SMLOUVA o poskytování služeb EDIH

uzavřená níže uvedeného dne, měsíce a roku podle právního řádu České republiky v souladu s ustanovením
§ 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, mezi těmito účastníky:

Smluvní strany

Objednatel

Moravskoslezské datové centrum, příspěvková organizace
se sídlem: Na Jízdárně 2824/2, 702 00 Ostrava - Moravská Ostrava
IČ: 06839517
DIČ: CZ06839517
zapsané v obchodním rejstříku vedeném u Krajského soudu v Ostravě, sp. zn. Pr 5292
zastoupené: Ing. RNDr. Aloisem Slovákem, ředitelem organizace
(dále jen“**objednatel**”)

Koordinátor

CyberSecurity Hub, z.ú.
se sídlem: Šumavská 416/5, 602 00 Brno - Ponava
IČ: 09705163
DIČ: CZ09705163
zapsaný v rejstříku ústavů vedeném u Krajského soudu v Brně, sp. zn. U 301
zastoupený: Mgr. Terezou Šamanovou, koordinátorkou EDIH, na základě pověření Romana Čermáka, M.Sc., MBA, ředitele ústavu
(dále jen **“koordinátor“)**

Seznam definic

Pro účely této smlouvy se níže uvedenými pojmy rozumí:

Cybersecurity Innovation Hub - Cybersecurity Innovation Hub (CIH) je jediným evropským digitálním inovačním centrem (EDIH) v České republice a jedním z mála ve střední Evropě, které se zaměřuje na kyberbezpečnost a důvěryhodnost. Hlavním cílem projektuje podpořit posílení konkurenceschopnosti ČR a EU urychlením digitální transformace a zaváděním nejmodernějších technologií v malých a středních podnicích a veřejných organizací při zohlednění rizik spojených s tímto procesem. Ve spolupráci s partnery v rámci sítě EDIH v ČR a EU bude CIH usilovat o vybudování efektivní platformy pro sdílení relevantních informací o dostupných nástrojích digitální transformace, o zvýšení know how, povědomí a znalostí relevantních subjektů v oblasti kyberbezpečnosti, o pomoc firmám a veřejné správě při zohledňování bezpečnostních parametrů při zavádění špičkových technologií do jejich procesů a o zajištění přístupu ke zdrojům financování zavádění inovací, a tím o snižování digitální propasti prostřednictvím mezisektorové a přeshraniční podpory.

DEP - program Digitální Evropa, který v rámci výzvy DIGITAL-2021-EDIH-01 financuje vytvoření a činnost Evropských center digitální inovací (EDIHs);

Koordinátor - osoba uvedená jako koordinátor v záhlaví této smlouvy;

NPO - Národní plán obnovy, který v rámci komponenty 1.5. Digitální transformace podniků, kofinancuje vytvoření a činnost Evropských center digitální inovací podpořených z programu Digitální Evropa;

Občanský zákoník - zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů;

Objednatel - osoba uvedená jako objednatel v záhlaví této smlouvy.

I. Předmět smlouvy

1. Předmětem této smlouvy je stanovení podmínek, za jakých koordinátor poskytne objednateli službu v rámci projektu Cybersecurity Innovation Hub. Koordinátor se zavazuje sjednané plnění provést včas a ve sjednané kvalitě. Zároveň objednatel bere na vědomí, že níže sjednané služby budou poskytovány prostřednictvím partnerů v rámci konsorcia EDIH Cybersecurity Innovation Hub. Za plnění a poskytování dílčích služeb nese odpovědnost koordinátor.
2. Koordinátor se touto smlouvou zavazuje zajistit poskytnutí těchto služeb objednateli:
    a. Dlouhodobá asistence pro organizaci objednatele na její cestě k digitální transformaci:
        i. Popis služby: Služba nabízí komplexní a dlouhodobou podporu během celé spolupráce. Pomáhá při řešení potíží a přizpůsobuje se individuálním potřebám každého klienta. Asistence zahrnuje reflexi specifických požadavků a zajišťuje, aby spolupráce byla synergická a efektivní. Důraz je kladen na poskytování kontinuální péče, která podporuje úspěšnou realizaci digitálních projektů. Služba je strukturována tak, aby maximálně reflektovala potřeby klientů a zajistila hladký průběh jejich digitální transformace.
        ii. Forma a místo poskytnutí služby: prostřednictvím pravidelných online jednání na platformě MS Teams
        iii. Rozsah poskytnutí služby: maximálně 40 hodin
        iv. Jednotková hodnota služby: 880 €
        v. Lhůta pro poskytnutí služby: od nabytí účinnosti této smlouvy průběžně až do 31. 12. 2025.
    b. Vyplnění úvodního i revizního Hodnocení digitální zralosti (Digital Maturity Assessment) pro organizaci objednatele:
        i. Popis služby: Digital Maturity Assessment (DMA) je nástroj pro hodnocení digitální vyspělosti organizace, vyvinutý Evropskou komisí.

Tento nástroj eviduje základní údaje o klientovi a hodnotí úroveň digitalizace v organizaci. Proces zahrnuje vyplnění formuláře DMA a následnou konzultaci výsledků. Na základě výsledků se navrhuje optimální mix služeb, které podpoří zvyšování digitální vyspělosti organizace. Prvotní hodnocení se realizuje při zahájení spolupráce a po roce se opakuje pro sledování pokroku.

ii. Forma a místo poskytnutí služby: prostřednictvím online konzultací na platformě MS Teams

iii. Rozsah poskytnutí služby: maximálně 2 h vyplnění hodnocení, do 35 h návrh opatření

iv. Jednotková hodnota služby: 780 €

v. Lhůta pro poskytnutí služby: do 31. 12. 2025.

c. Mikrokurz základů kyberbezpečnosti pro manažery:

i. Popis služby: Kurz účastníky seznamuje s riziky v digitální ekonomice a s problémy, kterým mohou čelit řídicí pracovníci firem a veřejných organizací. Účastníci se naučí základní principy obrany své organizace proti kybernetickým útokům, seznámí se s novou legislativou NIS2 a získají povědomí o základních technikách prevence a praktických krocích při obraně své organizace proti kyberútokům. Kurz poskytuje praktické rady, jak lépe řídit svou organizaci v prostředí zintenzivňujících se kybernetických hrozeb.

ii. Forma a místo poskytnutí služby: online (MS Teams) a fyzické školení (ve školicí místnosti zajištěné objednatelem) v rozsahu 2 hodiny

iii. Rozsah poskytnutí služby: školení pro 200 uživatelů

iv. Jednotková hodnota služby po množstevní slevě: 125 €

v. Lhůta pro poskytnutí služby: do 31. 12. 2025.

d. Základy kyberbezpečnosti pro uživatele - minikurz:

i. Popis služby: Kurz účastníky seznamuje s riziky v digitální ekonomice a s problémy, kterým mohou čelit jak řídicí, tak i řadoví pracovníci firem. Účastníci se naučí základní principy obrany svého podnikání, seznámí se s novou legislativou NIS2 a získají povědomí o základních technikách prevence a obrany proti kyberútokům. Kurz poskytuje praktické rady, jak lépe chránit digitální infrastrukturu své organizace.

ii. Forma a místo poskytnutí služby: online (MS Teams) a fyzické školení (ve školicí místnosti zajištěné objednatelem) v rozsahu 4 hodiny

iii. Rozsah poskytnutí služby: školení pro 200 uživatelů

iv. Jednotková hodnota služby po množstevní slevě: 125 €

v. Lhůta pro poskytnutí služby: do 31. 12. 2025.

e. Základní bezpečnost ICT pro správce ICT:

i. Popis služby: Kurz je zaměřen na vzdělávání správců ICT o klíčových kyberbezpečnostních tématech. Účastníci se naučí identifikovat a vyhodnocovat bezpečnostní zranitelnosti, nastavovat bezpečnou konfiguraci systémů a politiky hesel, a efektivně reagovat na incidenty. Skolení zahrnuje praktické úkoly a otázky k procvičení získaných znalostí, což umožní rychle nastavit základní úroveň kyberbezpečnosti v organizaci.

ii. Forma a místo poskytnutí služby: online (MS Teams) školení v rozsahu 4 x 4 hodiny

iii. Rozsah poskytnutí služby: školení pro 100 uživatelů

iv. Jednotková hodnota služby po množstevní slevě: 525 €

v. Lhůta pro poskytnutí služby: do 31. 12. 2025.

f. Základy Python:

i. Popis služby: Kurz seznamuje se základy programování v jazyce Python. Účastníci se naučí pracovat s prostředím a syntaxí Pythonu, správně členit kódy a pracovat se soubory. Dále se kurz zaměřuje na sběr, ukládání, vizualizaci a analýzu dat. Tento praktický přístup umožní účastníkům získat dovednosti potřebné pro efektivní práci s daty a jejich využití v různých oblastech, jako jsou ekonomie, informatika či medicína.

ii. Forma a místo poskytnutí služby: online (MS Teams) školení v rozsahu 4 x 4 hodiny

iii. Rozsah poskytnutí služby: školení pro 6 uživatelů

iv. Jednotková hodnota služby: 1 250 €

v. Lhůta pro poskytnutí služby: do 31. 12. 2025.

g. Penetrační testování webových aplikací (kurz):

i. Popis služby: Kurz poskytuje základy penetračního testování webových aplikací, zaměřuje se na základní postupy a metodologii black-box testování. Účastníci se seznámí s bezpečnostními standardy jako OWASP ASVS a OWASP Top 10, které jsou klíčové pro identifikaci a řešení zranitelností. Veškerá témata budou probírána jak teoreticky,

tak prakticky, což umožní účastníkům získat praktické dovednosti v oblasti penetračního testování a aplikovat je v reálném světě.

ii. Forma a místo poskytnutí služby: online (MS Teams) nebo fyzické školení v rozsahu 8 hodin

iii. Rozsah poskytnutí služby: školení pro 7 uživatelů

iv. Jednotková hodnota služby po množstevní slevě: 1 875 €

v. Lhůta pro poskytnutí služby: do 31. 3. 2025.

h. Pokročilé kyberbezpečnostní školení pro uživatele / správce ICT:

i. Popis služby: Toto školení se zaměřuje na prohloubení znalostí v oblasti kyberbezpečnosti prostřednictvím pokročilých témat a praktických příkladů.

- Verze pro uživatele: Zaměřuje se na phishingové útoky, včetně jejich identifikace a obraných technik. Účastníci se naučí, jak rozpoznat různé typy phishingu a jak se efektivně chránit.
- Verze pro správce ICT: Pokrývá pokročilé techniky pro zajištění bezpečnosti organizace, včetně penetračního testování a základů forenzní analýzy strojů.

Na konci školení absolvují účastníci prakticky orientovaný test, který ověří jejich nové dovednosti. Na žádost může být součástí školení také hodnotící workshop, kde budou diskutovány výsledky testu a poskytovány další rady a doporučení.

ii. Forma a místo poskytnutí služby: online (MS Teams) školení v rozsahu 8 - 25 hodin (dle dohody na úrovni kontaktních osob objednatele a koordinátora)

iii. Rozsah poskytnutí služby: školení pro 35 uživatelů

iv. Jednotková hodnota služby po množstevní slevě: 1 250 €

v. Lhůta pro poskytnutí služby: do 30. 6. 2025.

i. Pokročilá správa podnikových sítí:

i. Popis služby: Kurz nabízí komplexní školení v oblasti návrhu, zabezpečení, provozu a řešení problémů v moderních podnikových sítích. Účastníci se seznámí s architekturou podnikových sítí, WAN technologiemi, mechanismy zajištění kvality služeb a bezpečným vzdáleným přístupem. Kurz zahrnuje praktické ukázky a simulace, které umožňují aplikaci teoretických poznatků v reálných scénářích. Laboratoře jsou přístupné na dálku, což umožňuje simulaci témat

z pohodlí domova. Po úspěšném ukončení kurzu mohou absolventi získat slevu na průmyslový certifikát od CISCO.

ii. Forma a místo poskytnutí služby: online (MS Teams) školení v rozsahu 7 x 4 hodiny

iii. Rozsah poskytnutí služby: školení pro 6 uživatelů

iv. Jednotková hodnota služby: 1 700 €

v. Lhůta pro poskytnutí služby: do 30. 6. 2025.

j. Úvod do principů síťové bezpečnosti:

i. Popis služby: Kurz nabízí komplexní školení v oblasti návrhu, zabezpečení, provozu a řešení problémů v moderních podnikových sítích. Účastníci se seznámí s architekturou podnikových sítí, WAN technologiemi, mechanismy zajištění kvality služeb a bezpečným vzdáleným přístupem. Kurz zahrnuje praktické ukázky a simulace, které umožňují aplikaci teoretických poznatků v reálných scénářích. Laboratoře jsou přístupné na dálku, což umožňuje simulaci témat z pohodlí domova. Po úspěšném ukončení kurzu mohou absolventi získat slevu na průmyslový certifikát od CISCO.

ii. Forma a místo poskytnutí služby: online (MS Teams) školení v rozsahu 7 x 4 hodiny

iii. Rozsah poskytnutí služby: školení pro 7 uživatelů

iv. Jednotková hodnota služby: 1 700 €

v. Lhůta pro poskytnutí služby: do 30. 6. 2025.

k. Pokročilá správa podnikové sítě využívající produktů CISCO:

i. Popis služby: Kurz se zaměřuje na správu podnikových sítí využívajících produkty CISCO, rozšiřuje znalosti architektury a prohlubuje implementační dovednosti vyžadované podnikovými sítěmi. Účastníci se naučí pokročilé techniky přepínání, směrování, zabezpečení a správy bezdrátových sítí, a budou připraveni na zkoušku 350-401 ENCOR, která vede k získání certifikátu Enterprise Core Specialist. Doporučená příprava: CCNA 2,3 nebo ekvivalentní znalosti a dovednosti.

ii. Forma a místo poskytnutí služby: online (MS Teams) školení v rozsahu 7 x 4 hodiny

iii. Rozsah poskytnutí služby: školení pro 6 uživatelů

iv. Jednotková hodnota služby: 1 700 €

v. Lhůta pro poskytnutí služby: do 31. 12. 2025.

l. Kurz etického hackingu:

i. Popis služby: Kurz provede účastníky světem etického hackingu a penetračního testování. Zaměří se na techniky kontrolování a analýzy zranitelností, shromažďování informací a odhalování slabin systémů. Účastníci se naučí používat testovací nástroje, organizovat a řídit penetrační testy a efektivně reportovat výsledky a doporučení.

ii. Forma a místo poskytnutí služby: online (MS Teams) školení v rozsahu 5 x 4 hodiny

iii. Rozsah poskytnutí služby: školení pro 10 uživatelů

iv. Jednotková hodnota služby po množstevní slevě: 1 275 €

v. Lhůta pro poskytnutí služby: do 31. 12. 2025.

m. Kyberbezpečnostní dopady AI - Deepfakes:

i. Popis služby: Seminář se podrobně věnuje dopadům umělé inteligence v oblasti kyberbezpečnosti. Cílem je poskytnout účastníkům komplexní přehled o technologiích deepfakes, jejich využití a hrozbách. Součástí je interaktivní demonstrace, praktické zaměření na metody detekce a strategie obrany proti zneužití deepfakes.

ii. Forma a místo poskytnutí služby: online (MS Teams) školení v rozsahu 4 hodiny

iii. Rozsah poskytnutí služby: školení pro 20 uživatelů

iv. Jednotková hodnota služby po množstevní slevě: 750 €

v. Lhůta pro poskytnutí služby: do 30. 6. 2025.

n. Pokročilé kyberbezpečnostní cvičení v prostředí KYPO CRP:

i. Popis služby: Dvoudenní cvičení se zaměřuje na praktické řešení kyberbezpečnostního incidentu, během něhož účastníci z veřejných organizací a středních podniků zlepšují koordinaci a komunikaci svého týmu. Účastníci se naučí zvládat jednotlivé fáze incidentu, včetně technických, procesních a právních postupů nezbytných pro jeho úspěšné vyřešení. Cvičení zahrnuje simulaci reálných kyberútoků, jako jsou phishing, skenování portů a bruteforce útoky na hesla. Účastníci budou muset aktivně spolupracovat, předávat si informace a vypracovat závěrečné hodnocení incidentu. Znalost správy operačních systémů Windows a počítačových sítí je nezbytná, znalost systému Linux je výhodou.

ii. Forma a místo poskytnutí služby: cvičení s prezenční přítomností jeho účastníků v sídle poskytovatele služby (Masarykova univerzita, Brno) v rozsahu 17,5 hodin

iii. Rozsah poskytnutí služby: cvičení pro 4 týmy

iv. Jednotková hodnota služby: 10 000 €

v. Lhůta pro poskytnutí služby: do 30. 6. 2025.

o. Penetrační testování:

i. Popis služby: Penetrační testování pomáhá posoudit kyberbezpečnost organizace, a to buď z interního nebo externího pohledu. Interní testování hodnotí zabezpečení sítí, systémů nebo aplikací z perspektivy oprávněné osoby uvnitř organizace, což simuluje vnitřní hrozbu. Externí testování posuzuje zabezpečení z pohledu osoby zvenčí, pomocí simulace reálných kybernetických útoků a externích hrozeb. Služba z hmuje provedení testu, závěrečnou zprávu s nalezenými problémy a návrhy na zlepšení, a hodnotící workshop, který pomůže organizaci implementovat doporučená opatření.

ii. Forma a místo poskytnutí služby: zčásti v sídle objednatele, zčásti na dálku (formou e mailové komunikace a videokonferencí v prostředí MS Teams).

iii. Rozsah poskytnutí služby: 1 x provedení penetračního testu, celkový rozsah prací ze strany poskytovatele 8 x 10 hodin.

iv. Jednotková hodnota služby: 10 000 €

v. Lhůta pro poskytnutí služby: do 31. 12. 2025.

II. Cena a platební podmínky

1. Celková cena za plnění předmětu smlouvy je sjednána na základě ceníku služeb EDIH a je v rámci realizace projektu poskytována bezplatně v souladu s plněním cílů EDIH.

Tabulka č. 1

Řádek	**Cena služby dle ceníku EDIH**	**Cenové zvýhodnění od EDIHu (DEP + NPO)**	**Cenové zvýhodnění v režimu *de-minimis* (NPO)**	**Celková částka v Kč**
Služby a.	21 397,- Kč	21 397,- Kč	10 698,50 Kč	**0,-**
Služby b.	18 966,- Kč	18 966,- Kč	9 483,- Kč	**0,-**
Služby c.	607 875,- Kč	607 875,- Kč	303 937,50 Kč	**0,-**
Služby d.	607 875,- Kč	607 875,- Kč	303 937,50 Kč	**0,-**

Služby e.	1 276 538,- Kč	1 276 538,- Kč	638 269,- Kč	**0,-**
Služby f.	182 363,- Kč	182 363,- Kč	91 181,50 Kč	**0,-**
Služby g.	455 906,- Kč	455 906,- Kč	227 953,- Kč	**0,-**
Služby h.	1 063 781,- Kč	1 063 781,- Kč	531 890,50 Kč	**0,-**
Služby i.	248 013,- Kč	248 013,- Kč	124 006,50 Kč	**0,-**
Služby j.	289 349,- Kč	289 349,- Kč	144 674,50 Kč	**0,-**
Služby k.	248 013,- Kč	248 013,- Kč	124 006,50 Kč	**0,-**
Služby 1.	310 016,- Kč	310 016,- Kč	155 008,- Kč	**0,-**
Služby m.	364 725,- Kč	364 725,- Kč	182 362,50 Kč	**0,-**
Služby n.	972 600,- Kč	972 600,- Kč	486 300,- Kč	**0,-**
Služby o.	243 150,- Kč	243 150,- Kč	121 575,- Kč	**0,-**
CELKEM	**6 910 567,- Kč**	**6 910 567,- Kč**	**3 455 283,50 Kč**	**0,-**

2. Výše uvedená cena v sobě zahrnuje veškeré nezbytné náklady koordinátora a poskytovatele spojené s poskytováním služeb dle této smlouvy. Cena služeb uvedených v článku II., Tabulka 1 zůstává při navýšení počtu účastníků neměnná.

III. Povinnosti objednatele

1. Objednatel se zavazuje poskytovat veškerou součinnost nezbytnou k řádnému zajištění služeb koordinátorem, zejména mu pro tuto činnost včas předat veškeré potřebné informace a materiály, o které koordinátor objednatele požádá.

2. Za objednatele je kontaktní osobou ve věcech této smlouvy [redacted]

IV. Povinnosti koordinátora

1. Koordinátor je povinen postupovat s náležitou odbornou péčí v souladu s platnými právními předpisy, chránit práva a oprávněné zájmy objednatele. K plnění předmětu smlouvy je koordinátor povinen důsledně využívat všechny zákonné prostředky a uplatňovat vše, co podle svého odborného přesvědčení a příkazů objednatele pokládá za prospěšné.

2. Za koordinátora je kontaktní osobou ve věcech této smlouvy i v praktických záležitostech týkajících se poskytování služby je B[redacted]

V. Čestná prohlášení objednatele

Objednatel podpisem této smlouvy čestně prohlašuje, že:

1. Není ve střetu zájmů ve smyslu „Průvodce pro oblast střetu zájmů dle čl. 61 Finančního nařízení pro Národní plán obnovy na období 2021 2026“ dostupného v části Metodické pokyny Národního plánu obnovy na https://www.planobnovycr.cz/ke-stazeni.
2. V rámci evidence skutečných majitelů nemá povinnost zapisovat skutečné majitele dle § odst. 4 zákona č. 253/2008 Sb„ zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu a tito skuteční majitelé odpovídají definicím uvedených v zákoně č. 37/2021 Sb„ o evidenci skutečných majitelů a v Směrnici Evropského Parlamentu a Rady (EU) č. 2015/849 ze dne 20. května 2015 o předcházení využívání finančního systému k praní peněz a financování terorismu.
3. Poskytnutou službou nedochází k dvojímu financování.
4. Není podezřelý ze spáchání trestného činu podvodu nebo trestného činu majícího znaky korupčního chování ve smyslu zákona č. 40/2009 Sb„ trestního zákoníku, ve znění pozdějších předpisů a nebylo proti němu v této souvislosti zahájeno žádné trestní řízení.
5. Významně nepoškozuje environmentální cíle dle čl. 17 Nařízení Evropského parlamentu a Rady EU 2020/852 ze dne 18. června 2020 o zřízení rámce pro usnadnění udržitelných investic a o změně nařízení (EU) 2019/2088.
6. Bere za vědomí nutnost zpracování osobních údajů z důvodů evidence podpořených osob a evidence poskytnutých služeb EDIHu v projektu za účelem prokázání řádného a efektivního nakládání s prostředky, a to nejméně do 31.12.2035. Zároveň je si vědom svých práv podle zákona č. 110/2019 Sb., o zpracování osobních údajů.
7. Prohlašuje, že není podnikem ve smyslu Přílohy I Nařízení Komise (EU) č. 651/2014 ze dne 17. června 2014, kterým se v souladu s články 107 a 108 Smlouvy prohlašují určité kategorie podpory za slučitelné s vnitřním trhem a je daňovým rezidentem České republiky.

VI. Závěrečná ustanovení

1. Smluvní strany se dohodly, že tato smlouva a právní vztahy neupravené touto smlouvou se řídí výhradně příslušnými právními předpisy České republiky, zejména příslušnými ustanoveními zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
2. Smlouvu lze měnit nebo doplňovat pouze písemnými číslovanými dodatky podepsanými oběma smluvními stranami.
3. Nevynutitelnost a/nebo neplatnost a/nebo neúčinnost kteréhokoli ujednání této smlouvy neovlivní vynutitelnost a/nebo platnost a/nebo účinnost jejích ostatních ujednání, V případě, že by jakékoli ujednání smlouvy mělo pozbýt platnosti a/nebo účinnosti, zavazují se tímto smluvní strany zahájit jednání a v co možná nejkratším termínu

se dohodnout na přijatelném způsobu provedení záměrů obsažených v takovém ujednání, jež platnosti a/nebo účinnosti a/nebo vynutitelnosti pozbylo.

4. Veškeré spory vzniklé z právních vztahů založených smlouvou i z později uzavřených smluv prováděcích budou přednostně řešeny vzájemným jednáním a dohodou.
5. Tato smlouva může být ukončena písemnou dohodou smluvních stran, obsahující datum, k němuž bude smlouva ukončena, a způsob vzájemného vypořádání práv a povinností smluvních stran.
6. Smluvní strany jsou povinny bez zbytečného odkladu oznámit písemně druhé smluvní straně změnu údajů v záhlaví smlouvy.
7. Za písemnou formu oznámení se pro účely této smlouvy pokládají také oznámení učiněná faxem či elektronickou poštou na dohodnutá faxová čísla či elektronické adresy.
8. Strany se dohodly, že postoupení práv a povinností ze smlouvy třetí osobě je možné pouze se souhlasem druhé smluvní strany.
9. Tato smlouvaje uzavřena a účinná okamžikem podpisu smluvními stranami.
10. Smluvní strany prohlašují, že si tuto smlouvu před jejím podpisem přečetly, že byla uzavřena po řádném uvážení, svobodně a vážně, určitě a srozumitelně, nikoli v tísni za nápadně nevýhodných podmínek, s jejím obsahem bezvýhradně souhlasí a na důkaz toho připojují elektronické podpisy svých oprávněných zástupců.

[redacted]

(podepsáno elektronicky)
Mgr. Tereza Šamanová
koordinátorka EDIH Cybersecurity Innovation Hub
CyberSecurity Hub, z.ú.

(podepsáno elektronicky)
Ing. RNDr. Alois Slovák
ředitel organizace
Moravskoslezské datové centrum
příspěvková organizace