušný člen či členové Realizačního týmu musí reagovat na výzvu k poskytování Plnění dle odst. [3.7](#_bookmark9) tohoto článku Dílčí smlouvy nejpozději následující pracovní den po jejím předání Objednatelem, nedohodnou-li se Smluvní strany jinak (dále jen „**reakční**

**doba**“). V závažných případech může Objednatel po domluvě s Dodavatelem požadovat kratší reakční dobu.

* 1. Dodavatel (členové Realizačního týmu) se v souvislosti s realizací Plnění dle Dílčí smlouvy zavazuje poskytovat Objednateli Plnění s dostupností 5x8, tzn. 8 hodin denně v čase od 8:00 do 16:00 během pracovních dnů, případně dle dohody s Objednatelem. V případě nutnosti může být Objednatelem požadována po Dodavateli běžná dostupnost a/nebo pohotovost i mimo časový úsek uvedený v předchozí větě tohoto odstavce a/nebo o víkendech.
  2. Objednatel tímto sděluje Dodavateli a Dodavatel podpisem této Smlouvy souhlasí s tím, že příjemcem Služeb poskytnutých na základě této Smlouvy může být kromě Objednatele také Koncový zákazník.

#### Akceptační procedura k Plnění dle čl. [1](#_bookmark0) odst. [1.3](#_bookmark1) této Smlouvy u typu Dílčích smluv „Ad- hoc“ charakteru dle čl. [2](#_bookmark3) odst. 2.15 písm. [a)](#_bookmark5) této Smlouvy

* 1. Poskytování Plnění dle čl. [1](#_bookmark0) odst. [1.3](#_bookmark1) této Smlouvy u typu Dílčích smluv „Ad-hoc“ charakteru dle čl. [2](#_bookmark3) odst. 2.15 písm. [a)](#_bookmark5) této Smlouvy v rozsahu a za podmínek stanovených příslušnou Dílčí smlouvou, bude potvrzeno formou Výkazu práce, kterým se rozumí měsíční výkaz o poskytování Plnění zpracovaný Dodavatelem, tj. výkaz činnosti a odpracovaných hodin členů Realizačního týmu v jednotlivých rolích poskytnutých Dodavatelem.
  2. Výkaz práce bude Dodavatelem předložen kontaktní osobě Objednatele uvedené ve Smlouvě k odsouhlasení nejpozději třetí (3.) pracovní den po ukončení každého kalendářního měsíce, v němž bylo Plnění poskytováno. Objednatel potvrdí poskytnutí Plnění podpisem Výkazu práce, pokud bylo Plnění realizováno ve sjednaném rozsahu a kvalitě a údaje ve Výkazu práce odpovídají skutečně poskytnutému Plnění. Podpis Výkazu práce Objednatelem může být podmíněn předchozí akceptací Plnění Koncovým zákazníkem. Objednatel je oprávněn odmítnout potvrzení poskytnutí Plnění, pokud má za to, že údaje ve Výkazu práce neodpovídají skutečně poskytnutému Plnění. Odmítnutí potvrzení bude zachyceno ve Výkazu práce, přičemž Objednatel se zavazuje poskytnout Dodavateli potřebnou součinnost pro odstranění zjištěných nesrovnalostí.

#### Akceptační procedura k Plnění dle čl. [1](#_bookmark0) odst. [1.3](#_bookmark1) této Smlouvy u typu Dílčích smluv dle čl. [2](#_bookmark3) odst. 2.15 písm. [b)](#_bookmark6) této Smlouvy

* 1. Akceptační procedura u Plnění dle čl. [1](#_bookmark0) odst. [1.3](#_bookmark1) této Smlouvy u typu Dílčích smluv dle čl. [2](#_bookmark3) odst. 2.15 písm. [b)](#_bookmark6) této Smlouvy v rozsahu a za podmínek stanovených příslušnou Dílčí smlouvou zahrnuje ověření řádného provedení Plnění porovnáním skutečných vlastností Plnění s jeho specifikací stanovenou příslušnou Dílčí smlouvou. Akceptační

kritéria pro dané Plnění budou stanovena příslušnou Objednávkou, resp. Dílčí smlouvou. Řízení o akceptaci je zahájeno dnem předání Plnění Dodavatelem do akceptačního řízení a je ukončeno podpisem Akceptačního protokolu oběma Smluvními stranami. Akceptační protokol bude povinně obsahovat podrobný report činností poskytnutých členy Realizačního týmu v jednotlivých rolích, počet člověkohodin / MD poskytnutých Služeb v jednotlivých rolích, obsah a rozsah poskytnutých Služeb, závěry a výstupy z poskytnutých Služeb, popř. doporučení Dodavatele pro další postup Objednatele, přičemž k Akceptačnímu protokolu budou případně přiloženy dokumenty požadované Objednatelem.

* 1. Akceptační protokol bude Dodavatelem předložen kontaktní osobě Objednatele uvedené ve Smlouvě k odsouhlasení nejpozději pátý (5.) pracovní den po ukončení poskytování Plnění dle příslušné Dílčí smlouvy, pokud nebude v dané Dílčí smlouvě stanoveno jinak. Objednatel potvrdí poskytnutí Plnění podpisem Akceptačního protokolu, pokud bylo Plnění realizováno ve sjednaném rozsahu a kvalitě a údaje v Akceptačním protokolu odpovídají skutečně poskytnutému Plnění. Podpis Akceptačního protokolu Objednatelem může být podmíněn předchozí akceptací Plnění Koncovým zákazníkem.
  2. Objednatel je oprávněn odmítnout Akceptační protokol dle odst. [3.13](#_bookmark11) a [3.14](#_bookmark12) tohoto článku Smlouvy, pokud vykazované Plnění nebylo poskytnuto řádně v souladu s touto Smlouvou nebo Dílčí smlouvou nebo ve sjednané kvalitě nebo pokud případný písemný výstup neobsahoval veškeré údaje požadované Objednatelem nebo Objednatel nesouhlasí s počtem člověkohodin / MD poskytnutých Služeb, které budou Objednateli účtovány, přičemž v takovém případě Objednatel důvody odmítnutí převzetí Akceptačního protokolu písemně Dodavateli sdělí, a to nejpozději do pěti (5) pracovních dnů od termínu předání Akceptačního protokolu. Na následné předání Akceptačního protokolu se použijí výše uvedená ustanovení tohoto odstavce.
  3. Pokud Objednatel uplatní písemný nárok na odstranění vad uvedených v odst. [3.15](#_bookmark13) tohoto článku Smlouvy, zavazuje se Dodavatel tyto vady odstranit bez zbytečného odkladu, nejpozději však do pěti (5) pracovních dnů, nestanoví-li Objednatel lhůtu delší.
  4. Dodavatel je Objednateli povinen předat veškeré další případné dokumenty nezbytné pro řádné provedení Plnění (dále jen **„Dokumentace“**). Nestanoví-li Dílčí smlouva jinak, bude nedílnou součástí Výkazu práce / Akceptačního protokolu, následující Dokumentace:
     1. veškerá dokumentace vztahující se k předmětnému Plnění, zejména veškeré návody (manuály) k použití, doklady a dokumenty, jež jsou obvyklé, nutné (právními předpisy vyžadované) či vhodné k převzetí a k využití Plnění, uživatelská dokumentace, provozní dokumentace, bezpečnostní příručka, administrátorská dokumentace atp. Veškeré návody (manuály) k použití,

záruční listy, funkční specifikace, doklady a dokumenty budou v českém jazyce. Objednatel s ohledem na Plnění připouští po předchozí vzájemné domluvě obou Smluvních stran také dodání uvedených dokumentů v anglickém jazyce vyjma licenčních podmínek, které budou vždy dodávány výhradně v českém jazyce;

* + 1. vždy aktuální verzi zdrojových kódů včetně aktuálních verzí veškeré související dokumentace, bude-li Dodavatel povinen tyto zdrojové kódy a související dokumentaci v souladu s touto Smlouvou a Dílčí smlouvou poskytnout;
    2. jakékoli další materiály vztahující se k předmětnému Plnění.

Dokumentace předaná současně s Plněním do akceptačního řízení podléhá rovněž akceptačnímu řízení. Veškerá Dokumentace se stává výlučným vlastnictvím Objednatele dnem podpisu Výkazu práce / Akceptačního protokolu.

* 1. V případě, že Objednatel bude požadovat v rámci akceptačního řízení výstup v podobě písemného dokumentu, bude tento výstup předán Dodavatelem Objednateli v českém jazyce, a to tak, že Dodavatel jej předá Objednateli spolu s Výkazem práce / Akceptačním protokole v listinné formě vytištěné a podepsané ve dvou (2) originálech nebo v elektronické formě ve formátu Microsoft Word nebo v případě obrazových výstupů ve formátu PDF (Portable Document Format) nebo v běžně používaných grafických formátech (BMP, JPG, GIF) na nosiči dat, CD nebo DVD.
  2. Místem předání všech akceptačních dokumentů uvedených tomto článku Smlouvy je kontaktní adresa Objednatele, tj. Kodaňská 1441/46, Vršovice, 101 00 Praha 10, pokud nebude Objednatelem stanoveno jinak.
  3. Podpisem Výkazu práce / Akceptačního protokolu Objednatelem se má za to, že je částečně splněn závazek Dodavatele dle této Smlouvy provést Plnění a Dodavateli vzniká právo na zaplacení příslušné ceny za Plnění. Výkaz práce / Akceptační protokol budou vyhotovovány ve dvou (2) vyhotoveních a podepsány oběma Smluvními stranami. Každá ze Smluvních stran obdrží po jednom (1) vyhotovení.
  4. Smluvní strany sjednávají, že k podpisu všech akceptačních dokumentů uvedených v tomto článku Smlouvy jsou oprávněny osoby uvedené v čl. [8](#_bookmark19) této Smlouvy.
  5. Vzory Výkazu práce a Akceptačního protokolu jsou uvedeny v Příloze č. 3 této Smlouvy.

### Cena

* 1. Cena za poskytnutí Plnění dle konkrétní Dílčí smlouvy je tvořena součtem jednotkových cen bez DPH dle Přílohy č. 2 této Smlouvy za všechny člověkohodiny / MD v jednotlivých rolích dle Přílohy č. 4 této Smlouvy poskytnuté Dodavatelem Objednateli na základě dané Dílčí smlouvy (dále jen „**Cena**“).
  2. Jednotkové ceny pro jednotlivé role jsou uvedeny v Příloze č. 2 této Smlouvy a vycházejí z jednotkových cen uvedených v nabídce Dodavatele v rámci Zadávacího řízení. Jednotkové ceny jsou konečné a nejvýše přípustné a jsou v nich zahrnuty veškeré náklady Dodavatele související s plněním Smlouvy, Dílčí smlouvy a poskytnutím Plnění Objednateli. Dodavatel tímto Objednateli zaručuje úplnost cen plnění uvedených v Příloze č. 2 této Smlouvy.
  3. Veškeré ceny jsou uvedeny v Kč bez DPH. K Ceně bude připočítána DPH dle příslušných předpisů ve výši platné ke dni uskutečnění zdanitelného plnění.
  4. Celková cena za Předmět plnění poskytnutý na základě této Smlouvy nesmí převýšit částku 8 000 000,- Kč (slovy: osm milionů korun českých) bez DPH.
  5. Jedním člověkodnem (**MD**) se pro účely této Smlouvy rozumí součet osmi (8) člověkohodin odborných Služeb, které nemusí být poskytovány ve stejný den. Členové Realizačního týmu budou evidovat svoji práci s přesností na dokončenou půlhodinu.

### Platební podmínky

* 1. Cena (či její část) za Plnění poskytnuté na základě příslušné Dílčí smlouvy bude Objednatelem uhrazena na základě daňového dokladu (faktury) vystaveného Dodavatelem. Plněním se rozumí zdanitelné plnění, které se uskutečňuje v rozsahu a lhůtách sjednaných v Dílčí smlouvě. Plnění či jeho část se považuje za uskutečněné dnem podpisu Výkazu práce a/nebo Akceptačního protokolu oběma Smluvními stranami.
  2. Daňové doklady (faktury) za řádně realizované Plnění budou v případě typu Dílčích smluv dle čl. [2](#_bookmark3) odst. 2.15 písm. [a)](#_bookmark5) této Smlouvy či Dílčích smluv obdobného charakteru vystavovány měsíčně vždy po skončení příslušného kalendářního měsíce a budou v nich vyúčtovány Služby převzaté Objednatelem bez jakýchkoliv vad za předchozí kalendářní měsíc. Nedílnou součástí každého daňového dokladu bude Výkaz práce za příslušný měsíc podepsaný kontaktními osobami obou Smluvních stran dle čl. [8](#_bookmark19) této Smlouvy, případně osobou určenou příslušnou Dílčí smlouvou. Za den uskutečnění zdanitelného plnění se v tomto případě považuje den podpisu Výkazu práce Objednatelem.
  3. Daňové doklady (faktury) za řádně realizované Plnění budou v případě typu Dílčích smluv dle čl. [2](#_bookmark3) odst. 2.15 písm. b) této Smlouvy či Dílčích smluv obdobného charakteru vystavovány po akceptaci realizovaného Plnění či jeho části Objednatelem. Nedílnou součástí každého daňového dokladu bude Akceptační protokol podepsaný kontaktními osobami obou Smluvních stran dle čl. [8](#_bookmark19) této Smlouvy, případně osobou určenou příslušnou Dílčí smlouvou. Za den uskutečnění zdanitelného plnění se v tomto případě považuje den podpisu Akceptačního protokolu Objednatelem.
  4. Dodavatel je povinen, nebude-li Dílčí smlouvou stanoveno jinak, vystavit příslušný daňový doklad nejpozději do pěti (5) pracovních dnů po podpisu Výkazu práce a/nebo Akceptačního protokolu Objednatelem.
  5. Daňový doklad (faktura) vystavený Dodavatelem musí obsahovat náležitosti daňového dokladu podle příslušných právních předpisů, zejména pak § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „**Zákon o DPH**“), zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů a zejména tyto údaje:
     1. číslo Smlouvy;
     2. číslo Dílčí smlouvy a číslo objednávky;
     3. identifikační údaje Objednatele a Dodavatele
     4. místo a dobu poskytnutí Plnění;
     5. platební podmínky v souladu se Smlouvou a Dílčí smlouvou;
     6. popis fakturovaného Plnění, množství, jednotkovou cenu a celkovou Cenu.

Přílohou daňového dokladu bude kopie oběma Smluvními stranami podepsaného Výkazu práce / Akceptačního protokolu.

* 1. V případě, že daňový doklad nebude mít odpovídající náležitosti nebo nebude vystaven v souladu s touto Smlouvou nebo nebude obsahovat kopii oběma Smluvními stranami podepsaný Výkaz práce / Akceptační protokol, je Objednatel oprávněn zaslat jej ve lhůtě splatnosti zpět k doplnění Dodavateli, aniž se dostane do prodlení se splatností; lhůta splatnosti 30 (třicet) kalendářních dnů se tímto přerušuje a nová lhůta splatnosti v délce 30 (třiceti) kalendářních dnů počne plynout od data doručení nově vystaveného/opraveného daňového dokladu Objednateli.
  2. Daňové doklady budou zasílány Dodavatelem spolu s veškerými požadovanými dokumenty Objednateli do tří (3) pracovních dnů od jejich vystavení následujícími způsoby:
     1. v elektronické podobě na adresu: [faktury@nakit.cz](mailto:faktury@nakit.cz)
     2. doporučeným dopisem na následující adresu:

Národní agentura pro komunikační a informační technologie, s. p. Kodaňská 1441/46, Vršovice, 101 01 Praha10

* 1. Platba bude provedena v české měně formou bankovního převodu na účet Dodavatele uvedený v záhlaví této Smlouvy.
  2. Faktura se považuje za uhrazenou dnem odepsání příslušné finanční částky z účtu Objednatele ve prospěch účtu Dodavatele.
  3. Doba splatnosti daňového dokladu vystaveného na základě této Smlouvy je 30 (třicet) kalendářních dnů ode dne jeho doručení Objednateli.
  4. Objednatel neposkytuje Dodavateli jakékoliv zálohy na cenu.
  5. Smluvní strany se dohodly, že pokud bude v okamžiku uskutečnění zdanitelného plnění správcem daně zveřejněna způsobem umožňujícím dálkový přístup skutečnost, že dodavatel zdanitelného plnění (dále též „Dodavatel“) je nespolehlivým plátcem ve smyslu ust. § 106a Zákona o DPH, nebo má-li být platba za zdanitelné plnění uskutečněné Dodavatelem v tuzemsku zcela nebo z části poukázána na bankovní účet vedený poskytovatelem platebních služeb mimo tuzemsko, je příjemce zdanitelného plnění (dále též „Objednatel“) oprávněn část ceny odpovídající dani z přidané hodnoty zaplatit přímo na bankovní účet správce daně ve smyslu ust. § 109a Zákona o DPH. Na bankovní účet Dodavatele bude v tomto případě uhrazena část ceny odpovídající výši základu daně z přidané hodnoty. Úhrada ceny plnění (základu daně) provedená Objednatelem v souladu s ustanovením tohoto odstavce bude považována za řádnou úhradu ceny plnění poskytnutého dle Smlouvy.

Bankovní účet uvedený na daňovém dokladu, na který bude ze strany Dodavatele požadována úhrada ceny za poskytnuté zdanitelné plnění, musí být Dodavatelem zveřejněn způsobem umožňujícím dálkový přístup ve smyslu ust. § 96 Zákona o DPH. Smluvní strany se výslovně dohodly, že pokud číslo bankovního účtu Dodavatele, na který bude ze strany Dodavatele požadována úhrada ceny za poskytnuté zdanitelné plnění dle příslušného daňového dokladu, nebude zveřejněno způsobem umožňujícím dálkový přístup ve smyslu ust. § 96 Zákona o DPH a cena za poskytnuté zdanitelné plnění dle příslušného daňového dokladu přesahuje limit uvedený v ust. § 109 odst. 2 písm. c) Zákona o DPH, je Objednatel oprávněn zaslat daňový doklad zpět Dodavateli k opravě. V takovém případě se doba splatnosti zastavuje a nová doba splatnosti počíná běžet dnem doručení opraveného daňového dokladu Objednateli s uvedením správného bankovního účtu Dodavatele, tj. bankovního účtu zveřejněného správcem daně,

### Pojištění

* 1. Dodavatel se zavazuje mít po celou dobu účinnosti Smlouvy uzavřenou platnou a účinnou pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou Dodavatelem třetí osobě s limitem pojistného plnění, který nesmí být nižší než 20 000 000,- Kč (slovy: dvacet milionů korun českých). V případě, že plněním této Smlouvy dojde ke způsobení škody Objednateli nebo třetím osobám, která nebude kryta pojištěním sjednaným ve smyslu tohoto odstavce Smlouvy, bude Dodavatel povinen tyto škody uhradit z vlastních prostředků.
  2. Dodavatel se zavazuje, po předchozí písemné žádosti Objednatele, předložit nejpozději do sedmi (7) kalendářních dnů k nahlédnutí Objednateli platnou a účinnou

pojistnou smlouvu, a to i opakovaně. Bude-li zjištěno, že Dodavatel nedisponuje účinnou pojistnou smlouvou, jedná se o podstatné porušení Smlouvy a Objednatel je od této Smlouvy oprávněn odstoupit.

### Sankce

* 1. V případě prodlení Dodavatele se zahájením poskytování Plnění dle čl. [3](#_bookmark7) odst. [3.8](#_bookmark10) této Smlouvy z důvodů ležících na straně Dodavatele, je Objednatel oprávněn vyúčtovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 0,3 % z Ceny Plnění dle příslušné Dílčí smlouvy, a to za každý započatý den prodlení, maximálně však do výše Ceny za Plnění dle Dílčí smlouvy bez DPH. Tuto smluvní pokutu není povinen Dodavatel uhradit v případě, že důvodem neposkytnutí včasného Plnění dle Dílčí smlouvy jsou lékařem potvrzené zdravotní důvody, případně vyšší moc.
  2. V případě, že Dodavatel je v prodlení s poskytnutím Plnění dle příslušné Dílčí smlouvy, je Objednatel oprávněn vyúčtovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 0,3 % z Ceny Plnění dle příslušné Dílčí smlouvy, a to za každý započatý den prodlení.
  3. V případě porušení prohlášení Dodavatele dle čl. [1](#_bookmark0) odst. [1.4](#_bookmark2) této Smlouvy, je Objednatel oprávněn vyúčtovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 250 000,- Kč (slovy: dvě stě padesát tisíc korun českých) za každé jednotlivé porušení.
  4. V případě porušení povinností Dodavatele plynoucích z čl. [6](#_bookmark18) této Smlouvy, je Objednatel oprávněn vyúčtovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 100 000,- Kč (slovy: jedno sto tisíc korun českých) za každé jednotlivé porušení.
  5. V každém jednotlivém případě porušení povinností Dodavatele vyplývajících z ustanovení čl. [10](#_bookmark20) této Smlouvy, je Objednatel oprávněn vyúčtovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 50 000,- Kč (slovy: padesát tisíc korun českých).
  6. V každém jednotlivém případě porušení povinností Dodavatele vyplývajících z ustanovení čl. [11](#_bookmark21) této Smlouvy, je Objednatel oprávněn vyúčtovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 250 000,- Kč (slovy: dvě stě padesát tisíc korun českých).
  7. V případě prodlení Dodavatele s poskytnutím dokumentů či informací dle požadavků Objednatele v rámci exitové součinnosti dle čl. [12](#_bookmark22) odst. [12.10](#_bookmark24) této Smlouvy, je Objednatel oprávněn vyúčtovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 50 000,- Kč (slovy: padesát tisíc korun českých) za každý i započatý den takového prodlení.
  8. V případě, že Dodavatel bude k poskytování Plnění využívat poddodavatele nebo členy Realizačního týmu v rozporu se Smlouvou nebo příslušnou Dílčí smlouvou, je Objednatel oprávněn vyúčtovat a Dodavatel povinen zaplatit smluvní pokutu ve výši

50 000,- Kč (slovy: padesát tisíc korun českých) za každý jednotlivý případ takového porušení této Smlouvy.

* 1. V případě, že Dodavatel prokazatelně poruší své povinnosti uvedené v čl. [3](#_bookmark7) odst. 3.3 až [3.6](#_bookmark8) této Smlouvy, je Objednatel oprávněn vyúčtovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 50 000,- Kč (slovy: padesát tisíc korun českých) za každý i započatý den porušování těchto smluvních povinností.
  2. V případě, že se prohlášení Dodavatele obsažené v čl. [13](#_bookmark25) odst. [13.11](#_bookmark26) a/nebo [13.12](#_bookmark27) této Smlouvy ukáže jako nepravdivé, je Objednatel oprávněn vyúčtovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 5 000 000,- Kč (slovy: pět milionů korun českých).
  3. V případě, že Dodavatel prokazatelně poruší své povinnosti uvedené v čl. [13](#_bookmark25) odst. 13.2 a/nebo 13.4 této Smlouvy, a poskytne výhradní licenci ve smyslu čl. [13](#_bookmark25) této Smlouvy třetí straně, je Objednatel oprávněn vyúčtovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 5 000 000,- Kč (slovy: pět milionů korun českých) za každý jednotlivý případ takového porušení této Smlouvy.
  4. V případě nedodržení či porušení povinností Dodavatele vyplývajících ze ZoKB a VyKB (jak jsou tyto pojmy definované v čl. 14 této Smlouvy) a uvedených v čl. [14](#_bookmark28) této Smlouvy, je Objednatel oprávněn vyúčtovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 250 000,- Kč (slovy: dvě stě padesát tisíc korun českých) za každý jednotlivý případ porušení těchto povinností.
  5. V případě, že Dodavatel podstatným způsobem poruší svoji povinnost postupovat při plnění této Smlouvy v souladu s interními dokumenty Objednatele, se kterými byl seznámen, je Objednatel oprávněn vyúčtovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 50 000,- Kč (slovy: padesát tisíc korun českých) za každé jednotlivé porušení této povinnosti.
  6. Bude-li Objednatel v prodlení s úhradou daňového dokladu (faktury), má Dodavatel právo žádat na Objednateli úrok z prodlení v souladu s nařízením vlády č. 351/2013 Sb., kterým se určuje výše úroků z prodlení a nákladů spojených s uplatněním pohledávky, určuje odměna likvidátora, likvidačního správce a člena orgánu právnické osoby jmenovaného soudem a upravují některé otázky Obchodního věstníku a veřejných rejstříků právnických a fyzických osob, ve znění pozdějších předpisů.
  7. Uplatněním a zaplacením jakékoli smluvní pokuty není dotčeno právo Objednatele na náhradu vzniklé škody a ušlý zisk v celém rozsahu způsobené újmy. Výše smluvních pokut se do výše náhrady újmy nezapočítává.
  8. Vyúčtování smluvní pokuty / úroků z prodlení podle příslušných ustanovení této Smlouvy – penalizační faktura, musí být druhé Smluvní straně zasláno prokazatelným způsobem. Smluvní pokuta / úroky z prodlení jsou splatné ve lhůtě třiceti (30) kalendářních dnů ode dne doručení penalizační faktury. Úhrada smluvní pokuty / úroků

z prodlení se provádí bankovním převodem na účet oprávněné Smluvní strany uvedený v penalizační faktuře. Částka se považuje za zaplacenou okamžikem jejího připsání ve prospěch účtu oprávněné Smluvní strany.

* 1. Objednatel je v případě uplatnění smluvní pokuty vůči Dodavateli dle této Smlouvy a v případě neuhrazení smluvní pokuty ze strany Dodavatele oprávněn využít institut započtení vzájemných pohledávek.
  2. Není-li stanoveno jinak, zaplacení jakékoliv sjednané smluvní pokuty nezbavuje povinnou Smluvní stranu povinnosti splnit své závazky.

### Odpovědné osoby

* 1. Odpovědnými osobami Dodavatele a Objednatele ve věcech smluvních a obchodních pro účely této Smlouvy jsou:

Za Objednatele:

xxx

Za Dodavatele:

xxx

* 1. Odpovědnými osobami Dodavatele a Objednatele ve věcech technických pro účely této Smlouvy jsou:

Za Objednatele:

xxx

Za Dodavatele:

xxx

* 1. Bude-li z důvodů vzniklých na straně Dodavatele nutné nahradit kteroukoli odpovědnou osobu na straně Dodavatele ve věcech technických, bude tato osoba po předchozím projednání s Objednatelem nahrazena novou odpovědnou osobou s odpovídající nebo vyšší kvalifikací, a to do deseti (10) dní od oznámení důvodů pro nahrazení Objednateli. Objednatel je oprávněn jednostranně změnit odpovědnou osobu ve věcech technických, přičemž změna je účinná doručením písemného oznámení o takové změně Dodavateli. V případě změny odpovědné osoby podle tohoto odstavce Smlouvy není nutné k této Smlouvě uzavírat dodatek.
  2. Obě Smluvní strany jsou oprávněny jednostranně změnit odpovědné osoby ve věcech smluvních a obchodních bez nutnosti uzavření dodatku ke Smlouvě, přičemž změna je účinná doručením písemného oznámení o takové změně druhé Smluvní straně.

### Nemožnost plnění, náhrada újmy a vyšší moc

* 1. Jestliže vznikne na straně Dodavatele nemožnost plnění dle ustanovení § 2006 a § 2007 občanského zákoníku, Dodavatel písemně uvědomí bez zbytečného odkladu o této skutečnosti a její příčině Objednatele. Pokud není jinak stanoveno písemně Objednatelem, bude Dodavatel pokračovat v realizaci svých povinností vyplývajících ze smluvního vztahu v rozsahu svých nejlepších možností a schopností a bude hledat alternativní prostředky pro realizaci té části plnění, kde není možné plnit. Pokud by podmínky nemožnosti plnění trvaly déle než třicet (30) kalendářních dní, je Objednatel oprávněn od Smlouvy odstoupit.
  2. Každá ze Smluvních stran nese odpovědnost za způsobenou újmu v rámci platných právních předpisů a této Smlouvy. Obě Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.
  3. Žádná ze Smluvních stran neodpovídá za újmu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé Smluvní strany. V případě, že Objednatel poskytl Dodavateli chybné zadání a Dodavatel s ohledem na svou povinnost poskytovat plnění s odbornou péčí mohl a měl chybnost takového zadání zjistit, smí se ustanovení předchozí věty dovolávat pouze v případě, že na chybné zadání Objednatele písemně upozornil a Objednatel trval na původním zadání.
  4. Žádná ze Smluvních stran není odpovědná za újmu a není ani v prodlení, pokud k tomuto došlo výlučně v důsledku prodlení s plněním závazků druhé Smluvní strany nebo v důsledku překážek vylučujících povinnost k náhradě újmy ve smyslu § 2913 odst. 2 občanského zákoníku (dále jen „**vyšší moc**“).
  5. Za vyšší moc se podle této Smlouvy považují mimořádné nepředvídatelné a nepřekonatelné překážky bránící dočasně nebo trvale plnění povinností stanovených v této Smlouvě, pokud nastaly po jejím uzavření nezávisle na vůli povinné Smluvní

strany a jestliže tyto překážky nemohly být povinnou Smluvní stranou odvráceny ani při vynaložení veškerého úsilí, které lze rozumně v dané situaci požadovat.

* 1. Za vyšší moc se však nepokládají okolnosti, jež vyplývají z osobních nebo hospodářských poměrů povinné Smluvní strany a dále překážky plnění, které byla příslušná Smluvní strana povinna překonat nebo odstranit podle této Smlouvy, obchodních zvyklostí nebo obecně závazných právních předpisů nebo jestliže může důsledky své odpovědnosti smluvně převést na třetí osobu, jakož i okolnosti, které se projevily až v době, kdy povinná Smluvní strana již byla v prodlení.
  2. Smluvní strany se zavazují upozornit druhou Smluvní stranu bez zbytečného odkladu na vzniklé překážky vylučující povinnost k náhradě újmy. Zpráva musí být podána písemně, neprodleně poté, kdy se povinná Smluvní strana o překážce dozvěděla, nebo při náležité péči mohla dozvědět. Bezprostředně po zániku takové překážky povinná Smluvní strana obnoví plnění svých závazků vůči druhé Smluvní straně a učiní vše, co je v jejích silách, ke kompenzaci doby, která uplynula v důsledku takového prodlení. Pokud překážka nepomine do tří (3) pracovních dnů od doby svého vzniku, je Objednatel oprávněn od Smlouvy odstoupit. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání překážek vylučujících povinnost k náhradě újmy.
  3. Každá ze Smluvních stran je oprávněna požadovat náhradu újmy v plném rozsahu i v případě, že se jedná o porušení povinnosti, na kterou se dle této Smlouvy vztahuje smluvní pokuta.
  4. Případná náhrada újmy bude zaplacena v měně platné na území České republiky, přičemž pro propočet na tuto měnu je rozhodný kurs České národní banky ke dni vzniku újmy.

### Další práva a povinnosti Smluvních stran

* 1. Veškerá komunikace mezi Smluvními stranami je činěna písemně, není-li touto Smlouvou stanoveno jinak. Písemná komunikace se činí v listinné nebo elektronické podobě prostřednictvím doporučené pošty nebo e-mailu na adresy Smluvních stran uvedené v záhlaví a v čl. [8](#_bookmark19) této Smlouvy.
  2. Objednatel se zavazuje poskytnout Dodavateli součinnost potřebnou a přiměřenou k řádnému plnění této Smlouvy a Dílčí smlouvy. Tato součinnost zahrnuje také poskytnutí veškerých potřebných informací, dokumentů a dalších podkladů nezbytných pro řádné poskytování předmětu plnění dle této Smlouvy Dodavatelem.
  3. Dodavatel se zavazuje dodržovat v objektech Objednatele a v objektech subjektů určených Objednatelem, příslušné bezpečnostní předpisy, se kterými byl Dodavatel prokazatelně seznámen. Při plnění této Smlouvy v objektech Objednatele či jím

určených subjektů musí Dodavatel v maximální míře respektovat nutnost zajištění nerušeného užívání objektů jejich uživateli.

* 1. Při poskytování Plnění je Dodavatel vázán touto Smlouvou, Dílčí smlouvou, obecně závaznými právními předpisy a pokyny Objednatele, pokud tyto nejsou v rozporu s těmito normami nebo zájmy Objednatele. Dodavatel je povinen při výkonu své činnosti včas písemně upozornit Objednatele na zřejmou nevhodnost jeho pokynů, jejichž následkem může vzniknout újma nebo nesoulad se zákony nebo obecně závaznými právními předpisy.
  2. Po celou dobu plnění dle této Smlouvy Dodavatel zodpovídá za dodržování bezpečnosti a ochrany zdraví při práci a dodržování příslušných ustanovení zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, u svých zaměstnanců. Stejně tak zodpovídá i za dodržování požární ochrany při plnění dle této Smlouvy. Dodavatel i jeho pracovníci musí respektovat kontrolní činnost Objednatele či jím určených třetích subjektů přijímáním účinných opatření bez prodlení.
  3. Dodavatel není oprávněn použít ve svých dokumentech, prezentacích či reklamě odkazy na název Objednatele nebo jakýkoliv jiný odkaz, který by mohl, byť i nepřímo vést k identifikaci Objednatele, bez předchozího písemného souhlasu Objednatele.
  4. Dodavatel je povinen pověřit plněním povinností z této Smlouvy pouze ty své zaměstnance, kteří jsou k tomu odborně způsobilí.
  5. Dodavatel odpovídá Objednateli za své případné poddodavatele jako za plnění vlastní, včetně odpovědnosti za způsobenou újmu. Veškerou koordinaci případných poddodavatelů Dodavatele zajišťuje Dodavatel, nikoli Objednatel. Pokud si Objednatel nevyžádá jinak, bude komunikace vedena pouze na úrovni Objednatel – Dodavatel, nikoli mezi Objednatelem a případnými jednotlivými poddodavateli.
  6. Dodavatel odpovídá za integritu a celistvost veškerého plnění dle této Smlouvy a Dílčích smluv.
  7. Dodavatel je povinen při plnění povinností dle této Smlouvy a Dílčí smlouvy na žádost Objednatele aktivně spolupracovat s jím určenými subjekty.
  8. Dodavatel se dále zavazuje:
     1. plnit vlastním jménem, na vlastní odpovědnost, řádně a ve stanoveném termínu své povinnosti vyplývající z této Smlouvy a Dílčí smlouvy;
     2. informovat neprodleně Objednatele o všech skutečnostech majících vliv na plnění dle této Smlouvy a Dílčí smlouvy;
     3. požádat včas Objednatele o potřebnou součinnost za účelem řádného plnění této Smlouvy a Dílčí smlouvy;
     4. na vyžádání Objednatele se zúčastnit osobní schůzky, pokud Objednatel požádá o schůzku nejpozději pět (5) pracovních dnů předem. V mimořádně naléhavých případech je možno tento termín po dohodě obou Smluvních stran zkrátit;
     5. neprodleně písemně oznámit Objednateli změny svého majetkoprávního postavení, jako je např. přeměna společnosti, snížení základního kapitálu, vstup do likvidace, úpadek či zahájení insolvenčního řízení.
  9. Dodavatel se zavazuje provést na vlastní náklady likvidaci či uložení veškerých odpadů vzniklých při plnění dle této Smlouvy.
  10. V případě, že činností, nečinností anebo opomenutím Dodavatele anebo jeho zaměstnanců vznikne Objednateli nemajetková újma, je Dodavatel povinen ji odčinit.

### Obchodní tajemství, důvěrné informace a zpracování osobních údajů

* 1. Veškeré konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních kruzích běžně nedostupné skutečnosti související se Smluvními stranami, se kterými Smluvní strany při realizaci předmětu Smlouvy nebo v souvislosti s touto Smlouvou přijdou do styku, jsou obchodním tajemstvím.
  2. Smluvní strany se zavazují, že důvěrné informace a obchodní tajemství druhé Smluvní strany jiným subjektům nesdělí, nezpřístupní, ani nevyužijí pro sebe nebo pro jinou osobu. Zavazují se zachovat je v přísné tajnosti a sdělit je výlučně těm svým zaměstnancům nebo poddodavatelům, kteří jsou pověřeni plněním dle této Smlouvy a za tímto účelem jsou oprávněni se s těmito informacemi v nezbytném rozsahu seznámit. Smluvní strany se zavazují zabezpečit, aby i tyto osoby považovaly uvedené informace za důvěrné a zachovávaly o nich mlčenlivost.
  3. Povinnost plnit ustanovení dle čl. [11](#_bookmark21) Smlouvy se nevztahuje na informace, které:
     + je Smluvní strana povinna sdělit na základě zákonem stanovené povinnosti,
     + mohou být zveřejněny bez porušení této Smlouvy,
     + byly písemným souhlasem obou Smluvních stran zproštěny těchto omezení,
     + jsou známé nebo byly zveřejněny jinak než následkem zanedbání povinnosti jedné ze Smluvních stran,
     + příjemce je zná dříve, než je sdělí Smluvní strana,
     + jsou vyžádány soudem, státním zastupitelstvím nebo příslušným správním orgánem na základě zákona,
     + Smluvní strana je sdělí osobě vázané zákonnou povinností mlčenlivosti (např. advokátovi nebo daňovému poradci) za účelem uplatňování svých práv,
     + je Objednatel povinen sdělit svému zakladateli,
     + je Objednatel povinen sdělit jakékoli třetí osobě.
  4. Povinnost mlčenlivosti trvá bez ohledu na ukončení platnosti této Smlouvy.
  5. Pokud řádné poskytování plnění dle této Smlouvy vyžaduje zpracování osobních údajů zaměstnanců Objednatele, budou osobní údaje zaměstnanců Objednatele Dodavatelem zpracovány v rozsahu:
     + jméno, příjmení a titul,
     + adresa trvalého pobytu, doručovací adresa,
     + e-mailová adresa,
     + telefonní číslo.
  6. Zpracováním osobních údajů ve smyslu tohoto článku Smlouvy se rozumí zejména jejich shromažďování, ukládání na nosiče informací, používání, třídění nebo kombinování, blokování a likvidace s využitím manuálních a automatizovaných prostředků v rozsahu nezbytném pro zajištění řádného poskytování Plnění.
  7. Osobní údaje budou zpracovány po dobu poskytování Plnění. Ukončením této Smlouvy nezanikají povinnosti Dodavatele týkající se bezpečnosti a ochrany osobních údajů až do okamžiku jejich úplné likvidace či předání jinému zpracovateli.
  8. Smluvní strany se dohodly, že cena za zpracování osobních údajů na základě této Smlouvy je již zahrnuta v Ceně dle čl. [4](#_bookmark15) této Smlouvy, přičemž Dodavatel nemá nárok na náhradu nákladů spojených s plněním této povinnosti.
  9. Objednatel prohlašuje, že tyto údaje budou aktuální, přesné a pravdivé, jakož i to, že tyto údaje budou odpovídat stanovenému účelu zpracování.
  10. Objednatel je povinen přijmout vhodná opatření na to, aby poskytl subjektům údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace a učinil veškerá sdělení požadovaná Nařízením Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016, obecného nařízení o ochraně osobních údajů (dále jen „**Nařízení**“) ve spojení se zákonem o zpracování osobních údajů.
  11. Dodavatel je při plnění této povinnosti povinen:

1. zpracovávat osobní údaje pouze na základě doložených pokynů Objednatele;
2. zohledňovat povahu zpracování osobních údajů a být Objednateli nápomocen pro splnění Objednatelovi povinnosti reagovat na žádosti o výkon práv subjektu údajů, jakož i pro splnění dalších povinností ve smyslu Nařízení;
3. zajistit, že jeho zaměstnanci budou zpracovávat osobní údaje pouze za podmínek a v rozsahu Dodavatelem stanoveném.
   1. Dodavatel je při plnění této povinnosti oprávněn:

a) v rozsahu nezbytném pro plnění předmětu Smlouvy zapojit do zpracování i další případné zpracovatele pouze s předchozím písemným souhlasem Objednatele.

* 1. Smluvní strany jsou při zpracování povinny:

1. zavést technická, organizační, personální a jiná vhodná opatření ve smyslu Nařízení, aby zajistily a byly schopny kdykoliv doložit, že zpracování osobních údajů je prováděno v souladu s Nařízením a zákonem o zpracování osobních údajů tak, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům a k datovým nosičům, které tyto údaje obsahují, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití, a tato opatření podle potřeby průběžné revidovat a aktualizovat;
2. vést a průběžné revidovat a aktualizovat záznamy o zpracování osobních údajů ve smyslu Nařízení;
3. řádně a včas ohlašovat případná porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů a spolupracovat s tímto úřadem v nezbytném rozsahu;
4. navzájem se informovat o všech okolnostech významných pro plnění dle tohoto článku Smlouvy např. změna sídla, právní formy, změna bankovního spojení, zrušení registrace k DPH;
5. zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů, a to i po skončení této Smlouvy;
6. postupovat v souladu s dalšími požadavky Nařízení a zákona o zpracování osobních údajů, zejména dodržovat obecné zásady zpracování osobních údajů, plnit své informační povinnosti, nepředávat osobní údaje třetím osobám bez potřebného oprávnění, respektovat práva subjektů údajů a poskytovat v této souvislosti nezbytnou součinnost.

### Doba trvání Smlouvy

* 1. Smlouva nabývá platnosti dnem jejího podpisu oběma Smluvními stranami a účinnosti dnem zveřejnění této Smlouvy v registru smluv dle zákona o registru smluv.
  2. Smlouva se uzavírá na dobu určitou v délce trvání čtyřiceti osmi (48) měsíců. Tato Smlouva může být předčasně ukončena:
     1. písemnou dohodou Smluvních stran, jejíž nedílnou součástí je i vypořádání vzájemných dluhů a pohledávek;
     2. písemnou výpovědí Objednatele;
     3. odstoupením jedné ze Smluvních stran od této Smlouvy z důvodu podstatného porušení Smlouvy druhou Smluvní stranou, za podmínek uvedených v následujících odstavcích tohoto článku Smlouvy.
  3. Ukončení Smlouvy nemá vliv na platnost a účinnost jednotlivých Dílčích smluv, které byly uzavřeny Smluvními stranami před datem ukončení této Smlouvy. Práva a povinnosti z takto uzavřených Dílčích smluv se budou i nadále řídit ujednáními Smluvních stran uvedenými v této Smlouvě. V případě předčasného zániku účinnosti Smlouvy z jakéhokoliv důvodu není účinnost Dílčích smluv dotčena, ledaže by se důvod zániku účinnosti vztahoval i na tyto Dílčí smlouvy.
  4. Za podstatné porušení této Smlouvy Dodavatelem, které zakládá právo Objednatele na odstoupení od Smlouvy, se považuje zejména:
     1. prodlení Dodavatele s plněním jakékoliv povinnosti plynoucí z této Smlouvy nebo Dílčí smlouvy delší než patnáct (15) kalendářních dnů,
     2. Dodavatel se dopustil vůči Objednateli jednání vykazujícího znaky nekalé soutěže a toto porušení Smlouvy nenapravil ani přes písemnou výzvu Objednatele v přiměřené, k tomu stanovené lhůtě,
     3. Dodavatel opakovaně, tj. nejméně dvakrát (2x) během šedesáti (60) po sobě jdoucích kalendářních dnů, poruší svou povinnost dle této Smlouvy nebo Dílčí smlouvy,
     4. je-li Dodavatel v likvidaci nebo vůči jeho majetku probíhá insolvenční řízení, v němž bylo vydáno rozhodnutí o úpadku nebo insolvenční návrh byl zamítnut proto, že majetek nepostačuje k úhradě nákladů insolvenčního řízení, nebo byl konkurs zrušen proto, že majetek byl zcela nepostačující nebo byla zavedena nucená správa podle zvláštních právních předpisů,
     5. Dodavatel poruší či neplní kterékoliv z ustanovení Smlouvy:
        + týkajících se prohlášení uvedených v čl. [1](#_bookmark0) odst. [1.4](#_bookmark2) Smlouvy;
        + týkajících se vlastnických práv, licencí a podmínek užití Plnění dle čl. [13](#_bookmark25) Smlouvy;
        + uvedených v čl. [11](#_bookmark21) a [14](#_bookmark28) Smlouvy.
  5. Objednatel je oprávněn od této Smlouvy odstoupit v případě, že došlo k významné změně vlastnictví zásadních aktiv, změně kontroly nad Dodavatelem nebo změně oprávnění nakládat s aktivy využívanými Dodavatelem k plnění dle této Smlouvy.
  6. V případech uvedených v odst. [12.4](#_bookmark23) tohoto článku Smlouvy je Objednatel oprávněn odstoupit i pouze od příslušné Dílčí smlouvy.
  7. Dodavatel je oprávněn odstoupit od Smlouvy pouze v případě prodlení Objednatele s úhradou faktury delším než třicet (30) kalendářních dnů od písemného upozornění Dodavatele.
  8. Odstoupení je účinné od okamžiku, kdy je doručeno písemné prohlášení jedné Smluvní strany o odstoupení od Smlouvy druhé Smluvní straně. Plnění, které si Smluvní strany řádně poskytly před odstoupením od Smlouvy, se nevrací, nesjednají-li si Smluvní strany jinak. V případě sjednání vracení Plnění či jeho části jsou Smluvní strany povinny vzájemnou dohodou písemně vypořádat dosavadní přijaté smluvní plnění nejpozději do jednoho (1) měsíce od odstoupení od Smlouvy.
  9. Objednatel je oprávněn tuto Smlouvu vypovědět z jakéhokoli důvodu i bez udání důvodů s výpovědní dobou tří (3) kalendářních měsíců, jež začne plynout prvním dnem kalendářního měsíce následujícího po měsíci, v němž byla písemná výpověď doručena Dodavateli.
  10. V případě řádného i předčasného zániku účinnosti této Smlouvy je Dodavatel povinen poskytnout Objednateli na jeho vyžádání dokumenty a informace vztahující se k poskytnutému Plnění, a to ve lhůtě jednoho (1) měsíce ode dne odeslání takového požadavku Objednatelem a minimálně v následujícím rozsahu:
* aktuální stav vyčerpané alokace ke dni skončení účinnosti této Smlouvy u jednotlivých rolí v rámci příslušných Dílčích smluv účinných v den skončení účinnosti této Smlouvy a popis odvedené činnosti u dané role v rámci příslušné Dílčí smlouvy v porovnání s předpokladem stanoveným pro danou roli v příslušné Dílčí smlouvě.

Ustanovení tohoto odstavce se obdobně použijí v případě předčasného zániku účinnosti Dílčí smlouvy. Smluvní strany se dohodly, že cena za poskytnutí takovéto exitové součinnosti je již zahrnuta v Ceně dle čl. [4](#_bookmark15) této Smlouvy, přičemž Dodavatel nemá nárok na náhradu nákladů spojených s plněním této povinnosti.

* 1. Dodavatel se zavazuje i po ukončení účinnosti této Smlouvy, pokud Objednatel nestanoví odlišně, poskytovat bez přerušení Služby až do kompletního převzetí Služeb novým dodavatelem, popř. Objednatelem, a to za podmínek stanovených touto

Smlouvou, to vše maximálně po dobu šesti (6) měsíců. Podrobné podmínky poskytování Služeb pro toto období včetně cenových podmínek budou stanoveny v příslušné Dílčí smlouvě, kterou je Dodavatel povinen s Objednatelem na základě jím zaslané Výzvy a postupem dle této Smlouvy, uzavřít nejpozději v poslední den účinnosti této Smlouvy.

### Vlastnické právo, licence a podmínky užití Plnění

#### Vlastnické právo

* 1. Vlastnické právo k hmotným nosičům dat, na nichž jsou Autorská díla dle tohoto čl. [13](#_bookmark25) Smlouvy zaznamenána a k ostatním materiálům přechází na Objednatele okamžikem jejich převzetí. Nebezpečí škody na hmotných složkách Plnění přechází na Objednatele okamžikem jejich faktického předání do dispozice Objednatele, pokud o takovém předání byl sepsán písemný záznam podepsaný oprávněnými osobami Smluvních stran. Cena hmotných nosičů dat je již zahrnuta v Ceně stanovené dle čl. [4](#_bookmark15) této Smlouvy.

#### Základní rozsah licence

* 1. Smluvní strany sjednávají, že budou-li Dodavatelem v rámci činností dle čl. [1](#_bookmark0) odst. [1.3](#_bookmark1) této Smlouvy provedeny Služby, jejichž výsledek bude předmětem autorskoprávní ochrany podle 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 „**Autorský zákon**“), Dodavatel poskytne Objednateli výhradní oprávnění k výkonu práva užít takto vytvořené a/nebo upravené Autorské dílo či jeho část (výhradní licenci k užití takto vytvořeného a/nebo upraveného Autorského díla či jeho části), a to s účinností ode dne podpisu Výkazu práce / Akceptačního protokolu oběma Smluvními stranami v rámci akceptačního řízení, na jehož základě dochází k dodání Plnění dle Dílčí smlouvy, jehož součástí je příslušné Autorské dílo. Pro vyloučení pochybností se sjednává, že v rámci oprávnění k výkonu užít Autorské dílo či jeho část je Objednatel oprávněn Autorské dílo či jeho část dále rozvíjet podle svých potřeb.
  2. Předměty autorskoprávní ochrany podle Autorského zákona uvedené v odst. 13.2 tohoto článku Smlouvy budou v tomto čl. [13](#_bookmark25) Smlouvy dále označovány dohromady jako

„**Autorská díla**“ a jednotlivě jako „**Autorská dílo**“.

* 1. Majetková práva k výše uvedeným Autorským dílům jsou poskytována Dodavatelem Objednateli formou licenčního ujednání ve smyslu ustanovení § 2358 a násl. Občanského zákoníku majícího následující charakteristiky:
     1. výhradní licence k veškerým zákonem povoleným způsobům užití jednotlivých Autorských děl a jejich případných dalších verzí, zejména k účelu, ke kterému

byla taková Autorská díla Dodavatelem vytvořena v souladu se Smlouvou a Dílčí smlouvou, a to v rozsahu minimálně nezbytném pro řádné užívání předmětu plnění dle této Smlouvy a Dílčí smlouvy Objednatelem,

* + 1. licence neomezená územním (teritoriálním) či množstevním rozsahem a rovněž tak neomezená rozsahem užití, zejména neomezená počtem uživatelů či mírou využívání,
    2. licence neomezená časově, tzn. udělená na celou dobu trvání majetkových práv k předmětným Autorským dílům,
    3. licence převoditelná a postupitelná, tj. která je udělena s právem udělení podlicence či postoupení licence jakékoliv třetí osobě.

Z důvodu právní jistoty se sjednává, že licence je vždy udělena v maximálním rozsahu povoleném platnými právními předpisy.

Dodavatel zároveň uděluje Objednateli souhlas k tomu, aby nejpozději ke dni akceptace Plnění dle příslušné Dílčí smlouvy, v jehož rámci Autorské dílo vzniklo, byl Objednatel oprávněn jednotlivá Autorská díla zveřejnit, upravovat, modifikovat, zpracovávat, překládat, či měnit jejich název, a že je též oprávněn tato Autorská díla spojit s dílem jiným a zařadit je do díla souborného. Dodavatel uděluje Objednateli souhlas k tomu, aby Objednatel svěřil svá práva dle tohoto článku Smlouvy třetím osobám, které budou v budoucnu užívat Autorská díla vzniknuvší na základě této Smlouvy. Bude-li Autorské dílo nebo jeho část dílem zaměstnaneckým (dle § 58 AZ) nebo dílem kolektivním (dle § 59 AZ), je Dodavatel povinen vypořádat práva s autory takových děl (zejména opatřit potřebné souhlasy autorů a uhradit veškeré odměny autorům) tak, aby práva k takovému Autorskému dílu Objednateli mohl poskytnout v plném rozsahu dle tohoto článku Smlouvy a jejích příloh. Předáním části Předmětu plnění, které je Autorským dílem, Dodavatel poskytuje Objednateli potřebné Licence SW k Autorskému dílu a zároveň tím stvrzuje, že veškerá práva s autory zaměstnaneckých či kolektivních děl řádně vypořádal a je oprávněn je poskytnout Objednateli.

* 1. Vznikne-li v rámci Plnění dle této Smlouvy a Dílčí smlouvy plnění naplňující znaky databáze dle Autorského zákona, poskytuje Dodavatel Objednateli k okamžiku podpisu příslušného Akceptačního protokolu zvláštní právo pořizovatele databáze, a to zejména právo databázi vytěžovat i zužitkovávat, a to jak celý její obsah, tak i její kvalitativně nebo kvantitativně podstatné části. Dodavatel dále poskytuje Objednateli právo udělit oprávnění k výkonu práva pořizovatele databáze jinému v rozsahu, jak je udělil Dodavatel Objednateli.
  2. V případě programů vytvořených v programovacím jazyce se licence ve smyslu odst.

13.2 a 13.4 tohoto článku Smlouvy vztahuje ve stejném rozsahu na Autorská díla ve strojovém i zdrojovém kódu, jakož i k další Dokumentaci dle čl. [3](#_bookmark7) odst. [3.17](#_bookmark14) této

Smlouvy. Předchozí věta tohoto odstavce se vztahuje i na případné další verze Autorských děl vytvořených či upravených Dodavatelem na základě této Smlouvy a taktéž na související Dokumentaci.

* 1. Dodavatel prohlašuje, že udělení veškerých práv uvedených v čl. [13](#_bookmark25) odst. 13.2 až 13.7 této Smlouvy nelze ze strany Dodavatele vypovědět a že na udělení těchto práv nemá vliv ani případné ukončení platnosti Smlouvy. V souvislosti s tímto ujednáními o licenční smlouvě ve smyslu tohoto článku Smlouvy Smluvní strany výslovně vylučují ustanovení

§ 2378, § 2379, § 2380, § 2381 a § 2382 Občanského zákoníku.

* 1. Dodavatel se zavazuje v případě, že se právo užití Autorského díla vztahuje k programům vytvořeným v programovacím jazyce, poskytnout vždy Objednateli na jeho vyžádání strojové i zdrojové kódy takových programů vytvořených v programovacím jazyce, jakož i veškerou další Dokumentaci vztahující se k těmto zdrojovým kódům, to vše vždy v plném rozsahu a aktuální verzi.
  2. Dodavatel prohlašuje, že Autorská díla ani jejich části nemají žádné právní vady, že nejsou zatížena právy třetích osob týkajících se zejména vlastnického práva a práv duševního vlastnictví a že Dodavatel je zcela oprávněn disponovat bez jakéhokoliv omezení veškerými majetkovými právy k Autorským dílům a jejich částem a uzavřít s Objednatelem tuto Smlouvu na celý rozsah předmětu plnění. V případě, že se uvedené prohlášení Dodavatele nezakládá na pravdě, Dodavatel odpovídá Objednateli za vyplývající důsledky v plném rozsahu včetně odpovědnosti za skutečnou škodu a ušlý zisk. Uplatní-li třetí osoba své právo k Autorským dílům a/nebo jejich části, zavazuje se Dodavatel bez zbytečného odkladu a na vlastní náklady učinit potřebná opatření k ochraně oprávnění k výkonu práv užít Autorská díla Objednatelem, pokud jej k tomu Objednatel zmocní.
  3. Dodavatel zároveň prohlašuje, že užitím Autorských děl a databází Objednatelem v souladu s touto Smlouvou nejsou dotčena autorská ani jiná práva třetích osob. Dodavatel odpovídá Objednateli za škodu, která by vznikla Objednateli v důsledku uplatnění práv duševního vlastnictví třetích osob vůči Objednateli pro řádné užívání Autorských děl a databází, k němuž udělil nebo zajistil Dodavatel licenci či podlicenci na základě tohoto článku Smlouvy. Dodavatel se tímto zavazuje poskytnout Objednateli na svůj náklad veškerou účinnou součinnost nutnou pro úspěšnou obranu práv Objednatele ve vztahu k uplatnění práv duševního vlastnictví třetích osob. Objednatel se zavazuje bez zbytečného odkladu oznámit Dodavateli, že došlo k uplatnění nároků třetích osob pro porušování jejich práv duševního vlastnictví v souvislosti s plněním dle této Smlouvy.
  4. Dodavatel dále prohlašuje, že mu ke Autorským dílům a databázím náleží veškerá oprávnění, která Objednateli poskytuje, a to v rozsahu práv autorských, práv souvisejících s právem autorským i práv spadajících pod režim ostatních právních předpisů na ochranu duševního vlastnictví, ochranných známek a dále práv

osobnostních. Dodavatel dále prohlašuje, že nositelům výše uvedených práv nepřísluší a nebude příslušet vůči Objednateli žádné právo na odměnu, či jakékoli jiné plnění v souvislosti s realizací užití Autorských děl a databází. Dále Dodavatel zaručuje, že výše uvedená práva nebudou vůči Objednateli uplatněna ani samotnými nositeli, ani prostřednictvím kolektivních správců jejich práv.

* 1. Je-li část plnění dle této Smlouvy chráněna jiným způsobem, než jako Autorské dílo (ochrana jiných práv k duševnímu vlastnictví), uplatní se ustanovení tohoto článku analogicky tak, aby byl splněn účel této Smlouvy, tj. aby Objednatel obdržel dílo vč. všech jeho součástí vč. možnosti jej užívat, poskytovat k užívání, udržovat a rozvíjet, a to tak, aby tak mohl činit i samostatně nebo prostřednictvím třetí osoby. To se nevztahuje na začlenění proprietárních částí díla (např. knihoven), u nichž není možné taková práva zajistit, pokud s jejich začleněním Objednatel souhlasí. Dodavatel je povinen k dosažení shora uvedeného účelu poskytnout rovněž související informace, zejm. zdrojové kódy, popisy databází, popisy architektury a jiné informace.

#### Přechod práv, licenční odměna a garance rozsahu licence

* 1. Smluvní strany tímto výslovně souhlasí s tím, že veškerá finanční vyrovnání za poskytnutí oprávnění, licencí, postoupení a podlicencování oprávnění k výkonu majetkových práv autorských dle tohoto čl. [13](#_bookmark25) Smlouvy (a to včetně zdrojových a strojových kódů a veškeré Dokumentace) jsou již plně zahrnuta v Ceně stanovené dle čl. [4](#_bookmark15) této Smlouvy.
  2. Práva získaná v rámci plnění této Smlouvy přechází i na případného právního nástupce Objednatele. Případná změna v osobě Poskytovatele (např. právní nástupnictví) nebude mít vliv na oprávnění udělená v rámci této Smlouvy Dodavatelem Objednateli.
  3. Bez ohledu na formu uzavření licenční smlouvy platí, že Dodavatel je vždy povinen zajistit poskytnutí licence dle podmínek stanovených Smlouvou na Autorská díla.

### Kybernetická bezpečnost

* 1. Správcem budovaného informačního systému v rámci projektu „Vybudování Informačního systému pro veřejné služby a služby veřejné správy INSPIRE“ je Ministerstvo vnitra České republiky, Nad Štolou 936/3, 170 34 Praha 7 (MV). Správce informačního systému stanovil, že vytvořený informační systém musí splňovat bezpečnostní požadavky shodně, jako na významný informační systém (dále jen „**VIS**“) dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „**ZoKB**“). Důvodem je, že informační systém bude po vybudování naplňovat určující kritéria pro VIS.
  2. Dodavatel podpisem této Smlouvy akceptuje, že dodávané plnění dle této Smlouvy je ve prospěch informačního systému, na který jsou kladeny bezpečnostní požadavky

stejné jako na významný informační systém (VIS) dle ZoKB, a současně se zavazuje k zavedení a dodržování veškerých souvisejících bezpečnostních opatření požadovaných ZoKB a vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) (dále jen „**VyKB**“), a to minimálně po dobu plnění dle této Smlouvy.

* 1. Dodavatel je povinen:
     1. umožnit Objednateli provedení zákaznického auditu u Dodavatele a poskytnout mu k němu nezbytnou součinnost (dále jen „**zákaznický audit**“). Objednatel je oprávněn provést zákaznický audit v případě auditu kybernetické bezpečnosti, dle

§ 16 VyKB Objednatelem provozovaného VIS. Dále lze provést zákaznický audit v případě řešení kybernetického bezpečnostního incidentu v přímé souvislosti s plněním dle této Smlouvy. Zákaznický audit může za Objednatele provést pověřený zaměstnanec Objednatele nebo jiná pověřená osoba. Objednatel je oprávněn pověřit provedením zákaznického auditu třetí stranu. Rozsah auditu musí být rozsahem relevantní k předmětu a účelu této Smlouvy;

* + 1. dodržovat při poskytování Plnění příslušná ustanovení bezpečnostních politik, metodik a postupů předaných Dodavateli Objednatelem, resp. platné řídící dokumentace Objednatele či její části anebo platné řídící dokumentace, k jejímuž dodržování se Objednatel zavázal, pokud byl Dodavatel s takovými dokumenty nebo jejich částmi seznámen, a to bez ohledu na způsob, jakým byl s takovou dokumentací Objednatele seznámen (např. školením, protokolárním předáním příslušné dokumentace Dodavateli, elektronickým předáním prostřednictvím e- mailu, zřízením přístupu Dodavateli na sdílené úložiště aj.). V případě provedených změn v bezpečnostní dokumentaci VIS, bude Dodavatel informován. Dodavatel je povinen řídit se novým obsahem bezpečnostní dokumentace VIS od data stanoveného Objednatelem, nejdříve však ode dne, kdy byl o změně informován;
    2. informovat neprodleně Objednatele o kybernetických bezpečnostních incidentech na straně Dodavatele souvisejících s plněním dle této Smlouvy, a které by mohly mít dopad na kybernetickou bezpečnost u Objednatele. Kybernetický bezpečnostní incident je definován ustanovením § 7 odst. 2 ZoKB;
    3. informovat neprodleně Objednatele o změně ovládání Dodavatele podle zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích) nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s aktivy určených k plnění dle této Smlouvy.
  1. Dodavatel je při poskytování Plnění pro Objednatele oprávněn užívat data předaná Dodavateli Objednatelem za účelem plnění předmětu Smlouvy, avšak vždy pouze v rozsahu nezbytném ke splnění předmětu Smlouvy.
  2. Dodavatel se při poskytování plnění pro Objednatele zavazuje nakládat s daty pouze v souladu se Smlouvou a příslušnými právními předpisy, zejména ZoKB, VyKB a dalšími souvisejícími právními předpisy.
  3. Dodavatel bere na vědomí, že přístup k datům, informacím či zařízením souvisejícím s předmětem Smlouvy je možné povolit pouze fyzické identitě zaměstnance Dodavatele nebo poddodavatele Dodavatele zaevidované, a to na základě požadavku Dodavatele na přístup.
  4. Dodavatel bere na vědomí, že přidělení oprávnění zaměstnanci Dodavatele musí být řízeno zásadou tzv. „potřeba vědět“ (need to know) a není nárokové.
  5. Dodavatel se zavazuje, že udělený přístup nesmí být sdílen více zaměstnanci Dodavatele nebo poddodavatele Dodavatele.
  6. Dodavatel se zavazuje, že nebude instalovat a používat žádné nástroje, které nebyly předem písemně odsouhlaseny Objednatelem a jejichž užívání by mohlo ohrozit kybernetickou bezpečnost.
  7. Dodavatel se zavazuje, že nebude vyvíjet, kompilovat a šířit v jakékoliv části technologického nebo komunikačního systému programový kód, který má za cíl nelegální ovládnutí, narušení, nebo diskreditaci technologického nebo komunikačního systému nebo nelegální získání dat a informací. Dodavatel bere na vědomí, že přístup do interní sítě a/nebo k technologickým a komunikačním systémům bude realizován s využitím zařízení Objednatele. V případě, že Objednatel povolí Dodavateli přístup do interní sítě a/nebo k technologickým a komunikačním systémům Objednatele ze zařízení Dodavatele, musí veškerá tato zařízení Dodavatele splňovat příslušné bezpečnostní standardy Objednatele.
  8. Dodavatel se během poskytování Plnění pro Objednatele zavazuje dostatečně zabezpečit veškerý přenos dat a informací z pohledu bezpečnostních požadavků na jejich důvěrnost, integritu a dostupnost.
  9. Dodavatel se zavazuje plnit požadavky Objednatele v oblasti likvidace dat (ať už dat na papírových médiích, dat zpracovávaných elektronicky nebo prostřednictvím jakýchkoliv dalších nosičů dat) dle přílohy č. 4 VyKB.
  10. Dodavatel se zavazuje zajistit, aby osoby podílející se na poskytování Plnění Objednateli, kteří přistupují do interní sítě a/nebo technologického nebo komunikačního systému chránili autentizační prostředky a údaje k systémům Objednatele. Dodavatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako bezpečnostní incident ve smyslu příslušné řídící dokumentace a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům fyzických osob externího subjektu platí pro Dodavatele, pokud byl s takovou řídící dokumentací Objednatele seznámen).
  11. Dodavatel bere na vědomí, že postup zvládání bezpečnostního incidentu či skutečnost vzniklá v důsledku porušení bezpečnostních požadavků nebude posuzována jako okolnost vylučující odpovědnost Dodavatele za prodlení s řádným a včasným plněním předmětu Smlouvy a nebude důvodem k jakékoli náhradě případné újmy Dodavateli či jiné osobě ze strany Objednatele. Ostatní ustanovení ohledně odpovědnosti Dodavatele za prodlení obsažená v Smlouvě nejsou tímto ustanovením dotčena.
  12. Dodavatel se zavazuje poskytnout Objednateli veškerou nezbytnou součinnost ke splnění povinností Objednatele zejména při analýze souvisejících rizik, přijímání opatření za účelem snížení všech nepříznivých dopadů spojených se změnami, aktualizaci bezpečnostní dokumentace, souvisejícím testováním a zajištění možnosti navrácení do původního stavu.
  13. Dodavatel se zavazuje dodržovat požadavky Objednatele na řízení kontinuity činností.
  14. Dodavatel stanoví činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání bezpečnostních událostí a incidentů, podle takto stanovených a popsaných pravidel bude postupovat, a bude hlásit všechny bezpečnostní události a incidenty neprodleně po jejich detekci Objednateli prostřednictvím ohlašovacích kanálů Objednatele, v případech, kdy situace nestrpí odklad telefonicky. Dále se zavazuje vyhodnotit informace o bezpečnostních událostech a incidentech a o těchto informacích, vzniklých bezpečnostních incidentech, vč. krátkodobých a dlouhodobých nápravných opatřeních nad všemi částmi řešení, které jsou ve správě Dodavatele, a rizicích souvisejících s ohrožením kontinuity činností vést přiměřené záznamy a tyto uchovat pro jejich budoucí použití s ohledem na požadavky Objednatele a legislativy České republiky. Nastavená pravidla a postupy podléhají schválení Objednatelem.
  15. Dodavatel provede analýzu příčin bezpečnostního incidentu a navrhne opatření s cílem zamezit jeho opakování v případě, že Dodavatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

### Závěrečná ustanovení

* 1. Tato Smlouva se řídí právním řádem České republiky. Práva a povinnosti Smluvních stran výslovně v této Smlouvě neupravené se řídí příslušnými ustanoveními občanského zákoníku, Autorského zákona a ZZVZ.
  2. Smluvní strany si ve smyslu ustanovení § 1765 odst. 2 občanského zákoníku ujednaly, že Dodavatel na sebe přebírá nebezpečí změny okolností.
  3. Dodavatel tímto prohlašuje, že mu byly ze strany Objednatele sděleny veškeré skutkové a právní okolnosti související s uzavřením této Smlouvy a že Dodavatel je v tomto ohledu přesvědčen o jeho schopnosti uzavřít tuto Smlouvu, má zájem tuto Smlouvu uzavřít a je schopen plnit veškeré povinnosti z této Smlouvy plynoucí.
  4. Smluvní strany se dohodly, že veškeré spory vzniklé z této Smlouvy nebo v souvislosti s ní budou řešeny podle českého práva a místně příslušným soudem pro řešení případných sporů bude soud příslušný dle místa sídla Objednatele.
  5. Smlouvu lze měnit pouze na základě dohody formou písemných vzestupně očíslovaných dodatků potvrzených smluvními zástupci obou Smluvních stran. Veškerá oznámení učiněná podle Smlouvy budou zasílána na adresy a kontaktní adresy uvedené v čl. [8](#_bookmark19) této Smlouvy. Dnem doručení písemností odeslaných na základě této Smlouvy nebo v souvislosti s touto Smlouvou, pokud není prokázán jiný den doručení, se rozumí poslední den lhůty, ve které byla písemnost pro adresáta uložena u provozovatele poštovních služeb, a to i tehdy, jestliže se adresát o jejím uložení nedověděl. Smluvní strany tímto výslovně vylučují ustanovení § 573 občanského zákoníku.
  6. Pokud kterékoli ustanovení této Smlouvy nebo jeho část je nebo se stane neplatným či nevynutitelným, nebude mít tato neplatnost či nevynutitelnost vliv na platnost či vynutitelnost ostatních ustanovení této Smlouvy nebo jejích částí, pokud nevyplývá přímo z obsahu této Smlouvy, že toto ustanovení nebo jeho část nelze oddělit od dalšího obsahu. V takovém případě se obě Smluvní strany zavazují neúčinné a neplatné ustanovení nahradit novým ustanovením, které je svým účelem a významem co nejbližší ustanovení této Smlouvy, jež má být nahrazeno.
  7. Tato Smlouva je uzavírána elektronickou formou, kdy Dodavatel obdrží elektronický dokument, podepsaný v souladu s platnou právní úpravou.
  8. Smluvní strany prohlašují, že tato Smlouva je projevem jejich pravé a svobodné vůle a nebyla sjednána v tísni ani za jinak jednostranně nevýhodných podmínek. Na důkaz toho připojují Smluvní strany své podpisy.
  9. Nedílnou součástí Smlouvy jsou tyto přílohy:
     + Příloha č. 1 – Specifikace Služeb
     + Příloha č. 2 – Specifikace ceny Služeb pro jednotlivé role
     + Příloha č. 3 – Vzory dokumentů pro akceptační řízení
     + Příloha č. 4 – Specifikace rolí a Realizační tým
     + Příloha č. 5 – Minimální kapacita osob ve vybraných rolích
     + Příloha č. 6 – Rámcová pravidla vývoje aplikací pro ISSI

|  |  |
| --- | --- |
| Za Objednatele: | Za Dodavatele: |
| V Praze dne: | V Praze dne: |

|  |  |  |
| --- | --- | --- |
|  |  |  |
| xxx |  | xxx |
| xxx  **Národní agentura pro komunikační a informační technologie, s. p.** |  | xxx  **SEVITECH CZ s.r.o.** |

### Příloha č. 1 – Specifikace Služeb

Účelem této Smlouvy je zajištění integrace a konfigurace GIS Systému v rámci ISSI, které má v gesci Ministerstvo vnitra České republiky. Poptávaný GIS Systém, který je předmětem jiné smlouvy uzavřené na základě výsledku předmětného Zadávacího řízení, se skládá z několika SW komponent, které společně představují platformu pro kompletní řešení požadavků na zpracování dat v rámci INSPIRE.

Předmětem této Smlouvy je zejména personální a odborné zajištění při integračních a konfiguračních činnostech souvisejících s jednotlivými SW komponentami a GIS Systémem jako celkem. Realizační tým budou tvořit osoby poskytnuté Dodavatelem a splňující náležitosti, odbornost a specifikaci požadované pro předmětné role v rámci Zadávacího řízení. V rámci těchto rolí dojde k nastavení a optimalizaci (výkonové a funkční) dodané platformy GIS Systému a jeho plné integraci do prostředí ISSI. Rozsah znalostí jednotlivých rolí musí v určených oblastech korespondovat s dodanou technologií komponent GIS Systému.

**Příloha č. 2 – Specifikace ceny Služeb pro jednotlivé role**

|  |  |
| --- | --- |
| **ROLE** | **Cena za 1 MD [Kč bez DPH] (\*)** |
| **Projektový manažer** | 7 800,00 Kč |
| **DB analytik** | 2 500,00 Kč |
| **DB specialista** | 2 500,00 Kč |
| **DB vývojář** | 2 500,00 Kč |
| **Metadatový specialista** | 2 500,00 Kč |
| **GIS Specialista ETL** | 8 000,00 Kč |
| **GIS Vývojář** | 7 850,00 Kč |
| **GIS Analytik** | 2 500,00 Kč |
| *\*denní sazba může být v případě nutnosti dělena po jednotlivých hodinách (stanovena je pro 8h pracovní směnu)* | |

**Příloha č. 3 - Vzory dokumentů pro akceptační řízení**

1. **Akceptační protokol**

**Smlouva:**

**Číslo smlouvy:** **Akceptační protokol č. 1**

|  |  |
| --- | --- |
| Dodavatel |  |
| Objednatel |  |
| Rámcová dohoda |  |
| Dílčí smlouva |  |
| Název Projektu |  |
| Datum předání |  |

**Předmět akceptace**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Číslo | Popis | Akceptováno | Akceptováno s výhradou | Neakceptováno |
| 01 |  |  |  |  |

**Výhrady**

|  |  |  |  |
| --- | --- | --- | --- |
| Číslo | Popis výhrady | Kategorie vady | Termín pro vypořádání vady |
| 01 |  |  |  |
| 02 |  |  |  |
| 03 |  |  |  |
| 04 |  |  |  |

**Report poskytnutých Služeb**

|  |  |  |
| --- | --- | --- |
| Role | Popis činnosti | Počet člověkohodin  / MD |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Seznam příloh**

**Závěrečná ustanovení**

Dodavatel a Objednatel svým podpisem stvrzují akceptaci dle výše specifikované Dílčí smlouvy a Smlouvy.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Jméno a příjmení | Datum | Podpis |
| Akceptoval za Dodavatele |  |  |  |
| Akceptoval za Objednatele |  |  |  |

### Výkaz práce

**AKCEPTAČNÍ PROTOKOL č.…..**

|  |  |
| --- | --- |
| **Objednatel** | Národní agentura pro komunikační a informační technologie, s. p. |
| **Dodavatel** |  |
| **Název a číslo smlouvy** |  |
| **Název projektu** |  |

**Předmět akceptace**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Číslo** | **Předmět jednotlivé dílčí smlouvy** | **Počet člověkodnů za jednotlivé dílčí smlouvy** | **Datum**  **předání** | **Akceptováno**  **(ANO/NE)** | **Cena v Kč za služby dle jednotlivé dílčí smlouvy** |
| 01 |  |  |  |  |  |
| 02 |  |  |  |  |  |
| 03 |  |  |  |  |  |
| 04 |  |  |  |  |  |
| **Celkem akceptováno** | | **x** | **x** | **x** |  |

**Výhrady**

|  |  |
| --- | --- |
| **Číslo** | **Popis** |
| 01 |  |

Národní agentura pro komunikační a informační technologie a svým podpisem stvrzují předání

a Akceptaci výše uvedeného předmětu plnění. V Praze dne ……

|  |  |  |
| --- | --- | --- |
| **Společnost** | **Jméno** | **Podpis** |
| Předal za ……. |  |  |
| Akceptoval za Národní agentura pro komunikační a informační technologie, s.p. |  |  |

**Příloha č. 4 – Specifikace rolí a Realizační tým**

1. **Specifikace rolí**
   * **Projektový manažer**

Vede projekt na straně Dodavatele. Plánuje dílčí úkoly, kontroluje a dohlíží na jejich plnění. Spolupracuje s Projektovým manažerem na straně Objednatele.

### DB analytik

Umí vybrat vhodné databázové softwarové prostředky na základě požadavků. Vytváří logické i fyzické databázové modely. Navrhuje logiku databázových funkcí a umí připravit zadání pro jejich vývoj. Má odpovědnost za implementaci databázových modelů a schémat na dané technologii.

### DB specialista

Konfiguruje dané databázové softwarové prostředky a optimalizuje jejich výkon. Umí analyzovat výkoností problémy a navrhovat jejich řešení. Podílí se na implementaci, provozu a dohledu databázových softwarových prostředků. Má znalosti a zkušenosti se zálohováním, obnovou a replikací databázových dat.

### DB vývojář

Vyvíjí databázové funkce na základě požadavků a určuje jejich strukturu. Má zodpovědnost za kvalitu programového zdrojového kódu a jeho verzování. Připravuje automatické testy funkcí a implementaci programových změn. Pro naplnění požadavků dokáže zvolit vhodné programovací prostředky na základě určené databázové technologie.

### Metadatový specialista

Orientuje se v oblasti metadatových softwarových prostředků a formátů. Analyzuje požadavky na metadata a na jejich základě dokáže zvolit vhodné softwarové technologie a připravit zadání pro vývoj. Umí ověřit správnou funkci metadatových softwarových prostředků a validovat použité metadatové formáty.

### GIS Specialista ETL

Dle požadavků navrhuje a vytváří transformační procesy nad prostorovými daty. Orientuje se v oblasti GIS ETL softwarových prostředků a umí je využít. Má zodpovědnost za funkci, kvalitu a verzování vytvořených ETL procesů a dokáže připravit jejich automatické funkční testy. Podílí se na implementaci, provozu, dohledu a rozvoji ETL procesů.

### GIS Vývojář

Dokáže zvolit vhodné prostorové programovací prostředky dle požadavků. Zná problematiku souřadnicových systémů. Umí programově pracovat se souřadnicemi (manipulace, výpočty) a vizualizovat výsledky. Ovládá programové webové GIS technologie. Má zodpovědnost za kvalitu programového zdrojového kódu, jeho verzování a automatické testování. Podílí se na implementaci vyvinutých softwarových prostředků.

### GIS Analytik

Disponuje znalostmi v oblasti GIS technologií. Na základě požadavků navrhuje vhodná řešení a připravuje zadání pro vývoj softwarových prostředků. Podílí se na funkčním testování, kontrole zdrojového kódu, analýze chyb, implementaci a provozu. Má zodpovědnost za funkčnost navrženého řešení.

### Realizační tým – personální obsazení jednotlivých rolí

|  |  |
| --- | --- |
| **Role** | **Jméno člena týmu** |
| Projektový manažer | xxx |
| DB analytik | xxx |
| DB specialista | xxx |
| DB vývojář 1 | xxx |
| DB vývojář 2 | xxx |
| Metadatový specialista | xxx |
| GIS Specialista ETL 1 | xxx |
| GIS Specialista ETL 2 | xxx |
| GIS Vývojář 1 | xxx |
| GIS Vývojář 2 | xxx |
| GIS Analytik | xxx |

**Příloha č. 5 – Minimální kapacita osob ve vybraných rolích**

Dodavatel je povinen po celou dobu účinnosti této Smlouvy garantovat, že v každém okamžiku v průběhu účinnosti této Smlouvy disponuje minimální kapacitou osob v níže uvedených rolích:

|  |  |
| --- | --- |
| **Role** | **Minimální kapacita osob** |
| Projektový manažer | 1 |
| DB analytik | 1 |
| DB specialista | 1 |
| DB vývojář | 2 |
| Metadatový specialista | 1 |
| GIS Specialista ETL | 2 |
| GIS Vývojář | 2 |
| GIS Analytik | 1 |

**Příloha č. 6 – Rámcová pravidla vývoje, dodávek a souvisejících procesů a postupů**

**pro Informační systém pro veřejné služby a služby veřejné správy INSPIRE (ISSI)**

1. **Úvod**

Dokument nastavuje pravidla pro vývoj aplikací, webových portálů, SW řešení a formu spolupráce v prostředí Azure DevOps a návazné procesy vývoje včetně bezpečného vývoje pro projekt ISSI.

Na jednotlivé části plnění se užijí pouze ty číslované kapitoly těchto pravidel, které jsou pro příslušnou část plnění relevantní.

### Cílem je:

* + Standardizace a popis procesu a nutných předpokladů k předání binárních artefaktů a zdrojových kódů.
  + Odsouhlasení si jednotlivých kroků. Standardizace životního cyklu zdrojového kódu a přiřazení odpovědností.
  + Stanovení politiky verzování, jak pro zdrojové kódy, tak i binární artefakty (verzování jednotlivých dodávek jako celku).
  + Formální (závazný) popis požadavků implementace „automatizace“, tzn. politik GITu, kompilátorů a Cl/CD pipeline způsobem, že vynucení „bezpečného vývoje“ bude implicitní.
  + Základní identifikace procesu modelování hrozeb na úrovni komponent aplikace.
  + Pravidla pro externí programátory a vymezení základních pravidel, která budou v souladu s metodikou.
  + Navazuje na systém řízení bezpečnosti informací Ministerstva vnitra (dále jen „**ISMS MV**“) a detailněji rozpracovává bezpečnostní požadavky stanovené bezpečnostními politikami ISMS MV v souvislosti s vývojem aplikací pro projekty. S tím, že tyto aplikace jsou určeny, nebo naplňují určovací kritéria, jako kritická informační infrastruktura nebo významný informační systém dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „**ZoKB**“), a musí splňovat bezpečnostní požadavky určené legislativou v oblasti kybernetické bezpečnosti, především vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen

„**VyKB**“).

Vývojový tým (DEV tým) je tým vývojářů NAKIT a subdodavatele. Provozní tým (OPS tým) NAKIT, může využít služeb subdodavatelů na konkrétní úkoly na základě smluvního vztahu.

### Technické požadavky

* + Vývojové prostředí DEV NAKIT slouží pro potřeby vývoje a skládá se z AKS (Azure Kubernetes service) a dalších podpůrných serverů jako SQL servery, Redis, Azure Search, Azure Cosmos DB, Azure KeyVault apod. Členům OPS týmu budou předávány funkční SW celky. DEV NAKIT je oficiálním prostředím, které je ekvivalentem k TEST NAKIT. Prostředí samotných vývojářů mimo NAKIT je považováno za nedůvěryhodné pro jakékoliv reklamace, nebo srovnávání funkcionalit a provozu systému.
  + NAKIT GIT prostředí je chápáno jako primární. NAKIT může upravovat zdrojové kódy na základě autorských a licenční práv. Programátoři partnerů jsou zodpovědní za správný kontinuální přenos zdrojových kódů do určených repositářů. Pro hladký vývoj doporučujeme využívat pouze NAKIT GIT prostředí v Azure DevOps s jednotným GIT policy a GIT workflow.
  + Pro dodání binárních artefaktů je určena služba Azure DevOps Artifacts.
  + Základní běhové prostředí všech SW řešení pro projekt ISSI jsou **linuxové** docker kontejnery nasazované do Kubernetes.
  + Základní prostředí pro dohled a sběr telemetrie všech SW řešení je Azure application insights, ke kterým musí mít přístup členové provozu, vývoje a bezpečnosti, aby se tak předešlo případným neshodám ohledně výkonu a stability řešení. NAKIT předpokládá, že logování a sběr telemetrie probíhá dle best practices, dle jednotlivých SW frameworků použitých pro implementaci.
  + NAKIT před produkční prostředí (Stage NAKIT) bude ve stejné konfiguraci jako produkční prostředí.
  + Docker kontejnery musí podporovat non-root běh.
  + Při vytváření vlastních docker image se musí vycházet z oficiálních, digitálně podepsaných docker image ze služby Docker Hub, nebo oficiálního repositáře Microsoft a během procesu docker build je nutné tyto digitální podpisy kontrolovat.
  + Používání docker base image jiné, než oficiální je striktně zakázáno.
  + S každým git commitem musí být spojen ticket v Azure DevOps tak, aby bylo možné identifikovat, kdo a proč modifikoval zdrojové kódy SW řešení. Z těchto ticketů budou automaticky generovány release notes.
  + Git push do master větve bude zakázán. Společně s partnery bude definován Git workflow (např. jako [Git Workflow](https://www.atlassian.com/git/tutorials/comparing-workflows/gitflow-workflow#%3A%7E%3Atext%3DGitflow%20Workflow%20is%20a%20Git%2Cdesigned%20around%20the%20project%20release)) a jmenováni správci jednotlivých větví pro řešení pull requests. Správci mohou být zaměstnanci NAKIT i programátoři partnerů.
  + Release build musí probíhat v prostředí NAKIT Azure DevOps a výsledné docker images musí být podepsány klíči NAKIT a uložené v privátním docker repository odkud jsou nasazovány do prostředí Kubernetes.
  + V kontextu filozofie kultury DevOps jsou všichni členové vývoje a provozu zodpovědní za plynulou kontinuální integraci a kontinuální nasazování SW řešení. Provoz NAKIT připravuje CD/CI pipelines a musí informovat vývojové týmy o procesech automatizace, zprostředkovat logy, spustitelnou dokumentaci neobsahující tajemství (např. Helm šablony pro Kubernetes, ARM šablony pro Azure infrastrukturu apod.) tak, aby byla možná úzká spolupráce a pochopení potřeb a cílů DEV a OPS týmu.
  + Členové DEV týmu kontinuálně během vývoje udržují verze použitých frameworků a SW knihoven třetích stran v aktuálních stable verzích, aby výsledná SW řešení neobsahovala známé bezpečností díry. Využití knihoven třetích stran nesmí porušovat licenční politiku Ministerstva vnitra (např. použití knihovny GNU GPL v.2 by měla negativní dopad na celé dílo).
  + Všechna prostředí v NAKIT (Dev, Test, Stage, Produkce) používají Application Gateway s aktivovanou webovou firewall v blokujícím režimu. DEV tým tak musí implementovat svá řešení v souladu s požadavky OWASP 3.0.
  + Členové OPS týmu kontinuálně udržují všechna aktiva prostředí i SW řešení např. Kubernetes, Redis, Postgresql, Drupal, apod. v aktuálních stable verzích, aby celé prostředí neobsahovalo známé bezpečnostní díry, nebo neporušovalo ISO 27001 dle reportů Azure security center.

#### Požadavek na platformní služby

Při návrhu nových komponent a funkcí je nutné vždy upřednostňovat platformní Azure služby (PaaS, SaaS), které jsou podporované v datacentrech regionů západní, nebo severní Evropa a jsou pokryty adekvátní úrovní SLA v produkčních prostředích (minimálně 99,9 %).

### Přístupy administrátorů a vývojářů

Přístup do vývojového, testovacího, před produkčního, stage a produkčního prostředí s administrátorským oprávněním za účelem řešení problémů, které se projeví jako důležité pro ladění problémů je určené jen pro provozovatele – NAKIT, s. p.

Členové DEV týmu budou mít přístupy do prostředí application insights a databází DEV prostředí. Přístupy na stage a produkční prostředí jsou pro členy DEV týmu implicitně zakázány. V případě závažných incidentů v SW řešeních je možné na základě ticketu v Azure DevOps tato prostředí dočasně zpřístupnit pro analýzu chyb. Nicméně správné logování do Application insigts, které umožňuje proaktivní dohled a velmi detailní analýzu chování celého řešení by mělo tyto potřeby eliminovat na minimum.

#### Ochrana proti vnějším útokům

Aplikace musí být chráněny proti nejčastějším útokům, které byly identifikovány nezávislým společenstvím OWASP ([http://www.owasp.org](http://www.owasp.org/)) tím, že se při vývoji použijí principy definované dle této metodiky v aktuálním znění. Pozornost musí být věnována především následujícím zranitelnostem:A01 Broken Access Control

Řízení přístupu prosazuje zásady tak, aby uživatelé nemohli jednat v rozporu se svými určenými oprávněními. Selhání obvykle vede k neoprávněnému vyzrazení informací, modifikaci nebo zničení všech dat nebo k provedení obchodní funkce mimo omezení uživatele. Mezi běžné chyby řízení přístupu patří např:

* Porušení principu nejmenších oprávnění nebo odepření ve výchozím nastavení, kdy by přístup měl být udělen pouze určitým schopnostem, rolím nebo uživatelům, ale je dostupný komukoli.
* Obcházení kontrol řízení přístupu úpravou adresy URL (manipulace s parametry nebo vynucené procházení), interního stavu aplikace nebo stránky HTML nebo pomocí útočného nástroje upravujícího požadavky API.
* Povolení prohlížení nebo úprav cizího účtu poskytnutím jeho jedinečného identifikátoru (nezabezpečené přímé odkazy na objekty).
* Přístup k rozhraní API s chybějícími kontrolami přístupu pro POST, PUT a DELETE.
* Zvýšení oprávnění. Vystupování jako uživatel bez přihlášení nebo vystupování jako správce při přihlášení jako uživatel.
* Manipulace s metadaty, například přehrání nebo manipulace s tokenem řízení přístupu JSON Web Token (JWT) nebo se souborem cookie či skrytým polem manipulovaným za účelem zvýšení oprávnění nebo zneužití zneplatnění JWT.
* Chybná konfigurace CORS umožňující přístup k API z neautorizovaného/nedůvěryhodného prostředí.
* Vynucení procházení ověřených stránek jako neověřený uživatel nebo privilegovaných stránek jako standardní uživatel.

A02 Cryptographic Failures

Nejdříve je třeba určit potřeby ochrany dat při přenosu a v klidu. Například hesla, čísla kreditních karet, zdravotní záznamy, osobní údaje a obchodní tajemství vyžadují zvýšenou ochranu, zejména pokud se na tyto údaje vztahují zákony o ochraně osobních údajů, např. obecné nařízení EU o ochraně osobních údajů (GDPR), nebo předpisy, např. o ochraně finančních údajů, jako je standard PCI Data Security Standard (PCI DSS). U všech takových údajů:

* Jsou některá data přenášena v otevřeném textu? Týká se to protokolů, jako jsou HTTP, SMTP, FTP, které používají také vylepšení TLS, jako je STARTTLS. Externí internetový provoz je nebezpečný. Ověřte veškerý interní provoz, např. mezi load balancery, webovými servery nebo back-end systémy.
* Používají se nějaké staré nebo slabé kryptografické algoritmy nebo protokoly buď ve výchozím nastavení, nebo ve starším kódu?
* Používají se výchozí kryptografické klíče, jsou generovány nebo opakovaně používány slabé kryptografické klíče nebo chybí řádná správa či rotace klíčů? Jsou šifrovací klíče kontrolovány v úložištích zdrojového kódu?
* Není šifrování vynucováno, např. chybí bezpečnostní směrnice nebo hlavičky HTTP (prohlížeče)?
* Je přijatý certifikát serveru a řetězec důvěryhodnosti řádně ověřen?
* Jsou inicializační vektory ignorovány, opakovaně používány nebo nejsou generovány dostatečně bezpečné pro daný kryptografický režim práce? Je používán nezabezpečený režim provozu, například ECB? Používá se šifrování v případech, kdy je vhodnější autentizované šifrování?
* Používají se hesla jako kryptografické klíče, pokud chybí funkce odvození klíče ze základu hesla?
* Používá se pro kryptografické účely náhodnost, která nebyla navržena tak, aby splňovala kryptografické požadavky? I když je zvolena správná funkce, musí ji vývojář nasadit, a pokud ne, přepsal vývojář zabudovanou funkci silného nasazení seedem, který nemá dostatečnou entropii/nepředvídatelnost?
* Používají se zastaralé hashovací funkce, jako je MD5 nebo SHA1, nebo se v případě potřeby kryptografických hashovacích funkcí používají nekryptografické hashovací funkce?
* Používají se zastaralé kryptografické metody vyplňování, jako je PCKS číslo 1 v1.5?
* Jsou kryptografické chybové zprávy nebo informace postranního kanálu zneužitelné, například formou útoků typu padding oracle?

A03 Injection

Aplikace je zranitelná vůči útoku, pokud:

* Uživatelem zadaná data nejsou aplikací ověřována, filtrována nebo upravována.
* Dynamické dotazy nebo neparametrizovaná volání bez kontextového escapování jsou použity přímo v interpretu.
* Nepřátelská data jsou použita v rámci parametrů vyhledávání ORM (object-relational mapping) k získání dalších citlivých záznamů.
* Nepřátelská data se používají přímo nebo se spojují. SQL nebo příkaz obsahuje strukturu a škodlivá data v dynamických dotazech, příkazech nebo uložených procedurách.

Mezi nejběžnější injektáže patří injektáž SQL, NoSQL, příkaz OS, objektově relační mapování (ORM), LDAP a Expression Language (EL) nebo Object Graph Navigation Library (OGNL). Koncept je u všech interpretů shodný. Kontrola zdrojového kódu je nejlepší metodou, jak zjistit, zda jsou aplikace zranitelné vůči injektážím. Důrazně se doporučuje automatizované testování všech parametrů, hlaviček, adres URL, souborů cookie, datových vstupů JSON, SOAP a XML. Organizace mohou do CI/CD pipeline zahrnout nástroje pro statické (SAST), dynamické (DAST) a interaktivní (IAST) testování zabezpečení aplikací, aby identifikovaly zavedené chyby v oblasti injection ještě před produkčním nasazením.

A04 Insecure Design

Nezabezpečený design je široká kategorie představující různé nedostatky, vyjádřené jako "chybějící nebo neúčinný kontrolní design". Nezabezpečený design není zdrojem pro všechny ostatní kategorie rizik Top 10. Existuje rozdíl mezi nezabezpečeným návrhem a nezabezpečenou implementací. Nedostatky v návrhu a implementaci rozlišujeme z určitého důvodu, mají různé příčiny a způsoby nápravy. I bezpečný návrh může mít vady implementace vedoucí ke zranitelnostem, které mohou být zneužity. Nezabezpečený návrh nelze opravit dokonalou implementací, protože potřebné bezpečnostní kontroly nebyly z definice nikdy vytvořeny na obranu proti konkrétním útokům. Jedním z faktorů, které přispívají k nezabezpečenému návrhu, je nedostatečné profilování obchodních rizik, které je vlastní vyvíjenému softwaru nebo systému, a tedy neschopnost určit, jaká úroveň návrhu zabezpečení je nutná.

Shromážděte a projednejte obchodní požadavky na aplikaci s podnikem, včetně požadavků na ochranu důvěrnosti, integrity, dostupnosti a autenticity všech datových aktiv a očekávané obchodní logiky. Vezměte v úvahu, jak bude aplikace vystavena riziku a zda potřebujete oddělení uživatelů (navíc k řízení přístupu). Sestavte technické požadavky včetně funkčních a nefunkčních požadavků na zabezpečení. Naplánujte a vyjednejte rozpočet pokrývající všechny činnosti spojené s návrhem, sestavením, testováním a provozem, včetně bezpečnostních činností.

Bezpečný návrh je kultura a metodika, která neustále vyhodnocuje hrozby a zajišťuje, že kód je robustně navržen a testován tak, aby zabránil známým metodám útoku. Modelování hrozeb by mělo být začleněno do upřesňovacích sezení (nebo podobných činností); hledejte změny v datových tocích a řízení přístupu nebo jiných bezpečnostních kontrolách. Při vývoji uživatelského scénáře určete správné toky a stavy selhání, zajistěte, aby byly dobře pochopeny a odsouhlaseny odpovědnými a dotčenými stranami. Analyzujte předpoklady a podmínky pro očekávané a chybové toky, ujistěte se, že jsou stále přesné a žádoucí. Určete, jak ověřit předpoklady a prosadit podmínky potřebné pro správné chování. Zajistěte, aby výsledky byly zdokumentovány v příspěvku uživatele (user story). Poučte se z chyb a

nabídněte pozitivní pobídky na podporu zlepšení. Bezpečný návrh není doplněk ani nástroj, který můžete přidat do softwaru.

Bezpečný software vyžaduje bezpečný životní cyklus vývoje, určitou formu bezpečného návrhového vzoru, metodiku zpevněné cesty, knihovnu zabezpečených komponent, nástroje a modelování hrozeb. Obraťte se na odborníky na bezpečnost na začátku softwarového projektu v průběhu celého projektu a údržby softwaru. Zvažte využití modelu vyspělosti OWASP Software Assurance Maturity Model (SAMM), který vám pomůže strukturovat vaše úsilí o bezpečný vývoj softwaru.

A05 Security Misconfiguration Aplikace může být zranitelná, pokud:

* Chybí vhodné posílení zabezpečení v kterékoli části aplikačního stacku nebo jsou nesprávně nakonfigurována oprávnění ke cloudovým službám.
* Jsou povoleny nebo nainstalovány nepotřebné funkce (např. nepotřebné porty, služby, stránky, účty nebo oprávnění).
* Výchozí účty a jejich hesla jsou stále povoleny a nezměněny.
* Zpracování chyb odhaluje uživatelům stack traces nebo jiná příliš informativní chybová hlášení.
* U aktualizovaných systémů jsou nejnovější bezpečnostní funkce zakázány nebo nejsou bezpečně nakonfigurovány.
* Nastavení zabezpečení v aplikačních serverech, aplikačních frameworcích (např. Struts, Spring, ASP.NET), knihovnách, databázích atd. nejsou nastavena na bezpečné hodnoty.
* Server neposílá bezpečnostní hlavičky nebo směrnice nebo nejsou nastaveny na bezpečné hodnoty.
* Software je zastaralý nebo zranitelný

A06 Vulnerable and Outdated Components Pravděpodobně jste zranitelní:

* Pokud neznáte verze všech používaných komponent (na straně klienta i serveru). To zahrnuje komponenty, které používáte přímo, i vnořené závislosti.
* Pokud je software zranitelný, nepodporovaný nebo zastaralý. To zahrnuje operační systém, webový/aplikační server, systém správy databází (DBMS), aplikace, rozhraní API a všechny komponenty, běhová prostředí a knihovny.
* Pokud pravidelně nekontrolujete zranitelnosti a neodebíráte bezpečnostní bulletiny týkající se používaných komponent.
* Pokud neopravujete nebo neaktualizujete základní platformu, frameworky a závislosti včas a s ohledem na rizika. To se běžně stává v prostředích, kde je oprava měsíčním nebo čtvrtletním úkolem v rámci řízení změn, čímž se organizace dostávají do situace, kdy jsou dny nebo měsíce zbytečně vystaveny opraveným zranitelnostem.
* Pokud vývojáři softwaru netestují kompatibilitu aktualizovaných, upgradovaných nebo opravených knihoven.
* Pokud nezabezpečí konfigurace komponent.

A07 Identification and Authentication Failures

Potvrzení identity uživatele, ověřování a správa session jsou klíčové pro ochranu před útoky souvisejícími s ověřováním. Slabiny v ověřování mohou nastat, pokud aplikace:

* Umožňuje automatizované útoky, jako je například "credential stuffing", kdy má útočník k dispozici seznam platných uživatelských jmen a hesel.
* Umožňuje útoky hrubou silou nebo jiné automatizované útoky.
* Povoluje výchozí, slabá nebo dobře známá hesla, například "Password1" nebo "admin/admin".
* Používá slabé nebo neúčinné procesy obnovy pověření a zapomenutých hesel, například "odpovědi založené na znalostech", které nelze zabezpečit.
* Používá datová úložiště s prostým textem, šifrovanými nebo slabě hashovanými hesly.
* Má chybějící nebo neúčinné vícefaktorové ověřování.
* Vystavuje identifikátor relace v adrese URL.
* Opakovaně používá identifikátor relace po úspěšném přihlášení.
* Nezneplatňuje správně identifikátory session. Relace uživatele nebo autentizační tokeny (především tokeny jednotného přihlášení (SSO)) nejsou správně zneplatněny během odhlášení nebo období nečinnosti.

A08 Software and Data Integrity Failures

Selhání integrity softwaru a dat souvisí s kódem a infrastrukturou, které nechrání před porušením integrity. Příkladem je situace, kdy aplikace spoléhá na zásuvné moduly, knihovny nebo moduly z nedůvěryhodných zdrojů, úložišť a sítí pro doručování obsahu (CDN). Nezabezpečený CI/CD pipeline může představovat potenciál pro neoprávněný přístup, škodlivý kód nebo kompromitaci systému. A konečně, mnoho aplikací dnes obsahuje funkci

automatických aktualizací, kdy jsou aktualizace stahovány bez dostatečného ověření integrity a aplikovány na dříve důvěryhodnou aplikaci. Útočníci by mohli potenciálně nahrát vlastní aktualizace, které by byly distribuovány a spuštěny na všech instalacích. Dalším příkladem je situace, kdy jsou objekty nebo data zakódovány nebo serializovány do struktury, kterou může útočník vidět a modifikovat, je zranitelná nezabezpečenou deserializací.

A09 Security Logging and Monitoring Failures

Tato kategorie má pomoci odhalit, eskalovat a reagovat na aktivní narušení. Bez logování a monitorování nelze narušení odhalit. K nedostatečnému protokolování, detekci, monitorování a aktivní reakci dochází kdykoli:

* Události, které lze auditovat, jako jsou přihlášení, neúspěšná přihlášení a transakce s vysokým objemem, nejsou zaznamenávány.
* Výstrahy a chyby negenerují žádné, nedostatečné nebo nejasné zprávy logu.
* Protokoly aplikací a rozhraní API nejsou monitorovány z hlediska podezřelých aktivit.
* Protokoly jsou ukládány pouze lokálně.
* Nejsou zavedeny vhodné prahové hodnoty pro upozornění a procesy eskalace reakce nebo nejsou účinné.
* Penetrační testy a skenování pomocí nástrojů pro dynamické testování bezpečnosti aplikací (DAST) (například OWASP ZAP) nevyvolávají výstrahy.
* Aplikace nemůže detekovat, eskalovat nebo upozorňovat na aktivní útoky v reálném čase nebo téměř v reálném čase.

Jste zranitelní vůči úniku informací tím, že události protokolování a výstrah jsou viditelné pro uživatele nebo útočníka.

A10 Server Side Request Forgery (SSRF)

K chybám SSRF dochází vždy, když webová aplikace načítá vzdálený prostředek bez ověření uživatelem zadané adresy URL. Útočník tak může aplikaci přimět k odeslání vytvořeného požadavku na neočekávané místo určení, a to i v případě, že je chráněna bránou firewall, sítí VPN nebo jiným typem řízení přístupu (ACL).

Vzhledem k tomu, že moderní webové aplikace poskytují koncovým uživatelům pohodlné funkce, stává se načítání adresy URL běžným scénářem. V důsledku toho se zvyšuje výskyt SSRF. Také závažnost SSRF je stále vyšší v důsledku cloudových služeb a složitosti architektur.

Kromě aktuálních OWASP TOP10 je třeba věnovat pozornost také zranitelnostem, které se v tomto žebříčku umístily v minulých letech.

* XML External Entities (XXE): Mnoho starších nebo špatně nakonfigurovaných procesorů XML vyhodnocuje odkazy na externí entity v dokumentech XML. Externí entity mohou být použity k odhalení interních souborů pomocí jejich URI, interního sdílení souborů, skenování interních portů, vzdálenému spuštění kódu a útokům typu Denial of Service.
* Cross-Site Scripting XSS: K chybám XSS dochází vždy, když aplikace zahrne nedůvěryhodná data do nové webové stránky bez řádné validace nebo escapování nebo aktualizuje existující webovou stránku s daty poskytnutými uživatelem pomocí rozhraní API prohlížeče, které může vytvářet HTML nebo JavaScript. XSS umožňuje útočníkům spustit v prohlížeči oběti skripty, které mohou unést uživatelské relace, poškodit webové stránky nebo přesměrovat uživatele na škodlivé stránky.
* Cross Site Request Forgery: CSRF je technika, která umožňuje útočníkovi podvrhnout formulář na jiné stránce nebo pomocí některých HTTP metod přesměrovat prohlížeč oběti na skript zpracovávající legitimní formulář aplikace s daty, která můžou oběť poškodit.
* Nezabezpečené přesměrování: Využívá nezabezpečených přesměrování v aplikacích (redirect a froward) k tomu, aby z důvěryhodné stránky přesměrovala nic netušícího uživatele na stránku škodlivou.

Aplikace nesmí obsahovat žádné zranitelnosti, které jsou klasifikované jako střední, vysoké a kritické. O závažnosti jednotlivých zranitelností rozhoduje bezpečnostní manažer NAKIT.

#### Pravidla XML komunikace

Při použití XML komunikace by měly být prováděné tyto kontroly:

* + - Početní a délkové limity:
      * maximální počet atributů v elementu
      * maximální počet namespaces, namespace prefixů a obecně všech lokálních jmen v XML dokumentu
      * maximální délka jména elementu
      * maximální délka jména atributu
      * maximální délka identifikátoru namespace (URI)
    - Znakové sady:
      * konzistence deklarací (atribut „charset“ v HTTP request hlavičce „Content-Type“, BOM na začátku dat a atribut „encoding“ v hlavičce XML)
      * přítomnost netisknutelných znaků
    - Escaping:
      * escaping validních znaků (např. „&#x41;“ místo „A“, též např. „&#x42f;“ místo „Я“, pokud je použitý encoding některý z UTF apod.)
      * použití znaku „&“ mimo escape sekvenci
      * použití znaků „““ (uvozovky – ASCII 34), „’“ (apostrof – 39), „<“ a „>“ mimo místa, kde mají syntaktický význam
      * kontrola správného ohraničení CDATA sekcí (pokud se vůbec mohou vyskytovat, pokud ne, tak rovnou odmítat XML zprávy, které CDATA obsahují)
    - Přítomnost XML External Entity v DTD

#### JSON formát

Při použití JSON formátu pro výměnu externích dat (neplatí pro API v aplikaci) by měly být prováděné minimálně tyto kontroly:

* + - maximální velikost zprávy
    - maximální délka názvu klíče
    - neunikátní klíče
    - maximální počet elementů
    - maximální úroveň vnoření
    - maximální velikost pole (myšleno array, nikoli field)
    - komentáře, pokud jsou zakázané nebo limitované velikostí
    - limit objemu whitespace (tabulátory, mezery, odřádkování)
    - kontrola striktní syntaxe a struktury JSON dokumentu (některé parsery v aplikacích ledacos tolerují)
    - kontrola kanonické formy nebo provedení kanonizace (pokud je požadována)
    - kontrola obsahu (jména klíčů, hodnoty) na sekvence XSS či SQLi (s možností vypnout per element – nemusí být datově transparentní a někdy může hodnota naopak záměrně obsahovat renderované HTML)
    - provádí se kontrola syntaxe kódu JSON – parser pro RFC4627
    - validace key value, metoda zjišťuje, zda hodnoty použité v key value odpovídají typu definované hodnoty (numeric,boolean apod.)

### Pravidla logování

Základní prostředí pro dohled a sběr telemetrie všech SW řešení jsou Azure application insights, ke kterým musí mít přístup členové provozu, vývoje a bezpečnosti, aby se tak předešlo případným neshodám ohledně výkonu a stability řešení.

Projekty mohou využívat např. Google analytics pro vyhodnocování chování uživatelů na webových portálech. Google analytics se nesmí používat v privátní transakční části systému.

NAKIT předpokládá, že logování a sběr telemetrie probíhá dle best practices dle jednotlivých SW frameworků použitých pro implementaci SW řešení.

Logování SW řešení dodávaných partnery by se mělo nést v duchu, že logy jsou psány pro potřeby oddělení provozu a bezpečnosti (nikoli pouze pro debuggovací potřeby programátorů). Všichni členové týmu vývoje, provozu i bezpečnosti musí na základě informace z logu identifikovat a vyřešit problém.

Neošetřené výjimky, nebo informace v logu typu „došlo k neočekávané chybě“, ačkoli programátor mohl a měl specifikovat konkrétní chybu např. nedostupnosti prostředí třetích stran, vypršení certifikátu, nevalidní vstupní data apod, je projevem nekvalitního exception handlingu a NAKIT může vyzvat subdodavatele k nápravě.

Umožnit nastavení úrovně logování – například:

* Verbose, Debug, Info, Warn, Error, Fatal

Součástí logování musí být partnery definovaná a NAKIT předaná politika exception handling hlavně z důvodu, aby obsahem logů na produkci nebyla data obsahující tajemství (např. hesla, šifrovací klíče, emailové adresy, a další atributy citlivé dle GDPR).

Pokud existují záznamy, které je nutné logovat a zároveň podléhají GDPR je nutné tyto aspekty definovat v politice logování a exception handling a poskytnout členům OPS týmu tak, aby proces NAKIT popsal způsoby bezpečného ukládání a zpracování takovýchto informací.

Soupis specifických ID možných chyb s popisem musí být součástí programátorské dokumentace kontinuálně předávané členům OPS týmu.

### Požadavky na zaznamenávání událostí, jeho uživatelů a administrátorů

1. Jednoznačnou síťovou identifikaci zařízení původce, je-li v komunikační síti použit nástroj, který mění jeho síťovou identifikaci.
2. Sběr informací o bezpečnostních a provozních událostech; zejména zaznamenává:
   * datum a čas včetně specifikace časového pásma
   * typ činnosti
   * identifikaci technického aktiva, které činnost zaznamenalo
   * jednoznačnou identifikaci účtu, pod kterým byla činnost provedena
   * jednoznačnou síťovou identifikaci zařízení původce a
   * úspěšnost nebo neúspěšnost činnosti
3. Ochranu informací získaných podle písmen a) a b) před neoprávněným čtením a jakoukoli změnou.
4. Zaznamenávání:
   * přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů
   * činností provedených administrátory
   * úspěšné i neúspěšné manipulace s účty, oprávněními a práv
   * neprovedení činností v důsledku nedostatku přístupových práv a oprávnění
   * činností uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému
   * zahájení a ukončení činností technických aktiv
   * kritických i chybových hlášení technických aktiv
   * přístupů k záznamům o událostech, pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí

Logy se ukládají v prostředí Azure Log analytics po dobu 18 měsíců a jsou zároveň zasílány do DCeGOV (Dohledové centrum eGovernmentu).

### Dokumentace

* 1. ***Dokumentace při vytvoření díla***

## Bezpečnostní politika

* + - * musí být v souladu s VyKB
      * musí být v souladu s požadavky ISMS MV

#### Dokumentace k integraci řešení

* datové toky
* použité protokoly
* architektonický nákres komponent a jejich spolupráce
* diagram logického a fyzického zapojení

#### Systémová příručka

* Popis funkcí, včetně bezpečnostních, které používá správce systému pro provádění určených činností v informačním systému veřejné správy a návod na používání těchto funkcí.
* Parametry kvality vycházejí z požadavků na kvalitu.
* Podrobný popis IS nebo odkaz na dokument, ve kterém je popis uveden.
* Popis jednotlivých činností vykonávaných při správě IS, včetně činností definovaných pro role, určení fyzických osob, které tyto činnosti vykonávají a oprávnění nezbytných pro výkon těchto činností.
* Definování uživatelů nebo skupin uživatelů a jejich oprávnění a povinnosti při využívání aplikace.

#### Uživatelské příručky

* Uživatelská příručka

#### Provozní deník

Provozní deník je vedený v Azure DevOps v podobě ticketu typu service book.

#### Systém řízení dokumentů a záznamů

Provádí se dle **ISMS 02.03.01 Řízení dokumentů a záznamů**

### Zdrojový kód

Součástí dokumentace SW řešení je i vývojářská dokumentace v podobě doplňujících komentářů uvnitř funkcí, metod a popisů tříd.

Každý z programátorských jazyků má své best practice ohledně pojmenovávání tříd, atributů, názvu tříd a proměnných i postupů při programátorské dokumentaci. Společně s partnery budou tyto best practice kodifikovány jakožto závazné postupy dokumentace a tvorby SW.

Komentáře jsou součásti [syntaktických](https://cs.wikipedia.org/wiki/Syntaktick%C3%A1_anal%C3%BDza) pravidel zápisu programu v mnoha [programovacích](https://cs.wikipedia.org/wiki/Programovac%C3%AD_jazyk) [jazycích](https://cs.wikipedia.org/wiki/Programovac%C3%AD_jazyk). Komentář se vkládá před nebo za část [zdrojového kódu](https://cs.wikipedia.org/wiki/Zdrojov%C3%BD_k%C3%B3d) (např. příkaz, metodu, třídu), jehož funkci nebo význam je potřeba vysvětlit. Používání komentáře není povinné, umožňuje však napomoci k pochopení činnosti [programu](https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_program). Komentář nemá popisovat, co program dělá (protože to vyplývá ze zápisu programu), ale proč to dělá. Komentáře obecně mohou velmi usnadnit pochopení činnosti programu, mohou mít samo-dokumentující funkci. Syntaxe a pravidla pro přidávání komentářů budou dle konkrétního programovacího jazyka.

Kromě komentářů ve zdrojových kódech je zdrojový kód rovněž navázán na vývojářskou dokumentaci, obsahující popis konceptu a fungování každého bloku, tj. zdrojový kód každé komponenty je identifikován v příslušném schématu a popisu ve shodné jmenné konvenci.

Dokumentace rovněž obsahuje:

* podrobný popis konfiguračních parametrů vč. jejich formátu
* popis použitých API
* popis vazeb mezi jednotlivými komponentami
* seznam chybových kódů a jejich význam
* další nezbytné prvky, jako např. certifikáty, šifrovací klíče, logované údaje Požadavky na vývoj:
* Vyvíjená komponenta / aplikace musí splňovat požadavky Cloud native.
  + Definice cloud native: [Defining Cloud Native | Microsoft Docs](https://docs.microsoft.com/en-us/dotnet/architecture/cloud-native/definition)
  + Oficiální popis Cloud native nadace Cloud native computing foundation: [CNCF](https://github.com/cncf/foundation/blob/master/charter.md)
* Konfigurační soubory a tajemství nejsou součástí zdrojového kódu ani databáze. Předávají se do běhového prostředí přes environment variables
* Certifikáty a hesla jsou uloženy v chráněném úložišti (např. Kubernetes secrets, Azure key vault, apod.).
* Soubory (dokumenty, přílohy apod.) se neukládají do transakční databáze.
* U nových komponent / aplikace jsou součástí dodávky zdokumentovány Unit testy.
* Součástí dodávky jsou FAT testy a jejich výsledky.
* Každý kontejner / mikroslužba musí obsahovat API pro Kubernetes readiness a liveness probes.
* Sběr telemetrie přes Azure application Insights probíhá od prvních řádek kódu.
* Vyvíjené komponenty jsou multilplatforní a docker images musí podporovat non-root běh.
* Každá komponenta má healt-check pro její dohled a je implementován jako REST volání.

### Pravidla a chování Git, obecný flow vývoje

Projekt manažer nebo produkt manažer pravidelně aktualizuje plán release.

Ke každé release oddělení testování vytváří testovací protokol a uloží na SHP NAKIT.

Požadavky na zřízení přístupu do Azure DevOps se zasílají na PM.

#### Nové požadavky

Na základě požadavků MV projektový, nebo produktový manažer zřizuje v Azure DevOps tickety typu **Epic, Feature, Enhacement**. Epic slouží pro velké požadavky, který je dále rozdělen na jednotlivé **Feature.**

Jednotlivé požadavky jsou předány k vytvoření zadání a jsou ve stavu **Analyse.** Po vyjasnění zadání a provedení připomínkovacího řízení, PM požadavek předá k provedení odhadů pracnosti team leaderům a team leaderu subdodavatele. Po schválení od MV, PM požadavek zařadí do release plánu (plánované iterace) a předán subdodavateli. Subdodavatel potvrdí převzetí v release a nastaví jeho stav na **Active.** Po vyřešení a vložení zdrojového kódu do GITu, nastaví subdodavatel jeho stav na **Resolved**. Provozní podpora po schválení nasazení nasadí do prostředí DEV, nastaví stav na **ToTest** a přiřadí na vedoucího oddělení testování NAKIT, který přiřadí na konkrétního testera.

Po úspěšném otestování v prostředí **DEV**, tester nastaví stav chyby na **Tested DEV.** V případě chyby tester vrátí řešiteli a nastaví stav na Active.

PM po rozhodne o nasazení na Stage, provozní podpora nasadí na Stage a rozešle informaci, že je nová verze na Stage nasazena k testování Po úspěšném otestování v prostředí Stage, tester nastaví stav na **Tested Stage**. V případě chyby tester vrátí řešiteli a nastaví stav na **Active.**

Po nasazení do produkce a úspěšném otestování v produkčním prostředí, tester nastaví stav na **TestedProd**. V případě chyby tester vrátí řešiteli a nastaví stav na **Active.** PM po nasazení do produkce zkontroluje obsah release na nastaví na stav **Close.**

* 1. ***Řešení nahlášených incidentů***

## Zaevidování chyby

Chyby v **produkci** zaslané na email zaeviduje služba podpory provozu v Azure DevOps označí štítkem **PROD**, do názvu tiketu uvede: „Zkratku názvu projektu “\_“Zkratku prostředí“**:** Vyplní vždy kategorii (A, B, C, D), Device description (jeli známo) a číslo release. Dle povahy chyby předá na teamleadera řešitelů.

Chyby z **vývoje** zaslané na email, například z MV ČR, zaeviduje podpora provozu v Azure DevOps označí štítkem prostředí (DEV/ Stage), do názvu tiketu uvede **ISSI\_DEV** nebo **Stage**. Dále vyplní device description a kategorii chyby. **Dále bude uvedeno, jestli chyba vznikla neotestováním u partnerů při vývoji.** Dále musí být vyplněno Related, určení tasku, se

kterým souvisí. Chyby zjištěné oddělením testování NAKIT testeři zaevidují v Azure DevOps s vyplněním všech atributů. Všechny chyby jsou nejdříve přiděleny na PM. PM přidělí k řešení.

Chyba je ve stavu **New**.

## Proces odstraňování chyby

Řešitel převezme chybu a nastaví její stav na **Analyse**.

Po vyřešení chyby, kdy dojde k nastavení parametrů nebo release nastaví stav na **Resolve**. V případě, že je nutné nasadit opravu je nutné zaslat informaci na OPS tým Nakit. Provoz nasadí na DEV a po nasazení nastaví chybu do stavu **To Test** a přiřadí na testera.

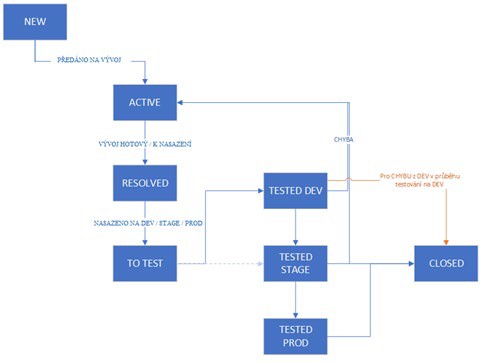
Po úspěšném otestování v prostředí DEV, tester nastaví stav chyby na **Tested DEV**. V případě chyby tester vrátí řešiteli a nastaví stav na **Active.**

Po úspěšném otestování v prostředí Stage, tester nastaví stav chyby na **Tested Stage.**

V případě chyby tester vrátí řešiteli a nastaví stav na **Active.**

Po nasazení do produkce a úspěšném otestování v prostředí, tester nastaví stav chyby na **Close**. V případě chyby tester vrátí řešiteli a nastaví stav na **Active.**

## Workflow odstranění chyby



#### Změnové požadavky

Zadávat vlastní nápady na vylepšení, které neprošli nějakým všeobecným odsouhlasením, jsou zadané jako **Issue** do Azure DevOps a jsou přiřazené na Projektového/Produktového manažera.

Postup:

1. Pokud se nápad **neodsouhlasí**, Projektový/Produktový manažer napíše komentář k **Issue**

proč a zavře jej – stav **CLOSED**.

1. Pokud se nápad **odsouhlasí:**
   1. Projektový/produktový manažer Issue přenastaví na typ **Enhacement**, změní stav na

**ANALYSE** a přiřadí jej na analytika.

* 1. Analytik projde případné další souvislosti a bude-li třeba, dopíše analýzu. Provede připomínkové řízení a po vypořádání připomínek předá na PM.
  2. PM provede nacenění, odsouhlasení vlastníka systému a zařazení do verze. Další postup dle kapitoly [6.1](#_bookmark29) této přílohy - „Nové požadavky“.

#### Dodržování jmenné konvence v Azure DevOps

TITLE=název – Chceme mít možnost je filtrovat podle kategorií. První slovo dle jednotlivých bodů rozdělení. Druhé slovo bude oblast v projektu, abychom to dobře roztřídili /důležité je nedělat překlepy/. To je důležité hlavně u požadavků, které se nebudou řešit hned. Prostředí bude v názvu požadavku specifikováno pouze pokud se bude jednat o

TEST prostředí nové ISSI (např. testování formuláře metodiky).

**Např.** nový ISSI: TEST-Formuláře-metodika chybný odkaz

V detailu popisku požadavku bude vložena vždy URL adresa stránky, na které se bug/enhancement vyskytl.

### Unit testování a pravidla přístupnosti

V souladu s normou WCAG 2.1, a zákonem č. 99/2019 Sb., o přístupnosti internetových stránek a mobilních aplikací a o změně zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů.

Kontroluje dodavatel front endu a vždy s každou release potvrdí, že je release v souladu s pravidly.

### Bezpečnost

* 1. ***Bezpečný vývoj***

## Minimální bezpečnostní požadavky na vývoj aplikací z hlediska jejich kritičnosti

Při vývoji softwarové aplikace musí být splněna řada bezpečnostních opatření, která mají vliv zajištění vysokého stupně důvěrnosti, dostupnosti a integrity informací v nich obsažených. Externí dodavatelé i interní vývoj musí splnit sadu opatření obsažených ve standardu [OWASP Application Security Verification Standard](https://owasp.org/www-project-application-security-verification-standard/).

Představuje seznam požadavků či testů z oblasti aplikační bezpečnosti, který je využitelný architekty, vývojáři, testery, bezpečnostními specialisty, výrobci nástrojů a uživatele (konzumenty) aplikací pro definování, vývoj a testování bezpečných aplikací.

Požadavky jsou členěny do 14 sekcí, kdy jednotlivé požadavky jsou doporučeny pro aplikace s nízkým (L1), středním (L2) a vysokým dopadem či hodnotou (L3) pro zákazníka.

Zmíněné oblasti požadavků ve standardu:

* + - 1. Ověřovací požadavky na architekturu, návrh a modelování hrozeb
      2. Ověřovací požadavky na autentizaci
      3. Ověřovací požadavky na správu relací
      4. Ověřovací požadavky na řízení přístupu
      5. Ověřovací požadavky na validaci, ošetřování a kódování
      6. Ověřovací požadavky na uloženou kryptografii
      7. Ověřovací požadavky na řízení chyb a logování
      8. Ověřovací požadavky na ochranu dat
      9. Ověřovací požadavky na komunikace
      10. Ověřovací požadavky na škodlivý kód
      11. Ověřovací požadavky na business logiku
      12. Ověřovací požadavky soubory a zdroje
      13. Ověřovací požadavky na API a webové služby
      14. Ověřovací požadavky na konfigurace

Dodavatel bude při vývoji, testování a nasazení aplikace naplňovat doporučené požadavky dle definované kritičnosti vyvíjené aplikace (L1, L2 nebo L3).

Každá vyvíjená softwarová aplikace musí splňovat specifické náležitosti a postupy během jejího vývoje. Detail a záběr bezpečnostních požadavků v každé fázi se odvíjí od míry citlivosti či kritičnosti dané aplikace.

Aplikace lze z pohledu potenciálního negativního dopadu při narušení bezpečnosti klasifikovat do 3 kategorií.

1. Kritická (L3) – významná aplikace, jejíž nedostupnost, narušení integrity nebo důvěrnosti by ohrozilo reputaci organizace nebo by plynuly významné finanční postihy. Aplikace nakládá s citlivými, osobními či jinak strategickými údaji a jejich ohrožení (zcizení, zveřejnění) může narušit chod (většiny) klíčových business procesů organizace. Je třeba klást nejvyšší možná bezpečnostní opatření na takovou aplikaci v oblasti důvěrnosti, integrity a dostupnosti.
2. Střední (L2) – aplikace, která nakládá s částečně citlivými či strategickými informacemi, jejichž zveřejnění bych vzhledem k povaze či kvantitě neohrozilo významným dopadem chod organizace či některého business procesu. Narušení její důvěrnosti, integrity nebo dostupnosti bude mít dopad na některé klíčové procesy, ale bez kritického dopadu na chod celé organizace či ohrožení reputační nebo finanční stability.
3. Základní (L1) – aplikace, která nenakládá s citlivými ani strategickými informacemi a nemá dopad na chod organizace. V případě narušení její důvěrnosti, integrity nebo dostupnosti se to nijak nedotkne klíčových procesů, pouze podpůrných s méně zřejmým přímým vlivem na hlavní procesy.

## Praktiky a zásady bezpečného vývoje a standardy při programování

* Aplikace standardů a konvencí – Jakmile budou přijata rozhodnutí o použitých technologiích, musí být vytvořeny, udržovány a sděleny příslušné vývojové standardy a konvence, které podporují jak psaní bezpečného kódu, tak opětovné použití vestavěných bezpečnostních funkcí a schopností.
* Používejte opakovaně vestavěné funkce zabezpečení ve vybraných vývojových frameworcích a nástrojích a zajistěte, aby byly ve výchozím nastavení zapnuté. To pomůže všem vývojářům řešit známé třídy problémů, a to systémově nikoli dle individuálního uvážení.
* Jakékoli použití frameworků / knihoven / komponent by mělo být v co nejmenší míře spojeno, aby je bylo možné v případě potřeby snadno vyměnit / upgradovat.
* Standardy musí být vynutitelné a realizovatelné
* Maximálně automatizujte revize kódu na zranitelnosti pro zefektivnění a zrychlení kontroly (minimálně v rozsahu OWASP Top 10)

## Bezpečné funkce

1. Zajistěte předpis (ne)povolených a kontrolu použitých funkcí dle použitého jazyka (Java, PHP, .NET) včetně doporučených ekvivalentů k těmto funkcím. Některé dynamické jazyky používají nebezpečné funkce generované v rámci běhové prostředí a jsou zdrojem zranitelností ([referenční seznam CWE Top 25](https://cwe.mitre.org/top25))
2. Využívejte statické analyzátory kódu, případně nástroje typu RASP (Runtime application self-protection), které mají kontextový vhled do volání funkcí uvnitř běžící aplikace. RASP zvyšuje bezpečnost softwaru sledováním jeho vstupů a blokováním těch, které by mohly umožnit útok, a zároveň chrání runtime prostředí před nežádoucími změnami a neoprávněnými zásahy. Chráněné aplikace spoléhají méně na externí zařízení, jako jsou firewally, aby poskytovaly ochranu zabezpečení v běhovém prostředí. RASP může být integrován jako framework nebo modul běžící ve spojení s programovým kódem, knihovnami a systémovými voláními.
3. Další metodou ochrany před zanesením kódu je integrace analyzátoru přímo do IDE nebo kontroly v rámci CI/CD při sestavování aplikace.
4. Používejte aktuální verze kompilátoru a nástrojů vývojové linky a bezpečné předvolby kompilátoru (např. ochrana před buffer overruns a underruns v podobě ochrany při kompilaci a v běhovém prostředí proti chybám poškození paměti)

## Bezpečné nakládání s daty

* Všechny uživatelské vstupy musí být považovány za nedůvěryhodné, proto využívejte striktní validaci vstupů od klienta, parametrizujte dotazy do databáze. Každá vrstva aplikační architektura by měla mít svou vlastní ochranu
* Kromě validace vstupů zvažte dle využitého kontextu vynutitelnost segregace dat, čímž zamezíte, aby se data stala součástí aplikační logiky
  + - 1. Kódování, které zajišťuje, že data jsou transformována tak, aby byla interpretována čistě jako data v kontextu, kde se používají
      2. Data binding zabraňuje interpretaci dat v podobě kontrolní logiky svázáním se specifickým datovým typem
* Jako prevenci před obejitím některých bezpečnostních filtrů zvažte použití kanonizace. Při rozhodování o bezpečnosti uživatelských vstupů by mělo být veškeré dekódování (decode) provedeno nejprve pomocí příslušných API, dokud nebude vyřešeno veškeré kódování (encode). Dále musí být vstup kanonizován a poté validován. Vstup po kanonizaci by měl být ověřen a buď přijat, nebo odmítnut. Teprve po kanonizaci může být učiněno rozhodnutí.
* Vstup z nedůvěryhodných zdrojů by měl být vždy ošetřen, a pokud jsou k dispozici, měly by být použity metody ošetření a validace poskytované komponentami, protože ošetření vytvořená na míru mohou často přehlédnout skryté složitosti.

## Řízení bezpečnostních rizik souvisejících s komponentami třetích stran

Použité komponenty třetích stran musí projít evidencí a kontrolou minimálně v tomto rozsahu:

* Vést seznam použitých komponent s unikátně identifikovaným číslem komponenty
* Vyhodnotit bezpečnostní rizika vůči známým zranitelnostem
* Zmírněte riziko aktualizacemi, záplatami nebo náhradou komponenty, popřípadě přijměte riziko
* Monitorujte změny a nové zranitelnosti, které se mohou u použitých komponent vyskytovat

## Testování a validace kódu

Využívejte maximálně automatizované testování za podpory kombinace nástrojů typu:

* Static Analysis Security Testing (SAST) - kontrola nedostatků zdrojového kódu nebo kompilovaného mezijazyka nebo binární komponenty. Hledá

známé problematické vzory v kódu založené pouze na aplikační logice, nikoli na chování aplikace při jejím spuštění

* + Kontrola na výskyt zranitelností během sestavování aplikace nebo rovnou během psaní kódu
  + SAST nepokrývá detekci zranitelností v business logice, problémy zavedené na více úrovních aplikace nebo třídy problémů vytvořené za běhu.
* Dynamic Analysis Security Testing (DAST) - testování předpřipravených útoků vůči plně běžící (kompilované) aplikaci s veškerou integrací potřebných komponent (podpora testování aplikace napsané i v jazyce nepodporovaném SAST nástrojem nebo v případech kdy aplikace využívá externích volání webových služeb nebo Javascript knihoven uložených mimo repozitář kódu)
* Fuzzing - mnohonásobné variabilní generování nebo mutace dat a jejich předání aplikačním data parserům (síťové protokoly, souborové, IPC). Dobré pokrytí kontroly kódu, zejména pro C, C++
* Software composition analysis (SCA) - zabývá se správou používání komponent s otevřeným zdrojovým kódem. Nástroje SCA provádějí automatické skenování kódové základny aplikace včetně souvisejících artefaktů, jako jsou kontejnery a registry, s cílem identifikovat všechny komponenty s otevřeným zdrojovým kódem, údaje o jejich souladu s licencemi a případné bezpečnostní zranitelnosti.
* K ověřování konfigurací a zmírnění rizik provozních platforem – využívejte ochranu před útoky na bázi mitigací OS:
  + ASLR (Address Space Layout Randomization)
  + DEP (Data Execution Prevention)
  + CFG (Control Flow Guard)
  + Služby a nástroje ověřující že webová stránka podporuje záhlaví HTTP související s bezpečností, jako jsou x-frame-options, politika zabezpečení obsahu, HSTS, zabezpečené a http Only cookie flagy, a že konfigurace SSL / TLS na serveru je bez nepodporovaných a zranitelných / nepodporovaných verzí protokolu a šifrovacích sad.
* Automatické funkční testování bezpečnostních požadavků a vlastností aplikace
  + Rozšiřte standardní unit testy o testování bezpečnostních vlastností stejně jako testujete standardní funkční vlastnosti aplikace.

#### Penetrační testy

(provádění penetračních testů není předmětem plnění, ledaže je tak výslovně stanoveno)

Bezpečnostní testy budou součástí rozvojových smluv mezi MV a NAKIT. Budou se provádět v souladu s požadavky § 13 VyKB. Vzhledem k trvalému vývoji minimálně dvakrát (2x) ročně za součinnosti Sekce bezpečnosti NAKIT, pokud MV jako správce systému nerozhodne jinak.

Provádění bezpečnostních testů se řídí § 25 VyKB. Bezpečnostní testy (vulnerability) testy je pak v souladu s výše uvedeným paragrafem nutné provést v souvislosti s významnou změnou podle § 11 odst. 3 VyKB. Při změně bude kompetentní osobou nebo garantem MV expertně posouzeno, jestli změna má dopad do aktiv nebo nepředstavují pro systém riziko.

Požadavky na Penetrační testování webové aplikace:

* Manuální testování všech požadavků a odpovědí mezi prohlížečem a cílovou aplikací.
* Manipulace se server-side a client-side komponenty aplikace.
* Manipulace s parametry dotazů s cílem přečíst chráněná data z databází (využití SQLi).
* Útoky pomocí Cross-site Request Forgery (CSRF).
* Využití Cross-site Scriptingu (XSS) k převzetí kontroly nad klientskou částí aplikace.
* Obejití sanitace souborů při uploadu k distribuci malwaru na server, například s cílem získat neoprávněný přístup k adresářům a souborům.
* Zneužití slabých procesů pro obnovu hesel, stále aktivní výchozí a testovací účty.
* Odposlech nezabezpečené komunikace serveru s klientem, vyhledávání nechráněných souborů, nešifrovaných záloh.

### 9. Zkratky, pojmy, definice

Tabulka 1 – Seznam zkratek

|  |  |
| --- | --- |
| **Azure** | Cloudová platforma v datových centrech Microsoftu |
| **Cl/CD pipeline** | Představuje sérii kroků, které je nutné provést, pro správné dodání nové verze softwaru |
| **Git** | je v informatice distribuovaný systém správy verzí vytvořený Linusem Torvaldsem pro vývoj jádra Linuxu |
| **INSPIRE** | Národní geoportál |

|  |  |
| --- | --- |
| **ISMS** | Systém řízení bezpečnosti informací (Information Security Management Systém) |
| **ISSI** | Informační systém pro veřejné služby a služby veřejné správy INSPIRE |
| **NAKIT** | Národní agentura pro komunikační a informační technologie, s. p. |
| **MV** | Ministerstvo vnitra České republiky |
| **OWASP** | Open Web Application Security Project |
| **PM** | Projektový manažer |
| **SW** | Software |