SMLOUVA O POSKYTOVÁNÍ SLUŽEB SERVERHOUSINGU

Smluvní strany:

Česká republika – Ústav zdravotnických informací a statistik České republiky

se sídlem: Palackého náměstí 4/375, 128 01 Praha 2

zastoupená: prof. RNDr. Ladislavem Duškem Ph.D., ředitelem

IČ: 00023833

DIČ: CZ00023833

bankovní spojení – [redacted]

(dále též jen „**objednatel**")

a

O2 Czech Republic a.s.

se sídlem: Praha 4 - Michle, Za Brumlovkou 266/2, PSČ 14022

IČO: 60193336, DIČ: CZ60193336

společnost zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze,

oddíl B, vložka 2322

bank. spojení: [redacted]

zastoupená: [redacted]

je plátce DPH

(dále též jen „**poskytovatel**")

dnešního dne uzavřely tuto smlouvu v souladu s ustanovením § 2201 a násl. a § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**občanský zákoník**") a zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen **„ZZVZ"**)

(dále jen „**Smlouva**")

1. ÚVODNÍ USTANOVENÍ

1.1 Objednatel zahájil zadávací řízení na zadání nadlimitní veřejné zakázky s názvem „**Datové centrum**“ ev. čísla Z2023-031459 (dále též jen „**Veřejná zakázka**“) dle ZZVZ. Na základě tohoto zadávacího řízení byla pro plnění Veřejné zakázky vybrána nabídka poskytovatele v souladu s ustanovením § 122 odst. 1 ZZVZ.

1.2 Objednatel prohlašuje, že:

a) je organizační složkou státu v přímé řídící působnosti Ministerstva zdravotnictví, splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené.

1.3 Poskytovatel prohlašuje, že:

a) je právnickou osobou řádně založenou a existující podle českého právního řádu;

b) splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn Smlouvu uzavřít a řádně plnit závazky v ní obsažené;

c) ke dni uzavření této Smlouvy není vůči němu vedeno řízení dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů (dále jen „**insolvenční zákon**“), a zavazuje se objednatele bezodkladně informovat o všech skutečnostech o hrozícím úpadku, popř. o prohlášení úpadku jeho společnosti, stejně jako o změnách v jeho kvalifikaci, kterou prokázal v rámci své nabídky na plnění Veřejné zakázky v dále uvedeném smyslu;

d) je dostatečně obeznámen s předmětem plnění této Smlouvy a okolnostmi s tím souvisejícími a s přihlédnutím k tomu prohlašuje, že disponuje veškerými odbornými dovednostmi, profesními předpoklady, zkušenostmi a prostředky umožňujícími mu splnit předmět této Smlouvy;

e) má zájem Veřejnou zakázku pro objednatele řádně a včas splnit za úplatu sjednanou v této Smlouvě. Dále poskytovatel prohlašuje, že se detailně seznámil s rozsahem a povahou předmětu Veřejné zakázky, že jsou mu známy veškeré technické, kvalitativní a jiné podmínky nezbytné k její realizaci, těmto podmínkám rozumí a je schopný je dodržet, a

f) disponuje veškerými profesními znalostmi a dovednostmi k řádnému splnění předmětu Veřejné zakázky, a že všechny osoby, které použije k plnění této Smlouvy, mají potřebné vzdělání, zkušenosti či jinou profesní způsobilost k plnění, které má poskytovatel dle této Smlouvy poskytovat;

g) bere na vědomí, že Objednatel je správcem významných informačních systémů dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „**ZKB**“), a zároveň Významným dodavatelem a Provozovatelem KII a VIS, jejichž správcem je Ministerstvo zdravotnictví, dle ZKB. Poskytovatel dále tímto bere na vědomí, že plnění dle této Smlouvy bude prováděno na podpůrných aktivech KII a VIS.

h) bere na vědomí, že informován objednatelem, Významným dodavatelem ve smyslu § 2 písm. n) a § 8 odst. 1 písm. f) a odst. 2 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „**VKB**“) ve znění přílohy č. 6.

1.4 Poskytovatel se zavazuje zajistit, aby výše uvedená prohlášení, která činí při podpisu této Smlouvy, byla pravdivá po celou dobu trvání jeho závazků z této Smlouvy a zavazuje se informovat objednatele bez zbytečného odkladu, pokud jakékoliv z těchto prohlášení je nebo se stane nepravdivým, neúplným či zavádějícím.

2. ÚČEL SMLOUVY

2.1 Účelem této Smlouvy je splnění předmětu Veřejné zakázky, jak vyplývá ze zadávací dokumentace k Veřejné zakázce (dále též jen „**ZD**“), tedy vybudování primárního datového centra elektronického zdravotnictví.

2.2 Poskytovatel bere na vědomí, že struktura provozovaných systémů v datovém centru elektronického zdravotnictví vyžaduje zajištění vysoké dostupnosti a úrovně zabezpečení dle ZKB a dalších právních předpisů upravujících provozování kritické informační infrastruktury a významných informačních systémů. Poskytovatel bere na vědomí, že nezajištění poskytování datových služeb dle této Smlouvy a dále v technické specifikaci, která je přílohou č. 1 této Smlouvy může mít za následek škody na životě a zdraví třetích osob.

2.3 Poskytovatel touto Smlouvou garantuje objednateli splnění zadání stanovené pro Veřejnou zakázku a všech z toho vyplývajících podmínek a povinností podle ZD. Pro vyloučení jakýchkoliv pochybností to znamená, že:

a) v případě chybějících ustanovení této Smlouvy budou použita dostatečně konkrétní ustanovení ZD;
b) v případě jakýchkoliv nejasností o výkladu této Smlouvy se použije výklad nejpřesněji odpovídající obsahu a účelu ZD;
c) poskytovatel je vázán svou nabídkou předloženou objednateli v rámci zadávacího řízení na zadání Veřejné zakázky, která se pro úpravu vzájemných vztahů vyplývajících z této Smlouvy použije subsidiárně.

3. PŘEDMĚT SMLOUVY

3.1 Předmětem této Smlouvy je závazek poskytovatele poskytovat objednateli služby serverhousingu, tj. přenechat objednateli k dočasnému užívání prostory v datovém centru včetně technologických zařízení za účelem umístění jeho HW (dále jen „**pronajaté prostory**“) a poskytovat mu služby s tím spojené, a to za podmínek blíže sjednaných v této Smlouvě včetně jejích příloh, zejména v technické specifikaci, která je přílohou č. 1 této Smlouvy (dále jen „**Služby**“) a závazek objednatele platit poskytovateli za tyto Služby sjednanou cenu.

3.2 Nedílnou součástí a přílohou č. 2 této Smlouvy je dále situační plánek s vyznačením pronajatých prostor datového centra včetně technologických zařízení poskytovatele, ve kterých budou servery umístěny (stojany, racky) a společně užívaných prostor. Popis pronajatých prostor je uveden v příloze č. 3 této Smlouvy.

3.3 Objednatel poskytne poskytovateli součinnost za předpokladu, že si poskytovatel tuto součinnost výslovně vyžádal a s ohledem na předmět plnění této Smlouvy lze její poskytnutí po objednateli spravedlivě požadovat. Objednatel zejména není povinen poskytnout poskytovateli požadovanou součinnost v rozsahu, v jakém si poskytovatel může zajistit obdobné plnění, jako je předmět požadované součinnosti, jinými způsoby než prostřednictvím součinnosti objednatele nebo je předmět požadované součinnosti součástí předmětu plnění této Smlouvy.

3.4 Poskytovatel se zavazuje Služby poskytovat sám, nebo s využitím třetích osob (poddodavatelů) uvedených v příloze č. 5 této Smlouvy. Jakákoliv dodatečná změna osoby poddodavatele nebo zvětšení rozsahu plnění svěřeného poddodavateli musí být předem písemně schválena objednatelem. Při poskytování Služeb poddodavatelem, ať již objednatelem schváleným či neschváleným, má poskytovatel odpovědnost, jako by Služby poskytoval sám.

3.5 Smluvní strany potvrzují, že rozsah zapojení poskytovatele na zajištění bezpečnostních aktiv informačních a komunikačních systémů kritické informační infrastruktury a aktiv významných informačních systémů je určen předmětem této Smlouvy.

4. CENA

4.1 Objednatel se zavazuje platit poskytovateli cenu za Služby. V ceně je obsažen nájem prostor, veškeré služby a činnosti dle čl. 3 Smlouvy potřebné pro řádné splnění předmětu Smlouvy.

4.2 Cena za Služby bude tvořena následujícími položkami:

a) - cenou za spotřebu 1 kWh elektrické energie včetně maximálně garantovaného PUE spotřebovanou dle skutečnosti servery [redacted]

b) - paušální cenou za poskytování datových a ostatních služeb [redacted]

Jednotlivé typy služeb jsou blíže specifikovány v příloze č. 1 Smlouvy, cena za jednotlivé Služby je dále přesněji specifikována v příloze č. 4 této Smlouvy.

4.3 Za den uskutečnění zdanitelného plnění se považuje vždy poslední kalendářní den v měsíci, ve kterém poskytovatel poskytoval objednateli Služby.

4.4 Objednatel se zavazuje poskytovateli hradit cenu elektřiny následovně:

a) v období počínaje dnem nabytí účinnosti Smlouvy, po dobu následujících 6 (slovy: šesti) celých kalendářních měsíců (dále také jen „**období s fixní cenou elektřiny**“) se zavazuje objednatel poskytovateli hradit cenu elektřiny dle skutečné spotřeby elektřiny potřebné k realizaci a poskytování předmětu plnění dle této Smlouvy vypočtené podle jednotkové ceny elektřiny (1kWh včetně maximálního garantovaného PUE), která je uvedena v tabulce Přílohy č. 4 této Smlouvy.

b) v období po skončení období s fixní cenou elektřiny do ukončení této Smlouvy (dále také jen „**návazné období**“) se zavazuje objednatel poskytovateli hradit cenu elektřiny dle skutečné spotřeby potřebné k realizaci a poskytování předmětu plnění dle této Smlouvy a dle příslušné jednotkové nákupní ceny elektřiny stanovené v ceníku dodavatele elektřiny, který elektřinu do datového centra, ve kterém je umístěna technika dle Přílohy č. 2 Smlouvy, dodává, navýšené o koeficient PUE jehož maximální garantovaná hodnota do ukončení této smlouvy nesmí překročit hodnotu 1,5; Poskytovatel se zavazuje objednatele vždy informovat nejpozději do 5 (slovy: pěti) pracovních dnů od obdržení nového ceníku elektřiny o změně příslušné jednotkové nákupní ceny elektřiny, či o změně výše koeficientu PUE a zároveň je povinen v této lhůtě objednateli nový ceník elektřiny, podle kterého bude stanovena cena za spotřebu elektřiny, zaslat na e-mailovou adresu kontaktní osoby, kterou je [redacted]

4.5 Cenu Služeb bude hradit objednatel poskytovateli měsíčně, a to vždy za každý ukončený kalendářní měsíc zpětně, přičemž poskytovatel provede vyúčtování Služeb vždy k poslednímu dni daného kalendářního měsíce, za který se spotřeba Služeb platí. Účetním obdobím je tedy jeden kalendářní měsíc (příp. jeho část).

4.6 Fakturace ceny elektřiny musí vždy odpovídat skutečné spotřebě zjištěné měřením na samostatném elektroměru. Přílohou daňového dokladu musí být vždy dokument obsahující informaci o spotřebě elektřiny potřebné k realizaci a poskytování předmětu plnění dle této smlouvy a výpočet ceny elektřiny za kalendářní měsíc, za který se cena elektřiny platí.

4.7 Faktura bude poskytovatelem vystavována pravidelně v měsíčních intervalech, a to vždy nejpozději do 10. dne kalendářního měsíce bezprostředně následujícího po skončení příslušného kalendářního měsíce.

4.8 Každá faktura musí splňovat všechny náležitosti podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů a musí obsahovat všechny údaje uvedené v ust. § 435 odst. 1 občanského zákoníku. Výše fakturované částky musí odpovídat sjednané ceně. Každá faktura musí obsahovat navíc tyto údaje:

a) označení povinné a oprávněné osoby, adresu, sídlo, DIČ,
b) číslo dokladu,
c) den odeslání a den splatnosti, den zdanitelného plnění,
d) označení peněžního ústavu a číslo účtu, na který se má platit, konstantní a variabilní symbol,
e) účtovanou částku, DPH, účtovanou částku vč. DPH,
f) název veřejné zakázky, označení části plnění veřejné zakázky (1. spotřeba el. energie, 2. poskytnutí datových a ostatních služeb)
g) důvod účtování s odvoláním na smlouvu;
h) razítko a podpis osoby oprávněné k vystavení daňového dokladu,
i) seznam příloh,
j) další náležitosti, pokud je stanoví obecně závazný předpis.

4.9 V případě, že faktura nebude obsahovat některou náležitost uvedenou v odst. 4.8 tohoto článku nebo ji bude obsahovat chybně, je objednatel oprávněn fakturu do data

splatnosti vrátit poskytovateli. Lhůta splatnosti v takovémto případě neběží, přičemž nová lhůta splatnosti počíná běžet až ode dne doručení opravené či doplněné faktury.

4.10 Splatnost faktury se sjednává na 30 dní ode dne doručení faktury objednateli. Platba se považuje za splněnou dnem odepsání z účtu objednatele ve prospěch účtu poskytovatele.

4.11 V případě prodlení objednatele se zaplacením peněžitého závazku, je objednatel povinen zaplatit poskytovateli úrok z prodlení ve výši jedné setiny procenta (0,01 %) z dlužné částky za každý i započatý den prodlení.

4.12 Objednatel bude hradit přijaté faktury pouze na bankovní účty poskytovatele zveřejněné správcem daně způsobem umožňujícím dálkový přístup ve smyslu § 96 odst. 2 zákona o DPH. V případě, že poskytovatel nebude mít svůj bankovní účet tímto způsobem zveřejněn, uhradí objednatel poskytovateli pouze základ daně, přičemž daň z přidané hodnoty (dále jen „**DPH**“) uhradí poskytovateli až po zveřejnění příslušného účtu poskytovatele v registru plátců a identifikovaných osob poskytovatelem.

4.13 Poskytovatel prohlašuje, že správce daně před uzavřením této Smlouvy nerozhodl, že poskytovatel je nespolehlivým plátcem ve smyslu § 106a zákona o DPH (dále jen „**nespolehlivý plátce**“). V případě, že správce daně rozhodne o tom, že poskytovatel je nespolehlivým plátcem, zavazuje se poskytovatel o tomto informovat objednatele do 2 pracovních dní. Stane-li se poskytovatel nespolehlivým plátcem, uhradí objednatel poskytovateli pouze základ daně, přičemž DPH bude objednatelem uhrazena poskytovateli až po písemném doložení poskytovatele o jeho úhradě této DPH příslušnému správci daně.

5. DOBA A MÍSTO PLNĚNÍ

5.1 Místem plnění je [redacted]

5.2 Poskytovatel se zavazuje poskytovat Služby po celou dobu trvání této Smlouvy.

6. PRÁVA A POVINNOSTI POSKYTOVATELE

6.1 Poskytovatel se zavazuje poskytovat objednateli Služby blíže vymezené v technické specifikaci v příloze č. 1 této Smlouvy. Smluvní strany se s odkazem na § 2 207 občanského zákoníku dohodly, že se poskytovatel zavazuje provádět veškerou údržbu a úklid.

6.2 Objednatel se zavazuje užívat pronajaté prostory způsobem, v rozsahu a za podmínek stanovených v této Smlouvě.

6.3 Poskytovatel zajistí převoz a implementaci serverů objednatele ze stávajícího umístění do pronajatých prostor a předá objednateli pronajaté prostory se vším, co je třeba k jejich řádnému užívání do užívání do 10 dnů ode dne nabytí účinnosti výzvy k poskytnutí služeb. Výzva k poskytnutí služeb bude zaslána objednatelem poskytovateli a účinnosti nenabyde dříve než 90 dnů po nabytí platnosti smlouvy. Výzva k poskytnutí služeb může nabýt účinnosti nejdříve dnem jejího doručení poskytovateli. O předání a převzetí serverů a pronajatých prostor bude sepsán předávací protokol. Čl. 6.3 a 6.4

Smlouvy neplatí pro poskytovatele, který poskytoval Služby objednateli dle smlouvy zveřejněné pod odkazem https://smlouvy.gov.cz/smlouva/11473292.

6.4 Implementací dle odst. 6.3 se rozumí:

- fyzická montáž HW do rackových skříní,

6.5 Poskytovatel se zavazuje dodržovat platné technické, stavební a bezpečnostní normy týkající se poskytovaných Služeb, a to v souladu s touto Smlouvou a s jejími přílohami.

6.6 Poskytovatel je povinen zajistit nepřetržitý provoz datového centra v režimu 24/7/po celý kalendářní rok.

6.7 Poskytovatel povinen zajistit 99,99 % dostupnost datových služeb a připojení k internetu měsíčně.

6.8 Výpočet měsíční dostupnosti služeb bude vycházet z následujícího vzorce:

$$\left[\frac{\text{Počet minut, ve kterých byla služba dostupná v kalendářním měsíci}}{\text{Celkový počet minut v kalendářním měsíci}}\right] * 100 = \text{měsíční dostupnost služby v \%}$$

6.9 Po celou dobu trvání této Smlouvy je poskytovatel povinen zajistit bezpečnost pronajatých prostor, resp. zajistit v rozsahu specifikovaném v technické specifikaci v příloze č. 1 této Smlouvy a dále v rozsahu obvyklém pro provozovatele datového centra provedení a dodržování dostatečných opatření, aby servery objednatele nebyly zničeny, poškozeny, nebo odcizeny, ani nedošlo ke zničení, poškození, odcizení nebo jinému neoprávněnému zpracování dat v nich umístěných. Pro tento účel je poskytovatel povinen zajistit stálou dohledovou službu monitorující pronajaté prostory a celkový stav datového centra jako funkčního celku. Jedná se zejména o monitoring veškeré infrastruktury datového centra - napájení, chlazení včetně alarmových a poruchových stavů a varování a neustálé monitorování pohybu osob okolo pronajatého prostoru tak, aby byla dokumentována veškerá manipulace s rack skříněmi, ve kterých budou umístěny servery objednatele a s jejich obsahem.

6.10 Poskytovatel zajistí příslušným pracovníkům objednatele přístup do pronajatých prostor po celou jeho provozní dobu.

6.11 Po uplynutí doby, na kterou je tato Smlouva sjednána, objednatel v souladu s § 2 225 občanského zákoníku vyklidí pronajaté prostory a odevzdá je poskytovateli v takovém stavu, v jakém byly v době, kdy je objednatel převzal, s přihlédnutím k obvyklému opotřebení při řádném užívání, ledaže by pronajaté prostory zanikly nebo se znehodnotily.

6.12 Poskytovatel je v případě změny jeho (poskytovatelových) vlastnických práv k pronajatým prostorám ve prospěch třetí osoby povinen tuto třetí osobu předem informovat o existenci nájemního vztahu dle této Smlouvy a o osobě objednatele.

6.13 Pro případ, že poskytovatel v rámci plnění Smlouvy získá nahodilý přístup k informacím, které budou obsahovat osobní údaje podléhající ochraně podle platných právních předpisů, je poskytovatel oprávněn přistupovat k takovým osobním údajům pouze v nezbytném rozsahu pro plnění předmětu Smlouvy. Poskytovatel se zavazuje zpracovat tyto osobní údaje v souladu s čl. 29 Nařízení

Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) pouze na základě pokynů objednatele jako správce osobních údajů a pro účely plnění Smlouvy, zachovat o nich mlčenlivost a zajistit jejich bezpečnost proti úniku, náhodnému nebo neoprávněnému zničení, ztrátě, pozměňování nebo neoprávněnému zpřístupnění třetím osobám.

6.14 V případě, kdy objednatel zjistí závadu poskytovaných Služeb co do jeho parametrů dle technické specifikace uvedené v příloze č. 1 této Smlouvy, bez zbytečného odkladu ji nahlásí poskytovateli na kontaktní údaje dle odst. 15.4 této Smlouvy, objednatel tak splní svou povinnost dle § 2 214 občanského zákoníku.

6.15 Poskytovatel je povinen po nahlášení závady dle této Smlouvy provést bez zbytečného odkladu analýzu závady, a pokud zjistí, že je závada na straně poskytovatele, závadu odstranit a tento stav oznámit objednateli.

6.16 Poskytovateli nenáleží za výše uvedené služby poskytované v souvislosti s realizací dohledu dle tohoto článku 6 této Smlouvy jakákoli úplata a tyto služby jsou poskytovatelem poskytovány bezúplatně.

7. POVINNOSTI SMLUVNÍCH STRAN

7.1 Poskytovatel se zavazuje poskytovat Služby dle této Smlouvy sám, nebo s využitím poddodavatelů uvedených v Příloze č. 5 této Smlouvy. Jakákoliv dodatečná změna osoby poddodavatele nebo rozsahu plnění svěřeného poddodavateli musí být předem písemně schválena Objednatelem, ledaže by plnění původně svěřené poddodavateli realizoval Poskytovatel sám. Smluvní strany výslovně uvádějí, že při poskytování plnění dle této Smlouvy prostřednictvím jakékoliv třetí osoby dle tohoto odstavce má Poskytovatel odpovědnost, jako by plnění dle této Smlouvy realizoval sám.

7.2 Poskytovatel se zavazuje:

a) upozorňovat objednatele včas na všechny hrozící vady svého plnění, a to včetně vad vycházejících ze stávající platné legislativy dle této Smlouvy, jakož i poskytovat objednateli veškeré informace, které jsou pro plnění této Smlouvy nezbytné;

b) na své náklady a s péčí řádného hospodáře podporovat, spravovat a udržovat veškeré technické prostředky objednatele, které Poskytovatel převzal do užívání;

c) neprodleně oznámit písemnou formou objednateli překážky, které mu brání v plnění předmětu této Smlouvy a výkonu dalších činností souvisejících s plněním předmětu této Smlouvy;

d) upozornit objednatele na potenciální rizika vzniku škod a včas a řádně dle svých možností provést taková opatření, která riziko zcela vyloučí nebo sníží;

e) postupovat při poskytování plnění podle této Smlouvy s odbornou péčí a aplikovat procesy „*best practice*“;

f) v případě potřeby průběžně komunikovat s objednatelem a třetími osobami, vyžaduje-li to řádné poskytnutí plnění, přičemž veškerá taková komunikace

bude probíhat v českém jazyce (případně slovenském, nebo za využití překladatele do českého jazyka);

g) informovat objednatele o plnění svých povinností podle této Smlouvy a o důležitých skutečnostech, které mohou mít vliv na výkon práv a plnění povinností Smluvních stran.

7.3 Poskytovatel se zavazuje, že nebude jakýmkoliv způsobem odporujícím oprávněným zájmům objednatele jednat v součinnosti s jakoukoliv jinou osobou, která se podílí na poskytování plnění, které bylo předmětem Veřejné zakázky, jako dodavatel objednatele nebo jeho poddodavatel. Poskytovatel zároveň prohlašuje, že není dodavatelem objednatele nebo jeho poddodavatelem a není ani v žádném personálním nebo organizačním propojením s osobou, která se podílí na poskytování plnění v rámci předmětu Veřejné zakázky jako dodavatel objednatele nebo jeho poddodavatel.

7.4 Všechna oznámení mezi smluvními stranami, která se vztahují k této Smlouvě, nebo která mají být učiněna na základě této Smlouvy, musí být učiněna v písemné podobě a druhé straně doručena buď osobně nebo doporučeným dopisem či jinou formou registrovaného poštovního styku na adresu uvedenou na titulní stránce této Smlouvy, není-li stanoveno nebo mezi smluvními stranami dohodnuto jinak. Nemá-li komunikace dle předchozí věty mít vliv na platnost a účinnost Smlouvy, připouští se též doručení prostřednictvím faxu nebo e-mailu. Poskytovatel je oprávněn komunikovat s objednatelem prostřednictvím datové schránky.

7.5 Poskytovatel se při plnění zavazuje dodržovat zásady bezpečnosti informací v souladu se ZKB a VKB. Bezpečností informací se v souladu se ZKB rozumí zajištění důvěrnosti, integrity a dostupnosti informací, které budou uchovávány, vytvářeny nebo zpracovávány v rámci plnění poskytovatele dle této Smlouvy nebo v systémech, které mají vazbu na plnění poskytovatele dle této Smlouvy a v souvislosti s kterými objednateli vznikají právní povinnosti na základě ZKB (§ 3 tohoto zákona).

7.6 Poskytovatel se dále zavazuje poskytnout objednateli veškeré informace potřebné ke splnění povinností objednatele dle § 219 ZZVZ, popř. dle právního předpisu jej nahrazujícího, zejména, nikoli však výlučně nejpozději do 28. února následujícího kalendářního roku informaci o ceně uhrazené za plnění dle této Smlouvy v předchozím kalendářním roce plnění Smlouvy.

8. PRÁVA A POVINNOSTI SMLUVNÍCH STRAN DLE ZKB A VKB

8.1 Poskytovatel je povinen:

a) bezodkladně oznamovat neobvyklé chování informačního a komunikačního systému a podezření na jakékoliv zranitelnosti bezpečnosti informací objednatele,

b) poskytnout součinnost při realizaci auditu poskytovatele objednatelem dle relevantních právních předpisů o kybernetické bezpečnosti,

c) informovat objednatele o výskytu bezpečnostních incidentů dle VKB,

d) informovat objednatele o rizicích Plnění a jejich řízení ze strany poskytovatele,

e) informovat objednatele o významné změně ovládání poskytovatele. Ovládáním se rozumí vliv ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů, či ekvivalentní postavení dle VKB.

8.2 Poskytovatel prohlašuje, že má zavedena všechna bezpečnostní opatření, procesy a technologie, které prohlásil za zavedené (odpověděl ANO) v dotazníku Významného dodavatel dle vyhlášky 82/2018 Sb., o bezpečnostních opatření, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, který tvoří přílohu č. 6 ZD.

8.3 Poskytovatel je povinen v rozsahu plnění této Smlouvy naplnit všechny bezpečnostní požadavky uvedené v příloze č. 6 této Smlouvy. Poskytovatel umožní objednateli v roční periodě po dobu platnosti této Smlouvy a 1 rok po ukončení její platnosti provedení zákaznického auditu (kontroly):

a) jehož rozsah bude ohraničen využíváním ICT prostředků poskytovatele pro potřeby plnění této Smlouvy a uloženými či zpracovávanými daty a informacemi objednatele v ICT prostředí poskytovatele a

b) jehož předmětem bude naplnění Kybernetických požadavků a vyhodnocení rizik dle § 5 přílohy č. 6 této Smlouvy.

8.4 Poskytovatel umožní objednateli kontrolu přílohy č. 6 této Smlouvy provedenou prostředky objednatele nebo třetí strany, a to v lokalitě poskytovatele i vzdáleně, pokud to technické prostředky poskytovatele umožňují.

8.5 Poskytovatel se nad rámec ustanovení této Smlouvy zavazuje poskytnout objednateli součinnost minimálně v rozsahu 10 MD (MD = člověkoden v rozsahu 8 pracovních hodin) při provádění každého zákaznického auditu ze strany objednatele a pro tuto činnost zajistit účast kvalifikovaných pracovníků.

8.6 Objednatel je oprávněn při kontrole dle přílohy č. 6 této Smlouvy využít třetí stranu. V případě využití třetí strany bude objednatel odpovídat za třetí stranu, jako by kontrolu prováděl sám, včetně odpovědnosti za způsobenou újmu.

8.7 Poskytovatel se dále zavazuje nedostatky zjištěné:

1) na základě provedení hodnocení rizik dle § 5 v příloze č. 6 této Smlouvy;

2) v rámci zákaznického auditu dle čl. 8.3 této Smlouvy;

odstranit ve lhůtě určené v písemném oznámení objednatele.

8.8 Čl. 8.3 až 8.6 této Smlouvy se neaplikují, pokud je poskytovatel pro poskytování předmětu plnění orgánem nebo osobou uvedenou v § 3 písm. a) až g) ZKB.

8.9 Poskytovatel se nad rámec ustanovení této Smlouvy také zavazuje:

a) Poskytnout na vyžádání objednateli dokumenty a obdobné vstupy, které budou prokazovat naplnění Kybernetických požadavků dle Přílohy č. 6 této Smlouvy.

b) Na požádání s objednatelem konzultovat kdykoli v průběhu realizace plnění dle této Smlouvy detailní nastavení bezpečnostních opatření k naplnění Kybernetických požadavků dle přílohy č. 6 této Smlouvy a pro takovéto konzultace

zajistit účast kvalifikovaných pracovníků.

c) Neprodleně informovat objednatele o všech významných změnách v naplnění Kybernetických požadavků dle přílohy č. 6 této Smlouvy, které nastanou kdykoli v průběhu trvání této Smlouvy.

d) Bezodkladně a s vyvinutím nejlepšího úsilí zajistit náhradní způsob naplnění Kybernetických požadavků dle přílohy č. 6 této Smlouvy, pokud stávající řešení přestalo být funkční a efektivní.

e) Bezodkladně informovat objednatele o bezpečnostních incidentech, které mohou ovlivnit realizaci plnění dle této Smlouvy.

f) Při výkonu své činnosti včas a prokazatelně upozornit objednatele na zřejmou nevhodnost jeho příkazů či doporučení vztahující se ke Kybernetickým požadavkům dle přílohy č. 6 této Smlouvy a jejichž následkem může vzniknout újma nebo nesoulad se zákony nebo obecně závaznými právními předpisy.

9. OCHRANA INFORMACÍ

9.1 Smluvní strany jsou si vědomy toho, že v rámci plnění závazků z této Smlouvy:

a) si mohou vzájemně vědomě nebo opominutím poskytnout informace, které budou považovány za důvěrné (dále jen „**důvěrné informace**“),

b) mohou jejich zaměstnanci a osoby v obdobném postavení získat vědomou činností druhé strany nebo i jejím opominutím přístup k důvěrným informacím druhé strany.

9.2 Za důvěrné informace jsou dle této Smlouvy smluvními stranami považovány veškeré informace poskytnuté vzájemně v písemné formě, zejména informace smluvních stran, které se strany dozvěděly v souvislosti s touto Smlouvou, jakož i know-how, jímž se rozumí veškeré poznatky obchodní, provozní, technické či ekonomické povahy související s činností smluvní strany, které mají skutečnou nebo alespoň potenciální hodnotu a které nejsou v příslušných obchodních kruzích běžně dostupné a mají být utajeny, a to bez ohledu na to, zda jsou nebo nejsou označené jako důvěrné informace.

9.3 Smluvní strany se zavazují, že žádná z nich nezpřístupní třetí osobě důvěrné informace, které při plnění této Smlouvy získala od druhé smluvní strany.

9.4 Za třetí osoby podle odst. 9.3 této Smlouvy se nepovažují:

a) zaměstnanci smluvních stran a osoby v obdobném postavení,

b) orgány smluvních stran a jejich členové,

c) ve vztahu k důvěrným informacím objednatele poddodavatelé poskytovatele,

za předpokladu, že se podílejí na plnění této Smlouvy nebo na plnění spojeném s Plněním dle této Smlouvy, důvěrné informace jsou jim zpřístupněny výhradně za tímto účelem a zpřístupnění důvěrných informací je v rozsahu nezbytně nutném pro naplnění jeho účelu a za stejných podmínek, jaké jsou stanoveny smluvním stranám v této Smlouvě.

9.5 Bez ohledu na výše uvedená ustanovení se za důvěrné nepovažují informace, které:

a) se staly veřejně známými, aniž by jejich zveřejněním došlo k porušení závazků přijímající smluvní strany či právních předpisů,

b) měla přijímající strana prokazatelně legálně k dispozici před uzavřením této Smlouvy, pokud takové informace nebyly předmětem jiné, dříve mezi smluvními stranami uzavřené smlouvy o ochraně informací,

c) jsou výsledkem postupu, při kterém k nim přijímající strana dospěje nezávisle a je to schopna doložit svými záznamy nebo důvěrnými informacemi třetí strany,

d) mají být zpřístupněny, vyžaduje-li to zákon či jiný právní předpis včetně práva EU nebo závazné rozhodnutí oprávněného orgánu veřejné moci,

e) po podpisu této Smlouvy poskytne přijímající straně třetí osoba, jež není omezena v takovém nakládání s informacemi.

9.6 Za porušení povinnosti mlčenlivosti smluvní stranou se považují též případy, kdy tuto povinnost poruší kterákoliv z osob uvedených v odst. 9.4 této Smlouvy, které daná smluvní strana poskytla důvěrné informace druhé smluvní strany.

9.7 Poruší-li poskytovatel povinnosti vyplývající z této Smlouvy ohledně ochrany důvěrných informací, je povinen zaplatit objednateli smluvní pokutu ve výši 100.000,- Kč (slovy: jedno sto tisíc korun českých) za každé porušení takové povinnosti. Zaplacením smluvní pokuty není dotčeno právo objednatele na náhradu škody v plném rozsahu.

9.8 Ukončení účinnosti této Smlouvy z jakéhokoliv důvodu se nedotkne ustanovení tohoto článku 9 této Smlouvy a jejich účinnost přetrvá i po ukončení účinnosti této Smlouvy.

9.9 Poskytovatel prohlašuje, že tato Smlouva neobsahuje obchodní tajemství. Poskytovatel výslovně uděluje svůj souhlas k tomu, aby objednatel uveřejnil tuto Smlouvu včetně všech jejich dodatků a příloh v plném rozsahu v podepsané podobě a včetně všech údajů informací, k jejichž uveřejnění vyplývá pro objednatele povinnost dle právních předpisů.

10. POJIŠTĚNÍ

10.1 Poskytovatel se zavazuje udržovat v platnosti a účinnosti po celou dobu účinnosti Smlouvy a trvání záruky za jakost pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou poskytovatelem třetí osobě (objednateli), a to tak, že limit pojistného plnění vyplývající z pojistné smlouvy nesmí být nižší než 250.000.000,- Kč (slovy: dvěstěpadesát milionů korun českých). Na požádání, nejpozději však do 10 pracovních dnů od výzvy objednatele, je poskytovatel povinen objednateli takovou smlouvu, příp. certifikát o pojistném krytí vystavený pojišťovnou, předložit nejpozději v pracovní den následující po doručení žádosti objednatele o poskytnutí předmětné smlouvy.

10.2 Jestliže poskytovatel nebude udržovat v účinnosti vyžadované pojištění nebo nepředloží objednateli doklady podle tohoto článku, může objednatel odstoupit od této Smlouvy nebo svým jménem kdykoliv sjednat a udržovat jakékoliv pojištění pokrývající rizika spojená s poskytováním Služeb a platit jakékoliv pojistné, které je přiměřené pro takové

účely, a to na náklady poskytovatele, jakož i započítávat takto placené částky na jakékoliv platby poskytovateli, které jsou splatné nebo se splatnými teprve stanou.

10.3 Každá ze stran nese odpovědnost za způsobenou škodu v rámci platných právních předpisů a této Smlouvy. Obě strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.

11. SOUČINNOST A VZÁJEMNÁ KOMUNIKACE

11.1 Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace nezbytné pro řádné plnění svých závazků vyplývajících ze Smlouvy. Smluvní strany jsou povinny informovat druhou smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této Smlouvy.

11.1 V případě, že dojde k uzavření nové smlouvy týkající se Předmětu nájmu nebo jakékoli její části s osobou odlišnou od poskytovatele, zavazuje se poskytovatel před a po skončení účinnosti této Smlouvy (nebo její části) poskytovat objednateli nebo jím určeným třetím stranám veškerou součinnost potřebnou pro účely plynulého a řádného poskytování služeb obdobných Službám dle této Smlouvy či jejich příslušné části jinou osobou, pokud bude naplnění tohoto cíle záviset na znalostech poskytovatele získaných na základě plnění této Smlouvy. Poskytovatel se zavazuje tuto součinnost poskytovat s odbornou péčí, bez zbytečného odkladu a zodpovědně, a to minimálně po dobu 3 měsíců před a 6 měsíců po skončení účinnosti této Smlouvy (nebo její části). Smluvní strany se dohodly, že cena za plnění dle tohoto odstavce je součástí ceny za poskytování Služeb dle této Smlouvy.

12. NÁHRADA ŠKODY

12.1 Každá ze smluvních stran nese odpovědnost za způsobenou škodu 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.

12.2 Žádná ze smluvních stran není odpovědná za škodu a není ani v prodlení, pokud k tomuto došlo v důsledku prodlení s plněním závazků druhé smluvní strany nebo v důsledku mimořádné nepředvídatelné a nepřekonatelné překážky vzniklé nezávisle na její vůli (§ 2913 občanského zákoníku, dále jen „**okolnosti vylučující odpovědnost**“).

12.3 Smluvní strany se zavazují upozornit druhou smluvní stranu bez zbytečného odkladu na vzniklé okolnosti vylučující odpovědnost bránící řádnému plnění této Smlouvy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání okolností vylučujících odpovědnost.

13. SANKCE

13.1 V případě nezajištění bezvýpadkového napájení serverů elektrickou energií, se poskytovatel zavazuje zaplatit objednateli smluvní pokutu ve výši 2.000,- Kč za každou minutu výpadku.

13.2 v případě prodlení Poskytovatele s předložením pojistné smlouvy Objednateli ve lhůtě dle odst. 10.1 této Smlouvy vzniká Objednateli nárok na smluvní pokutu ve výši 10.000,-

Kč za každý i započatý den prodlení, přičemž se jedná o podstatné porušení této Smlouvy;

13.3 V případě neposkytnutí součinnosti ze strany poskytovatele k provedení jeho auditu dle čl. 8.3 písm. a) a b) kontrole naplnění požadavků na systém řízení bezpečnosti informací ve smyslu §8 Vyhlášky 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) uvedených v příloze č. 6B Smlouvy, má Objednatel nárok na zaplacení smluvní pokuty ve výši [redacted]

13.4 Pro případ prokazatelného porušení povinnosti poskytovatele být pojištěn po celou dobu účinnosti Smlouvy a trvání záruky ze strany poskytovatele je objednatel oprávněn po poskytovateli požadovat smluvní pokutu ve výši [redacted] a to za každý den, kdy poskytovatel nebyl pojištěn.

13.5 Zaplacení smluvní pokuty nezbavuje poskytovatele povinnosti splnit závazky stanovené Smlouvou.

13.6 Smluvní pokuta je splatná na základě faktury vystavené stranou oprávněnou do 30-ti (třiceti) dnů ode dne jejího doručení druhé smluvní straně.

13.7 Zaplacením smluvní pokuty není dotčeno právo objednatele na náhradu škody v celém rozsahu. Výše smluvních pokut se do výše náhrady škody nezapočítává.

14. UKONČENÍ SMLOUVY

14.1 Objednatel je oprávněn od Smlouvy odstoupit zejména v případě podstatného porušení smluvní nebo zákonné povinnosti poskytovatele.

14.2 Za podstatné porušení povinnosti dle odst. 14.1 této Smlouvy se považuje zejména výpadek poskytování datových služeb delší než celkem 1,6 hod/rok nebo opakované výpadky (více jak 1x za kalendářní rok) poskytování datových služeb, výpadky elektrického proudu bez napájení.

14.3 Odstoupení od Smlouvy ze strany objednatele je dále možné v případě, že:

a) v insolvenčním řízení bude zjištěn úpadek poskytovatele nebo insolvenční návrh bude zamítnut pro nedostatek majetku objednatele v souladu se zněním zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů;

b) poskytovatel vstoupí do likvidace.

14.4 Poskytovatel má právo odstoupit od Smlouvy v případě prodlení objednatele se zaplacením ceny plnění delším než 30 dní po skončení doby splatnosti faktury, a po zaslání písemné výzvy k úhradě.

14.5 Účinky odstoupení od Smlouvy nastávají dnem doručení písemného oznámení o odstoupení druhé smluvní straně.

14.6 Smlouvu lze ukončit vzájemnou písemnou dohodou smluvních stran.

14.7 Objednatel je oprávněn vypovědět smlouvu, a to i bez udání důvodu, s výpovědní dobou 3 měsíce, přičemž výpovědní doba začíná běžet prvního dne měsíce následujícího po měsíci, v němž byla výpověď doručena.

14.8 Ukončením účinnosti této Smlouvy nejsou dotčena ustanovení Smlouvy týkající se převodu vlastnického práva a užívacích práv, oprávnění k výkonu práv duševního vlastnictví, nároků z odpovědnosti za vady, nároků z povinnosti nahradit škodu a nároků ze smluvních pokut, ustanovení o ochraně informací, ustanovení o povinnosti zajistit technickou podporu výrobce, ani další ustanovení a nároky, z jejichž povahy vyplývá, že mají trvat i po zániku účinnosti této Smlouvy.

15. OZNÁMENÍ A KOMUNIKACE

15.1 Veškerá oznámení a komunikace uskutečněná na základě nebo v souvislosti s touto Smlouvou budou probíhat způsobem stanoveným v tomto čl. 15.

15.2 Smluvní strany se zavazují spolu komunikovat prostřednictvím osobního doručování, doručování doporučených zásilek prostřednictvím poskytovatele poštovních služeb či elektronickou poštou, a to na níže uvedené adresy kontaktních osob. Smluvní strany jsou oprávněny změnit adresy kontaktních osob, a to písemným oznámením druhé smluvní straně. Změna adresy kontaktní osoby je vůči druhé smluvní straně účinná okamžikem doručení takového písemného oznámení dle předchozí věty.

15.3 Kontaktními osobami za stranu objednatele jsou:

a) ve věcech smluvních a obchodních [redacted]

b) v otázkách technických [redacted]

15.4 Kontaktními osobami za stranu poskytovatele jsou:

a) ve věcech smluvních a obchodních [redacted]

b) v otázkách technických [redacted]

15.5 Požadavky na poskytnutí Služeb uvedených v technické specifikaci bude poskytovatel přijímat na tel.: [redacted]

16. ZÁVĚREČNÁ USTANOVENÍ

16.1 Tato Smlouva se uzavírá na dobu určitou, a to na dobu maximálně 4 let ode dne nabytí účinnosti Smlouvy. Tato Smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami. Smlouva nabývá účinnosti dnem uveřejnění výzvy k poskytnutí služeb prostřednictvím registru smluv dle zákona č. 340/2015 Sb., o registru smluv. Zveřejnění Smlouvy a výzvy k poskytnutí služeb v registru smluv zajistí objednatel.

16.2 Pokud ve Smlouvě není stanoveno jinak, řídí se právní vztahy z ní vyplývající příslušnými ustanoveními občanského zákoníku.

16.3 Smluvní strany se dohodly, že nad rámec výslovných ustanovení této Smlouvy nebudou jakákoliv práva a povinnosti dovozovány z dosavadní či budoucí praxe zavedené mezi smluvními stranami či zvyklostí zachovávaných obecně či v odvětví týkajícím se předmětu plnění této Smlouvy, ledaže je ve Smlouvě výslovně sjednáno jinak. Pro vyloučení pochybností smluvní strany výslovně potvrzují, že na závazky z této Smlouvy vzniklé se nepoužijí tato ustanovení § 1765 občanského zákoníku.

16.4 V případě, že některé ustanovení této Smlouvy je nebo se stane v budoucnu neplatným, neúčinným či nevymahatelným nebo bude-li takovým příslušným orgánem shledáno, zůstávají ostatní ustanovení této Smlouvy v platnosti a účinnosti, pokud z povahy takového ustanovení nebo z jeho obsahu anebo z okolností, za nichž bylo uzavřeno, nevyplývá, že je nelze oddělit od ostatního obsahu této Smlouvy. Smluvní strany se zavazují nahradit neplatné, neúčinné nebo nevymahatelné ustanovení této Smlouvy ustanovením jiným, které svým obsahem a smyslem odpovídá nejlépe ustanovení původnímu a této Smlouvě jako celku.

16.5 Všechny spory mezi Smluvními stranami, vzniklé z právních vztahů založených Smlouvou a/nebo v souvislosti s ní, budou řešeny smírnou cestou. V případě, že smluvní strany nedosáhnou jednáním smírného řešení kteréhokoliv sporu vzniklého z právních vztahů založených Smlouvou nebo v souvislosti s ní, může se kterákoli smluvní strana obrátit na věcně a místně příslušný soud České republiky s návrhem na rozhodnutí sporné otázky.

16.6 Veškeré změny či doplnění této Smlouvy s výjimkou změn oprávněných osob lze činit pouze na základě písemné dohody Smluvních stran. Takové dohody musí mít podobu datovaných, číslovaných a oběma Smluvními stranami podepsaných dodatků Smlouvy. Oprávněné osoby jsou Smluvní strany oprávněny kdykoli změnit, a to jednostranným prohlášením. Změna je účinná okamžikem doručení oznámení druhé Smluvní straně.

16.7 Poskytovatel nesmí postoupit jakoukoliv pohledávku vzniklou z této Smlouvy, nebo v souvislosti s ní, třetí straně bez předchozího písemného souhlasu Objednatele.

16.8 Nedílnou součást Smlouvy tvoří tyto přílohy:

Příloha č. 1:	Technická specifikace
Příloha č. 2:	Situační plánek
Příloha č. 3:	Popis pronajatých prostor
Příloha č. 4:	Cena
Příloha č. 5:	Seznam poddodavatelů
Příloha č. 6A	Vyrozumění o významném dodavateli
Příloha č. 6B:	Požadavky na systém řízení bezpečnosti informací (Kybernetické požadavky)
Příloha č. 7	Dotazník Významného dodavatele

Příloha č. 8 Čestné prohlášení o neexistenci střetu zájmů

Příloha č. 9 Čestné prohlášení účastníka o splnění nařízení Rady EU 2022/576

16.1 Poskytovatel souhlasí s uveřejněním Smlouvy na profilu objednatele (zadavatele) a v registru smluv, a to včetně požadovaných metadat, dle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů.

16.2 Smlouva je vyhotovena a smluvními stranami podepsána ve čtyřech (4) vyhotoveních s platností originálu, z nichž objednatel obdrží (2) vyhotovení a poskytovatel (2) vyhotovení. Je-li Smlouva podepsána elektronicky, pak je podepsána v jednom (1) originále pomocí uznávaných elektronických podpisů osob oprávněných jednat za smluvní strany.

16.3 Smluvní strany prohlašují, že si Smlouvu řádně přečetly, s jejím obsahem souhlasí a na důkaz toho ji stvrzují svými podpisy.

Za objednatele	**Za poskytovatele**
[redacted]	
Česká republika - Ústav zdravotnických informací a statistiky České republiky prof. RNDr. Ladislav Dušek, Ph.D. ředitel ÚZIS	**O2 Czech Republic a.s.** [redacted]

Příloha č. 1

Technická specifikace

Technická specifikace

Cílem zadavatele je vybudování primárního datového centra elektronického zdravotnictví. Struktura provozovaných infomačních systémů v tomto datovém centru vyžaduje zajištění vysoké dostupnosti a úrovně zabezpečení dle zákona 181/2014 Sb., a návazných legislativních norem pro provoz kritické informační infrastruktury (dále jen „**KII**“) a významné informační systémy (dále jen „**VIS**“).

Z těchto důvodu požadujeme, aby Účastník disponoval prostorem pro účely provozování datových center s vysokými technickými parametry nejméně dle standardu TIER III a následujících parametrů, Zadavatel požaduje zajištění uvedených parametrů po dobu maximálně 4 let od podpisu smlouvy a požaduje v rámci výše uvedených parametrů poskytnutí služby v následujícím rozsahu:

Požadavky na datové centrum (pro účely Smlouvy také jen „ostatní služby“):

Požadavky na umístění

Zadavatel požaduje, aby datové centrum bylo umístěno ve vzdálenosti od sídla Zadavatele a sekundárního datového centra DC2 v Praze tak, aby nemusel doplnit infrastrukturu SAN o speciální prvky umožňující komunikaci SAN po optickém kabelu na trase delší 25 km.

Bezpečnostní požadavky

- Neustálé kamerové monitorování datového centra v režimu 24/7 po celý kalendářní rok.
- Neustálé kamerové monitorování pohybu osob okolo rack skříní tak aby byla dokumentována veškerá manipulace s rack skříněmi a jejich obsahem v režimu 24/7 po celý kalendářní rok.
- 24x7 ostraha s podporou elektronického zabezpečovacího systému.
- Oddělení zařízení do bezpečnostních zón, pomocí kterých je pohyb řízen elektronickým systémem kontroly přístupu.
- Bezpečnostní postupy pro všechny provozní scénáře datového centra.
- Automatická detekce požáru a systému rychlé detekce kouře včetně stabilního centrální hasícího systému .
- Poskytovatel se zavazuje v řádném termínu a včas implementovat požadavky připravované směrnice NIS2 a novely zákona o kybertické bezpečnosti, dle https://osveta.nukib.cz/course/view.php?id=145

Provozní požadavky

- Poskytnutí vyhrazené klimatizované uzavřené klece s elektronicky řízeným přístupem (přístupové karty nebo jiný předmět vydaný na osobu nebo pomocí biometriky (otisk prstu, sítnice apod.)), a stálým kamerovým monitoringem pro 5 standardních „hlubokých“ RACK skříní 19“ s rozměrem 60x120cm, které budou doplněné o další jednu až dvě RACK skříně v průběhu druhé poloviny roku 2024 s možností rozšíření o další 3 RACK skříně v průběhu účinnosti Smlouvy.

- Zajištění služby vyhrazeného trezoru pro zálohovací pásky o kapacitě min. 60ti pásek LTO8. s řízeným přístupem pro vybrané pracovníky Zadavatele v režimu 24x7.
- Zajištění služby vzdálených rukou 24x7.
- Redundantní chladící systémy s možností chlazení rackových skříní na stabilní teplotu maximálně 25°C.
- Zajištění stabilní relativní vlhkosti 20 až 55% při teplotě 20°C.
- Zajištění řízeného přístupu 24x7 ke kleci zaměstnanců Zadavatele a jejich doprovodu. Zadavatel s určitostí neví jak často a v jakých hodinách bude ke svému technickému vybavení docházet. Zadavatel předpokládá, že jednou týdně vyjma řešení technických incidentů a událostí, které bude nucen bezodkladně řešit v jakémkoli čase a dni.
- Zajištění neustálého kamerového monitoringu se záznamem uchovávaným min. 90 kalendářních dní. Zadavatel požaduje umožnění přístupu k uloženým kamerovým záznamům včetně provedení kopie záznamu bez udání důvodu.
- Prostor s plášťovou ochranou bez oken.
- Možnost zavedení redundantní připojení k páteři internetu k rackovým skříním.
- Možnost zavedení DarkFiber k rackovým skříním.

Požadavky na dodávku elektrické energie

- Zajištění redundantního napájení elektrickou energií (A+B) 230 AC min. 6kW/Rack na jednu skříň včetně jištění min. 3x 16A a měřením spotřeby elektrické energie na každý Rack samostatně.
- Zajištění bez výpadkového provozu 24x7.
- Datové centrum má zajištěné přednostní dodávky paliva pro záložní zdroje elektrické energie
- Disponuje bez výpadkovým záložním zdrojem elektrické energie s autonomním provozem bez nutnosti doplnění paliva generátorů v délce minimálně 24h.
- Disponuje dva a více nezávislých elektrických okruhů.

Požadavky na datové služby (pro účely Smlouvy také jen „datové služby“):

- Zajištění redundantního připojení k síti internet bez omezení 2x2Gbps.
- Zajištění čtyř optických propojení tzv. DarkFiber (čtyři páry) s lokalitou stávajícího datového centra zadavatel DC2 pro redundantní komunikaci SAN a LAN.
- Zajištění 128 pevných veřejných IP adres IPV4 v jednom Subnet a 256 IPV6 s možností dalšího navýšení počtu.

Stěhování techniky ze stávajícího datového centra

Zadavatel v současné době provozuje své provozní prostředí v DC1. V tomto datovém centru má instalováno pět technikou osazených 19“ racků. Zadavatel požaduje, aby dodavatel zajistil přesun této techniky do prostor svého datového centra, provedl její zapojení a ve spolupráci se Zadavatelem zajistil její opětovné uvedení do provozu.

Zadavatel požaduje, aby dodavatel přemístil techniku na své náklady a zaručil, že technika nebude nijak poškozena, v případě poškození uhradil veškeré škody plynoucí, zejména:

- Oprava nebo výměna poškozené techniky;
- Náhrada škod způsobených nedostupností služeb, které jsou provozovány v rámci provozního prostředí Zadavatele, tedy i systémů KII dle zákona 181/2014 Sb. o kybernetické bezpečnosti;

- Náhrada veškerých nákladů zadavatele spojených s obnovou provozu služeb způsobených poškozením techniky.

Zadavatel požaduje, aby přemístění techniky nezpůsobilo výpadek provozu provozovaných systémů v pracovních dnech a ve dnech pracovního klidu. Přemístění techniky bude umožněno v nočních hodinách v rozmezí nocí z pátku na sobotu nebo ze soboty na neděli v časovém intervalu 20 – 05 hodin s tím, že v rozmezí 06-19h musí být vždy všechny provozované služby plně dostupné.

Podmínky pro stěhování výpočetní techniky do nového datového centra

Ústav zdravotnických informací a statistiky ČR (ÚZIS ČR) je provozovatelem a správcem řady infomačních systémů včetně Národního zdravotnického systému NZIS a Integrovaného infomačního systému hygienické služby IISHS. Mimo tyto systémy provozuje ÚZIS ČR řadu dalších provozních a agendových systémů včetně systému spisové služby, ekonomických systémů apod.

Vybrané provozované systémy jsou navíc provozovány v režimu dle zákona 181/2014 Sb. o kybernetické bezpečnosti v režimu VIS a KII. Tyto systémy včetně dalších systémů, které v rámci NIZIS nebo IISHS sbírají nebo poskytují data pro další resortní systémy musí být provozovány v režimu vysoké dostupnosti bez výpadkově nebo s minimálním plánovaným výpadkem mimo dobu aktivního používání, převážně nočních hodinách, ale mimo čas, kdy probíhají sběry a vyhodnocování dat.

Případně stěhování techniky musí být podřízeno výše uvedeným provozním a časovým aspektům a veškeré kroky a činnosti pečlivě naplánovány.

Stávající stav

ÚZIS ČR provozuje výše uvedené systémy v rámci hardware umístěného do pěti rackových skříní. Skříně obsahují síťové prvky, servery, datová úložiště, prvky bezpečnostní infrastruktury a další. V rámci hardware je provozováno 187 virtuálních serverů a diskový prostor o objemu cca 380 TB.

V případě, kdy bude uzavřena smlouva s vybraným účastníkem, který provozuje datové centrum v jiné lokalitě, zajistí vybraný účastník veškeré podmínky pro co nejrychlejší znovu zprovoznění techniky a infomačních systémů.

Přesný postupový a časový plán stěhování techniky bude stanoven před zahájením prací dohodu obou stran. Zásadní podmínkou je, aby toto stěhování nezpůsobilo Zadavateli, žádné více náklady a neohrozilo kontinuální provoz systémů.

Zadavatel požaduje, aby vybraný dodavatel zajistil na své náklady náhradní hardware pro dočasnou instalaci systémů Zadavatele včetně zajištění potřebné konektivity do internetu a sekundárního datového centra Zadavatele ve stejných parametrech, jak je uvedeno v Zadávacích podmínkách. Instalace a konfigurace všech potřebných systémů na náhradní hardware zajistí také dodavatel dle informací poskytnutých zadavatelem.

Dále Zadavatel požaduje, aby nový Dodavatel poskytl veškerou součinnost při:

1) Tvorbě postupového a časového plánu stěhovaní, zejména:
   a) Příprava a parametry síťové konektivity
   b) Plán dočasných instalací
   c) Provozní plán dočasného provozu
   d) Expediční plán přesunu techniky
   e) Plán znovu zprovoznění systému
   f) Plán ukončení dočasného provozu

2) Zajištění provozního prostředí
   a) Zajištění síťové konektivity
   b) Zajištění vlastního provozního prostoru
3) Zajištění přesunu techniky
   a) Zajištění tras pro přesun
   b) Zajištění bezpečné dopravy
   c) Zajištění náhradního hardware v případ poškození přesouvané techniky
   d) Zapojení techniky v provozním prostoru spočívající:
      I. Zajištění elektrického napájení v místě umístění techniky
      II. Zajištění objednané síťové konektivity
      III. Umístění racků do provozního prostoru
      IV. Poskytnutí součinnosti při kontrole stavu kybernetické bezpečnosti
         1. Předložení provozního řádu/provozních metodik datového centra
         2. Předložení metodiky a vlastního provozního deníku
         3. A dalších náležitostí dle požadavků na významného dodavatele dle ZoKB.
4) Poskytnutí součinnosti při znovu zprovoznění systémů
   a) Poskytnutí veškerých technických parametrů pro konfiguraci síťového prostředí
   b) Poskytnutí maximální součinnosti při migraci dat z dočasného provozního prostředí
   c) Ukončení dočasného provozu včetně auditovaného výmazu dat z dočasného úložiště dat nebo auditované fyzické zničení disků.

Ostatní podmínky

Zadavatel požaduje, aby vybraný účastník měl zajištěný náhradní hardware pro případ, kdy dojde během přesunu techniky k jejímu poškození. Náhradní technika bude ve stejné nebo vyšší konfiguraci nežli stěhovaná technika, viz Seznam stěhované techniky. V případě, kdy dojde k poškození techniky poskytne dodavatel náhradní bez zbytečného odkladu maximálně však do 24h od zjištění poškození.

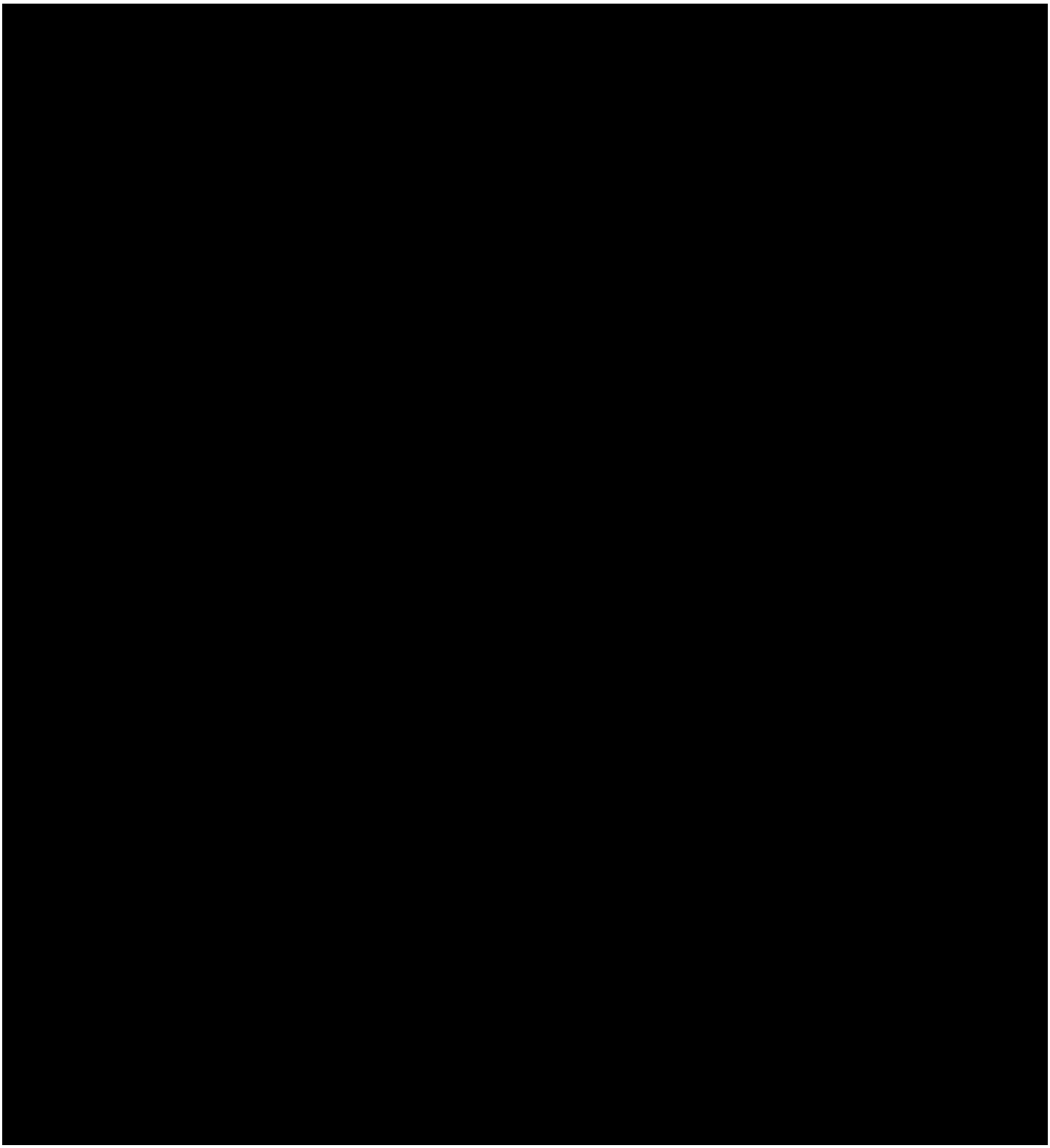
Seznam stěhované techniky

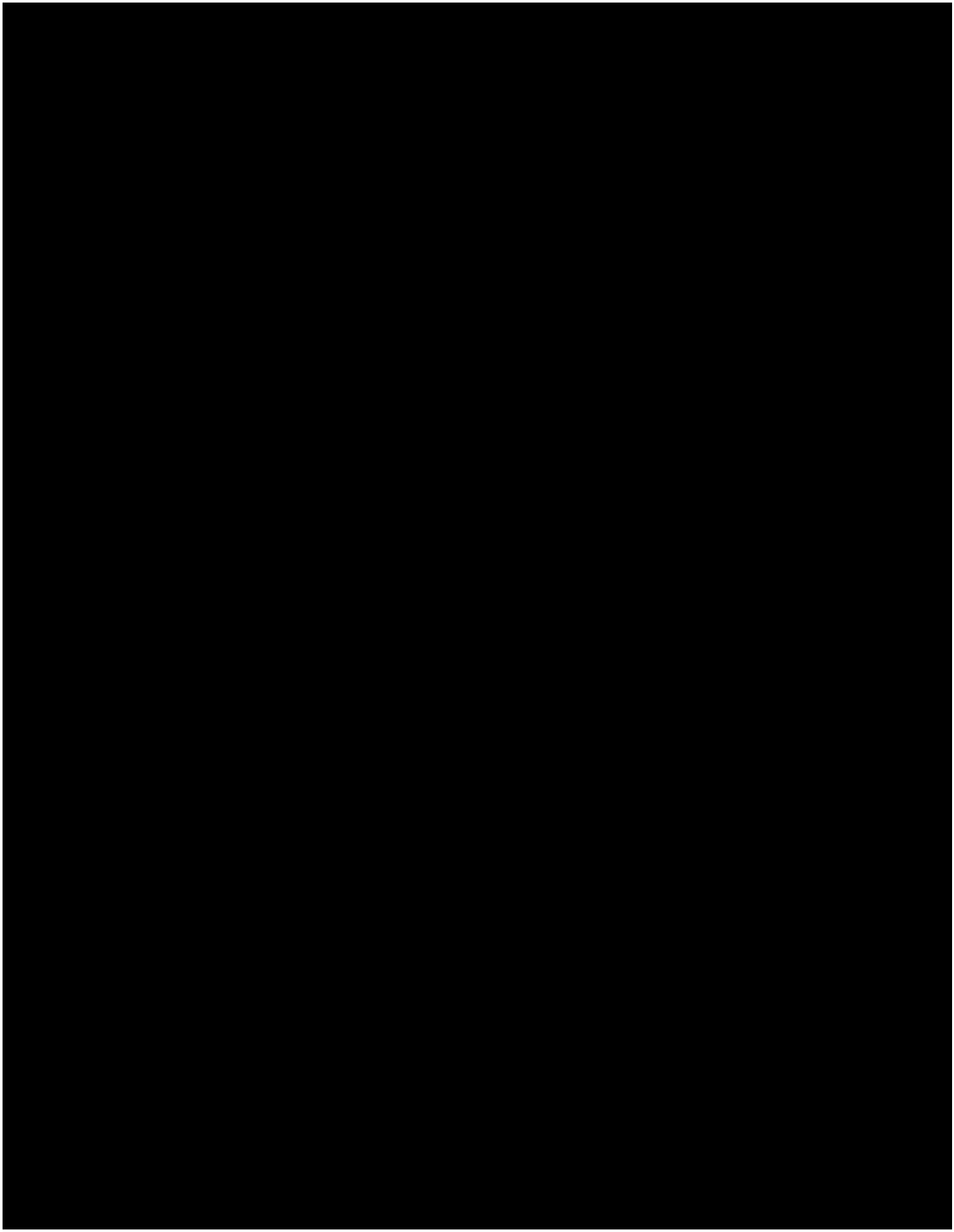
Název	Model a výrobce	Konfigurace	Ks
Firewall	FortiGate 1200D	*(přesně určeno daným typem)*	2
Aplikační balancer	FortiADC-400F	*(přesně určeno daným typem)*	1
Aplikační firewall	FortiWeb 1000E	*(přesně určeno daným typem)*	1
Centrální switch	HPE 10504	96*10GE SFP+ (48+48), 96 *GE (48+48)	1
Optický switch	HPE 5940	24*10GE SFP+, 4*40GE QSFP+, 24*X130 SFP+	2
SAN switch	HPE SN6000B	24 (max 48) * FC16, 23*SW SFP+, 1*LW SFP+ 20km	2
LAN switch	HPE 5130-48G PoE	48*GE, 4*10GE SFP+, PoE2, 4*X130 SFP+	2
WLAN controller	HPE 7205 RW	*(přesně určeno daným typem)*	1
HSM modul	Luna 7 S750	5 partitions, 10 client licences	2
Diskové pole	HP 3PAR 8400	Celkem 12 polic, z toho 9 polic po 22 discích FC 1.8TB 10K SFF, dvě police po 16 discích 1.92TB SSD SFF a jedna police s 12 disky 6TB LFF. Celková kapacita diskových polí činí 22TB SSD a 380 TB FC prostoru.	1
Pásková knihovna	HPE MSL3040	80 slotů (kapacita 960TB), 2*LTO8 Ultrium 30750 FC8 Drive	1

Serverové chassis	HPE Synergy 12000	HPE Synergy 12000 frame, 8*10GLAN, 8*FC8, o sazeno 12ks HPE Synergy 480 Gen10 (1*Intel Xeon 6248, 2*240GB SSD, 512GB RAM, HPE Synergy 3820C 20GB CNA), Win2019DTC,...	2
Server	HPE DL360 Gen10	1*Xeon 4210, 1*600GB, 128GB RAM, 4GLAN, 2FC16, 8SFF, ...	2
Server	HPE DL380 Gen10	2*Xeon 4210, 28*2.4TB, 512GB RAM, 4GLAN, 2FC16,24SFF, ...	2
Server	HP DL 380 Gen9	2*Xeon E5-2640v5, 12*6TB + 2*800GB, 64RAM, 2xSFP+, 2xFC16, ...	1
Server	HP DL 320e	1*Xeon E3-1220v2, 4*4TB, 32RAM, 4GLAN	1
Synology	RS3617xs	12*6TB	1
Synology	RS1221+	8*12TB, 2xSFP+	1
Synology	RS819	4*6TB	1
Synology	DX418	4*12TB	1
SMS brána	nxs-9700 4G	*(přesně určeno daným typem)*	2
SMS brána	hwg-sms-gw3	*(přesně určeno daným typem)*	1

Příloha č. 2

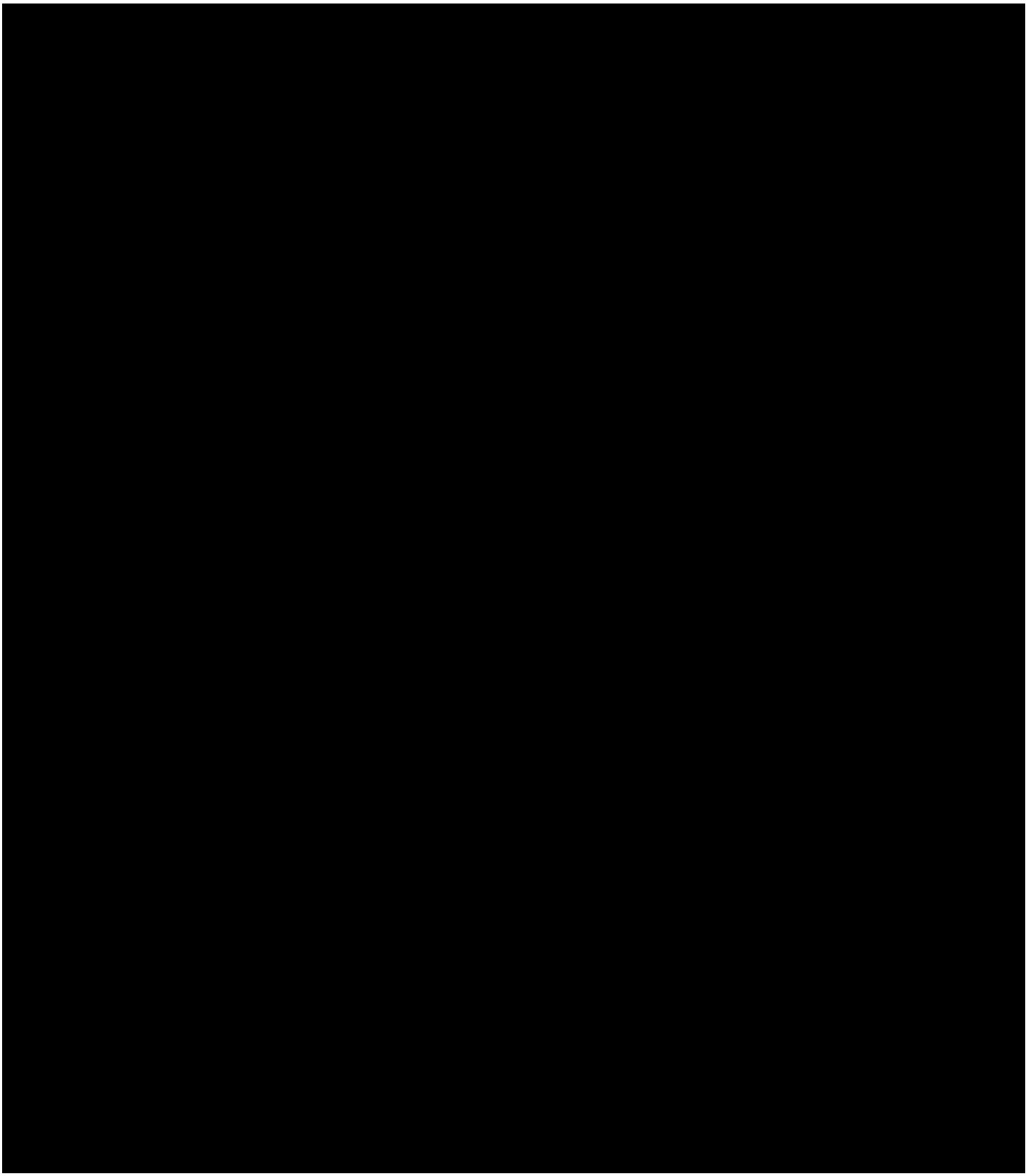
Situační plánek

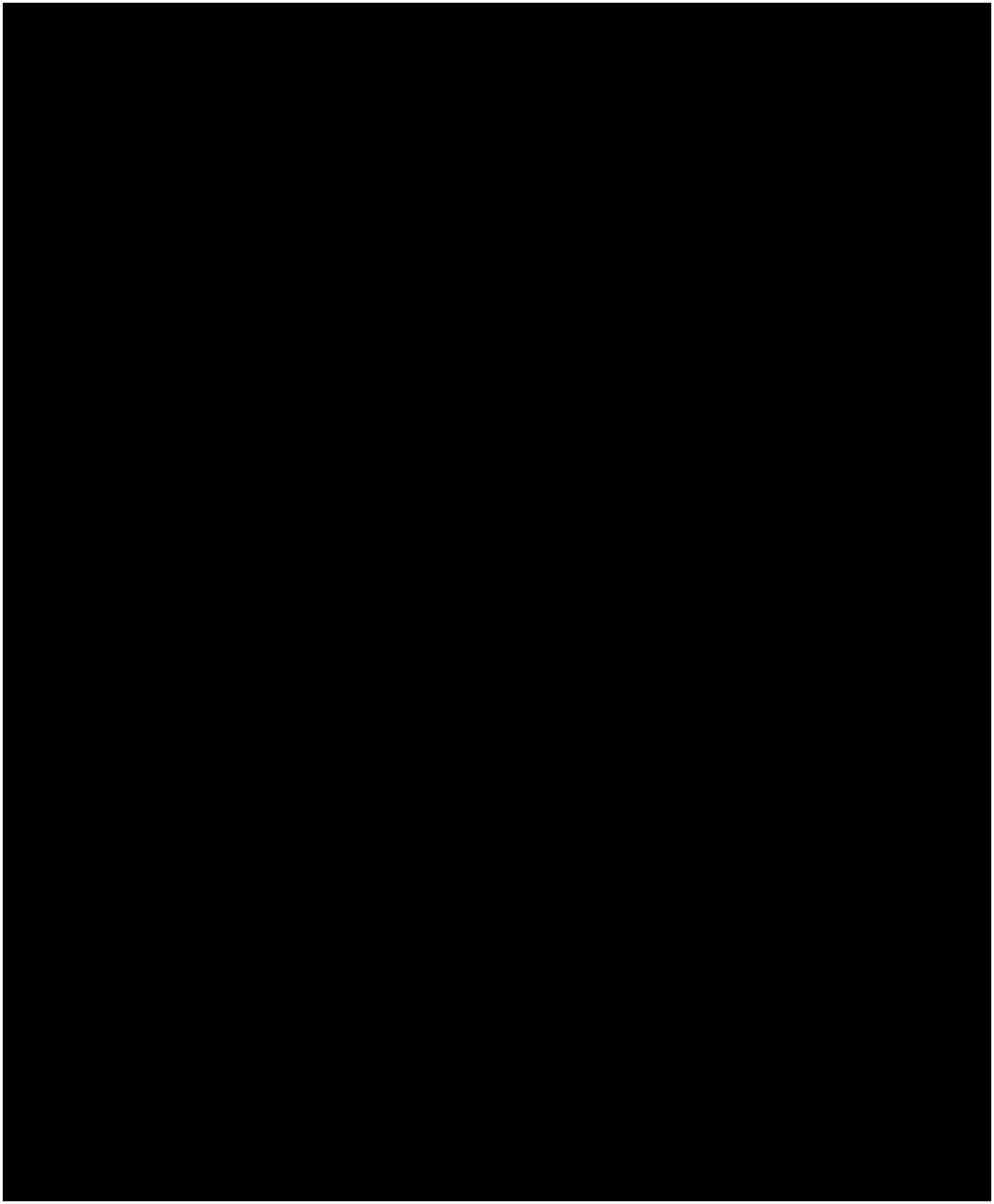


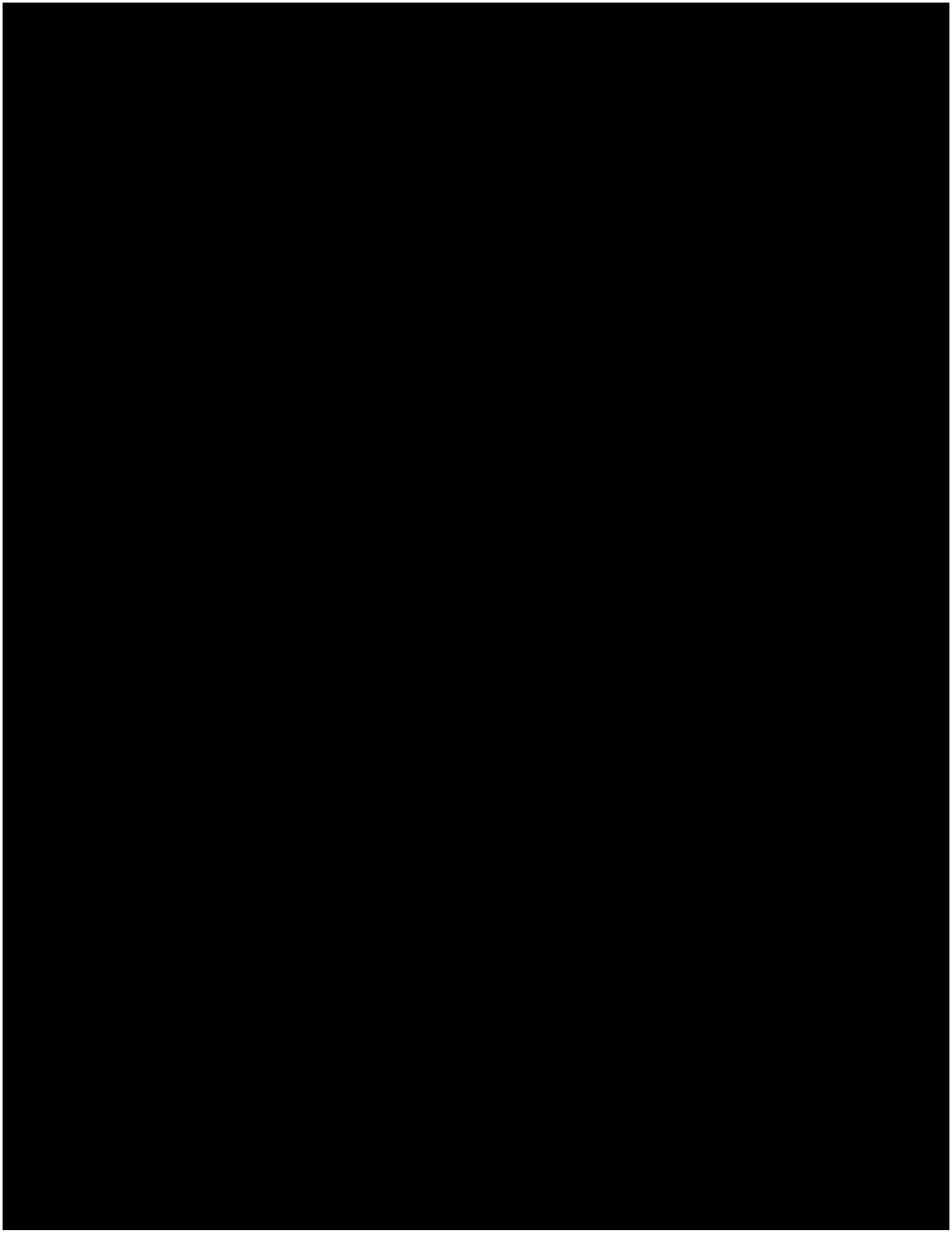


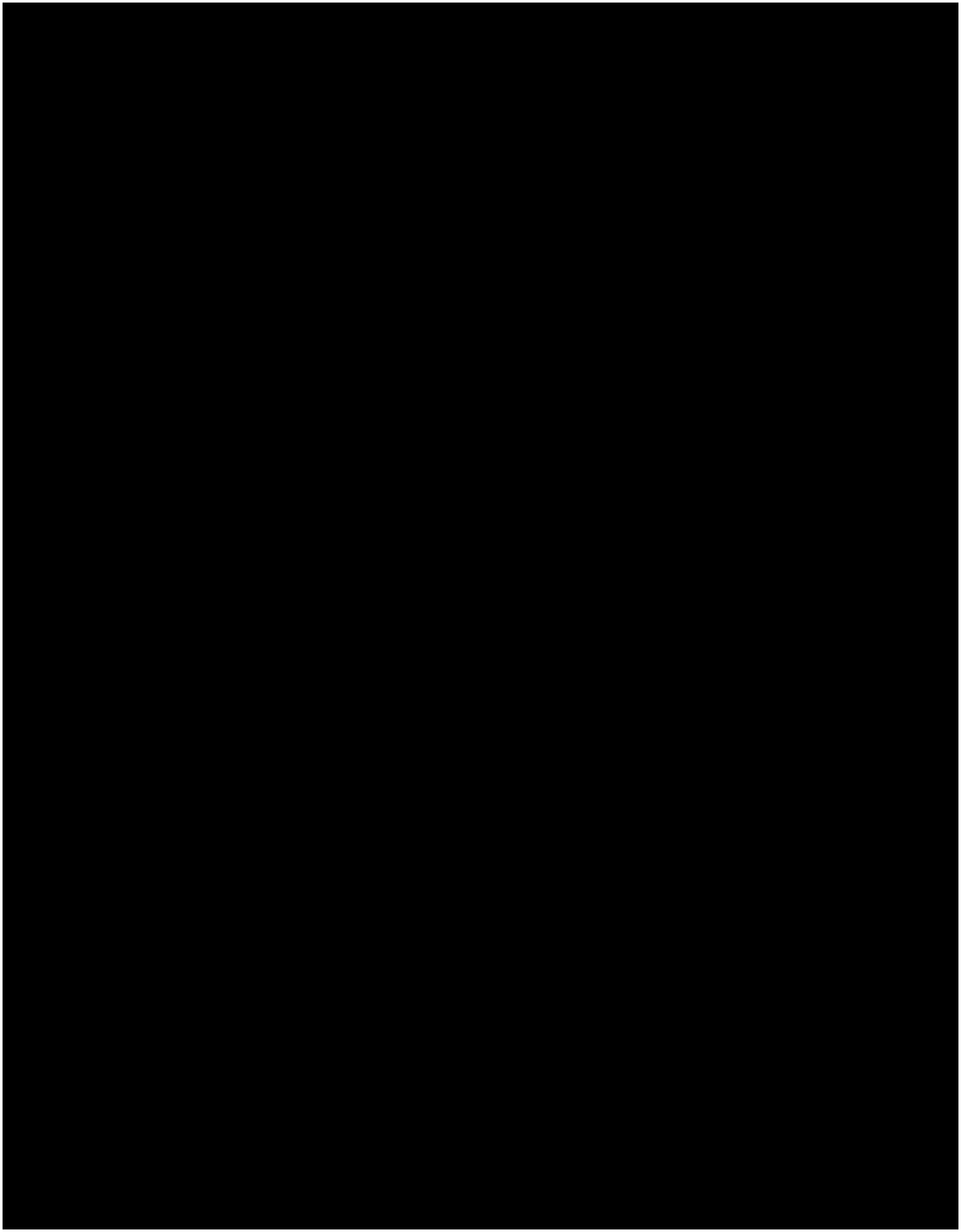
Příloha č. 3

Popis pronajatých prostor









Příloha č. 4

Cena

Cena poskytnutí služby - "Datové centrum"

Služby	Cena v CZK bez DPH za 1 měsíc[1]	Cena v CZK s DPH za 1 měsíc
Poskytnutí datových a ostatních s užeb d e techn cké spec f kace (vyjma dodávky (spotřeby) e . energ e včetně PUE)	[redacted]	[redacted]

Energie	Cena v CZK za 1kWh vč. PUE	Cena v CZK bez DPH za 1 měsíc[2]	Cena v CZK s DPH
Dodávka (spotřeba) e ektr cké energ e včetně max má ního garantovaného PUE[3]	[redacted]	[redacted]	[redacted]

PŘEDMĚT HODNOCENÍ:	Cena v CZK bez DPH	Cena v CZK s DPH
Nabídková cena celkem za 1 měsíc[4]	[redacted]	[redacted]

Pozn. č. 1: ***fixní cena služeb dle technické specifikace (vyjma dodávky elekrické energie včetně maximálně garantovaného PUE) po celou dobu účinnosti smlouvy***
Účastník souhrnně nacení do buňky G6 níže uvedené datové a ostatní služby za jeden kalendářní měsíc:

Pozn. č. 2: ***v buňce G 10 je dopočítána cena za dodávku elektrické energie včetně maximálně garantovaného PUE za 1 kalendářní měsíc, tj. za dodání 8000 kWh (průměrná spotřeba za 1 kalendářní měsíc) včetně maximálně garantovaného PUE, které by nemělo přesáhnout hodnotu 1,5***

Pozn. č. 3: ***fixní cena za 1 kWh včetne maximálně garantovaného PUE je závazná v prvních 6ti měsících od data zahájení plnění; ukazatel PUE nesmí přesáhnout maximální garantovanou hodnotu 1,5***

Pozn. č. 4: ***nabídková cena za 1 měsíc plnění (fixní cena za poskytnutí datových a ostatních služeb + fixní cena za dodávku el. energie včetně PUE v prvních 6ti měsících plnění)***

Příloha č. 5

Seznam poddodavatelů

1.

Název:	CETIN a.s.
Sídlo:	Českomoravská 2510/19, Libeň, 190 00 Praha 9
Právní forma:	Akciová společnost
Identifikační číslo:	04084063
Rozsah plnění Smlouvy:	Pronájem prostor v datovém centru

Příloha č. 6 A

Vyrozumění o Významném dodavateli

Vyrozumění Poskytovatele o skutečnosti, že v souladu §8 s vyhláškou 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 Vyhláška ZoKB) se podpisem této Smlouvy stává Významným dodavatelem.

1. Identifikace Správce a Provozovatele
   Ústav zdravotnických informací a statistiky České republiky
   Organizační složka státu
   se sídlem: Palackého náměstí 4, PSČ 128 01 Praha 2
   IČO: 00023833
   zastoupen: prof. RNDr. Ladislavem Duškem, Ph.D. ředitelem
   (dále jen „Správce a Provozovatel“)

2. Identifikace informačního a komunikačního systému
   a) ICT infrastruktura Datových center, které je využita pro provoz Významných infomačních systémů a Kritických infomačních systémů ve smyslu zákona 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů.
   b) ICT infrastruktura umístěna v ostatních prostorách Správce a Poskytovatele, či Správce za jejichž provoz Správce a Provozovatel odpovídá a ve smyslu Vyhlášky ZoKB je Provozovatelem.
   c) Veškeré Typové infomační systémy ve smyslu Vyhlášky ZoKB

Vysvětlení.:
ICT infrastrukturou jsou myšleny všechny aktivní i pasivní prvky počítačové sítě, servery a jejich operační systémy, úložiště dat, zálohovací systémy a hardware, dohledové a SIEM aplikace a hardware, veškeré koncové stanice, databázové stroje, a další Podpůrná či technická aktiva využívaná pro provoz a správu KII a VIS ve smyslu zákona 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů.

3. Identifikace Významného dodavatele

Název společnosti	O2 Czech Republic a.s.
Sídlo	Praha 4 - Michle, Za Brumlovkou 266/2, PSČ 14022
IČO	60193336
Zastoupen	[redacted]

(dále jen „Významný dodavatel“)

4. Pravidla Poskytovatele

   V souladu s §8 odstavce 1 písmene a) vyhlášky 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) je Významný dodavatel povinen dodržovat pravidla, která zohledňují požadavky systému řízení bezpečnosti informací dle Přílohy č. 6B této Smlouvy.

Příloha č. 6 B

Požadavky na systém řízení bezpečnosti informací ve smyslu §8 Vyhlášky 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

(Kybernetické požadavky)

§ 3 Systém řízení bezpečnosti informací

Poskytovatel (pro účely této přílohy dle VKB dále jen „**Dodavatel**“) se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §3 vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (dále jen „**VKB**“), které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:

a. Prosadit bezpečnostní zásady a procesy, které budou pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně Dodavatele při poskytování předmětu plnění.

b. Na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění, monitorovat je, vyhodnocovat jejich účinnost.

c. Vést záznamy o vytváření a zpracování dat a informací v rozsahu poskytovaného předmětu plnění, zaznamenávat veškeré podstatné okolnosti související se zajištěním bezpečnosti těchto dat a informací a na vyžádání tyto záznamy Objednateli zpřístupnit.

d. Stanovit a udržovat aktuální bezpečnostní politiku, která bude pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně Dodavatele při poskytování předmětu plnění. Bezpečnostní politika musí obsahovat hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací.

e. Stanovit a udržovat aktuální opatření bezpečnosti ve formě procesů a technologií, které zajišťují naplnění bezpečnostní politiky.

§ 4 Řízení aktiv

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §4 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:

    a. Stanovit a udržovat rozsah a seznam aktiv využívaných pro plnění této Smlouvy (pro účely této přílohy dle VKB dále jen „smlouva“) (aktivy se rozumí např. data a informace k předmětu plnění dle této smlouvy, systémy ICT, moduly, HW prvky - infrastruktura hlasové a datové komunikace, aplikace, databáze, servery, úložiště, koncová zařízení – pracovní stanice typu osobní počítač nebo notebook, mobilní koncová zařízení – přenosná zařízení typu telefon, tablet, notebook, netbook, PDA, apod.), a tato aktiva strukturovaně popsat a Objednateli předložit do 30 dnů od podpisu této smlouvy a následně na vyžádání, a to po celou dobu trvání smlouvy a do 2 let po jejím ukončení.

§ 5 Řízení rizik

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §5 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:
    a. Řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění.
    b. V minimálním intervalu 1x ročně vytvořit a předložit Zprávu o řízení kybernetických rizik, která bude minimálně pokrývat:
        i. Vyhodnocení stavu kybernetické bezpečnosti za hodnocený rok
        ii. Identifikaci a hodnocení rizik s vazbou na předmět plnění
        iii. Realizovaná bezpečnostní opatření
        iv. Nepokrytá bezpečnostní rizika a návrh opatření
        v. Vyhodnocení bezpečnostních událostí a incidentů
        vi. Aktuální stav souladu Dodavatele s těmito Kybernetickými požadavky

§ 6 Organizační bezpečnost

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §6 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:
    a. Jmenovat nejpozději do 5 dnů po uzavření této smlouvy odpovědnou kontaktní osobu pro potřeby zajištění plnění těchto Kybernetických požadavků a související komunikaci mezi Stranami dohody (dále také jen „Kontaktní osoba“). Kontaktní osobu sdělí Dodavatel písemně Objednateli v téže lhůtě. Objednatel stanovuje, že určení Kontaktní osoby pro bezpečnost na straně Dodavatele nemá dopad na odpovědné osoby ve věcech smluvních a technických.
    b. Využívat pro poskytování předmětu plnění pouze oprávněných osob, které byly řádně seznámeny příslušnými ustanoveními interních řídících aktů Objednatele a mají ověřenou kvalifikaci, znalosti a zkušenosti k řádnému poskytování předmětu plnění.

§ 8 Řízení dodavatelů

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §8 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:
    a. Využívá-li při poskytování předmětu plnění poddodavatele, zajistit adekvátní dodržování Kybernetických požadavků rovněž ve smluvních vztazích se svými poddodavateli, přičemž tuto skutečnost se Dodavatel zavazuje doložit Objednateli do 10 dnů od podpisu příslušné Prováděcí smlouvy, na jejímž plnění se budou poddodavatelé podílet, písemné prohlášení o dodržování Kybernetických požadavků u svých poddodavatelů.
    b. Pokud při poskytování předmětu plnění dochází ke zpracování osobních údajů, zajistit uzavření samostatných smluv (tj. smluv se svými poddodavateli, zaměstnanci a

případnými dalšími osobami podílejícími se na poskytování plnění z této smlouvy) ve smyslu GDPR a ZZOÚ

§ 9 Bezpečnost lidských zdrojů

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §9 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:
    a. Zajistit, aby Kontaktní osoba nejpozději do 30 dnů od uzavření smlouvy potvrdila písemně Objednateli, že všechny osoby podílející se na poskytování předmětu plnění za stranu Dodavatele byly prokazatelně seznámeny s těmito Kybernetickými požadavky a příslušnými ustanoveními interních řídících aktů Objednatele.
    b. Dodržovat příslušná ustanovení interních řídících aktů Objednatele v rozsahu, v jakém byl s těmito akty seznámen. Za prokazatelné seznámení se považuje školení pracovníků Dodavatele zajištěné Objednatelem, protokolární či elektronické předání příslušné dokumentace nebo Objednatelem zajištěný přístup na sdílené úložiště obsahující příslušné interní akty řízení.
    c. V případě, že je součástí předmětu plnění služba dohledu nad předmětem plnění, definovat a naplnit role a odpovědnosti pro monitoring sítě a zařízení v rozsahu předmětu plnění.
    d. Zajistit, aby osoby podílející se na poskytování plnění Objednateli v prostředí nebo s prostředky Objednatele, a to i tehdy, pokud jsou prostředky Objednatele používány mimo jeho prostředí:
        i. Pro uložení a sdíleni dat a informací Objednatele využívali pouze k tomu schválené prostředky (aktiva);
        ii. Neukládali ani nesdíleli data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno Objednatele;
        iii. Nestahovali, nesdíleli, neukládali, nearchivovali ani neinstalovali datové a spustitelné soubory v rozporu s licenčními podmínkami nebo AZ;
        iv. Nenavštěvovali internetové stránky s eticky nevhodným obsahem;
        v. Nerealizovali pokusy o neautorizovaný přístup ke zdrojům Objednatele ani ke zdrojům jiných subjektů;
        vi. Nerealizovali pokusy o neoprávněnou modifikaci ani jiné neoprávněné zásahy do prostředků Objednatele, a to ani v případě, kdy jim byl prostředek Objednatele svěřen do správy;
        vii. Nepodíleli se s prostředky Objednatele na šíření spamu ani škodlivého softwaru.
2. Dodavatel si je vědom, že součástí podmínek pro získání přístupu ke zdrojům a aktivům Objednatele je na straně Objednatele *zpracování osobních údajů* pracovníků Dodavatele, kteří se podílejí na zajištění předmětu plnění. Pokud nebude Objednateli umožněno osobní údaje dotčených pracovníků Dodavatele zpracovat, nebude těmto pracovníkům umožněn žádný přístup ke zdrojům Objednatele.

§ 10 Řízení provozu a komunikací

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §10 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:

    a. Zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění.

    b. Na vyžádání poskytnout Objednateli přehled, report, či jinou adekvátní informaci o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře.

    c. Zajistit, že pro poskytování předmětu plnění budou využívány pouze aplikace a technologie, které jsou v souladu s platnou českou a evropskou legislativou, především s ohledem na licenční podmínky a AZ.

§ 11 Řízení změn

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §11 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:

    a. Přiměřeně reagovat na změny na straně Objednatele a upravit na své straně technická a organizační opatření tak, aby odpovídala novému stavu po provedení změny.

    b. Aktivně spolupracovat při testování významné změny.

§12 Řízení přístupu

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §12 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:

    a. Přidělovat oprávnění svým jednotlivým pracovníkům ve smyslu oprávnění k výkonu činností tak, aby byla minimalizována rizika nežádoucího přístupu k aktivům Objednatele.

    b. Zajistit, aby udělený přístup nebyl sdílen více osobami za stranu Dodavatele, pokud sdílený přístup nevyžaduje využívaná technologie. V takovém případě musí Dodavatel vést evidenci využívání sdílených přístupů a tuto na vyžádání předložit Objednateli kdykoli v průběhu trvání účinnosti této smlouvy a 2 roky po ukončení její platnosti.

    c. Stanovit v požadavku na přístup rozsah dat/informací, služby, účelu, pro které je přístup k systému ICT objednatele požadován a časový údaj o délce platnosti přístupu (např.: na dobu neurčitou / 1 rok / 1 měsíc / 1 den).

    d. Zajistit, aby osoby podílející se na poskytování předmětu plnění a mající přístup k informačním aktivům Objednatele chránily autentizační prostředky a údaje a nikdy neposkytovaly neautorizovaný přístup dalším osobám.

    e. Průběžně kontrolovat a vyhodnocovat oprávněnost a potřebu přístupu, jak fyzického, tak i logického, u všech osob na straně Dodavatele, které přistupují do prostředí Objednatele.

2. Dodavatel bere na vědomí, že přístup k systému ICT je možné povolit pouze fyzické identitě zaměstnance Dodavatele / poddodavatele Dodavatele zaevidované v *Active Directory* (registr identit), a to na základě požadavku Dodavatele na přístup.
3. Dodavatel bere na vědomí, že přidělení oprávnění zaměstnanci Dodavatele musí být řízeno principem nezbytného minima a není nárokové.
4. Dodavatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele (osoby za stranu Dodavatele) může být příslušný účet zablokován a řešen jako bezpečnostní incident a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům Objednatele).

§ 13 Akvizice, vývoj a údržba

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §13 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:
    a. Zajistit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, které jsou předmětem plnění.
    b. Předat Objednateli dokumentaci předmětu plnění minimálně v následujícím rozsahu:
        i. dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů
        ii. dokumentaci obsahující popis autorizačního konceptu a oprávnění
        iii. dokumentaci obsahující instalační a konfigurační postupy
2. V případě, že předmět plnění zahrnuje vývoj softwaru, zavazuje se Dodavatel:
    a. Dodržovat a implementovat nejlepší praktiky pro bezpečný vývoj softwaru definované na základě smluvního vztahu.
    b. Na vyžádání umožnit Objednateli provedení auditu prováděného nebo provedeného plnění, předložit objednateli vyvíjený kód SW a výstupy z provedeného codereview (automatizovaně prostřednictvím bezpečnostního nástroje i manuálně), po jeho dokončení, pokud není v této smlouvě stanoveno jinak, a to zejména za účelem ověření skutečnosti, zda Dodavatel postupuje či postupoval při poskytování plnění v souladu se smlouvou a těmito Kybernetickými požadavky.
    c. Poskytovat Objednateli v termínech stanovených Objednatelem, resp. bez zbytečného odkladu požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje softwaru či kdykoli po jeho předání.
    d. Zajistit, že plnění bude obsahovat jen ty součásti, které jsou objektivně potřebné pro řádné provozování softwaru a/nebo které jsou specifikovány výslovně ve smlouvě (zejména, že software nebude obsahovat žádné nepotřebné komponenty, žádné programové vzorky apod.).
    e. Pokud je součástí plnění i instalace operačního systému případně softwaru třetích stran, zajistit v průběhu jeho instalace, že budou použity předepsané verze těchto produktů kompatibilní a funkční v prostředí Objednatele.
    f. Zajistit bezpečnost testovacího prostředí u Dodavatele a ochranu poskytnutých testovacích dat Objednatelem.

g. Zajistit, že do produkčního prostředí Objednatele bude dodán jen předmětem smlouvy specifikovaný kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování předmětu plnění.

h. Zajistit, že v rámci poskytovaného plnění bude dodávaný software

   i. v souladu s bezpečnostními politikami a standardy Objednatele

   ii. otestován na soulad s bezpečnostními politikami Objednatele (platí pro Dodavatele, pokud byl s takovými bezpečnostními politikami seznámen)

i. Instalovat software pouze na základě Objednatelem předem schválených migračních postupů.

j. Předat zdrojový kód Objednateli bezpečnou formou zajišťující jeho integritu.

k. Zajistit řízení verzí zdrojového kódu.

l. Zajistit zálohování zdrojového kódu a jeho uložení mimo produkční prostředí.

m. Zajistit, aby distribuce zdrojových kódy obsahovala soubor z vývojového prostředí na řízenou kompilaci těchto zdrojových kódů.

n. Nevyvíjet, nekompilovat a nešířit v prostředí Objednatele programový kód, který má za cíl nelegální ovládnutí, narušení dostupnosti, důvěrnosti nebo integrity nebo neautorizované či nelegální získání dat a informací.

§ 14 Zvládání kybernetických bezpečnostních událostí a incidentů

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §14 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:

   a. Stanovit a popsat na své straně činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání bezpečnostních incidentů.

   b. Bez zbytečného odkladu hlásit Objednateli všechny bezpečnostní události a incidenty s potenciálním negativním dopadem na Objednatele, a to stanoveným komunikačním kanálem nebo prostřednictvím Kontaktní osoby.

   c. Vyhodnocovat informace o bezpečnostních incidentech a uchovávat je pro budoucí použití s ohledem na požadavky platné české a evropské legislativy.

   d. V případě vzniku bezpečnostní události a následného zvládání a vyhodnocování bezpečnostního incidentu a/nebo v případě podezření na bezpečnostní incident poskytnout Objednateli aktivní součinnost a relevantní informace o podezřelém zařízení či osobě na straně Dodavatele.

   e. Bez zbytečného odkladu a po dohodě s Objednatelem realizovat opatření požadovaná Objednatelem v dohodnutých termínech ke snížení dopadu bezpečnostního incidentu nebo zamezení pokračování incidentu.

   f. Spolupracovat při analýze příčin bezpečnostního incidentu a navrhnout opatření s cílem zamezit jeho opakování v případě, že Dodavatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

2. Dodavatel bere na vědomí, že postup zvládání bezpečnostního incidentu či jiný důsledek porušení Kybernetických požadavků, jehož příčina je na straně Dodavatele, nebude posuzován jako okolnost vylučující odpovědnost Dodavatele za prodlení s řádným a včasným plněním předmětu této 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 této smlouvě nejsou tímto ustanovením dotčena.

§15 Řízení kontinuity činností

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §15 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:
    a. Zajistit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování předmětu plnění.
    b. Pravidelně kontrolovat a testovat, že je schopen kontinuitu aktiv zajistit dle sjednané úrovně služeb.

§ 16 Kontrola a audit

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §8 a §16 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění poskytnout adekvátní součinnost při výkonu kontroly Objednatele ze strany Úřadu dle § 23 ZKB.

§ 17 Fyzická bezpečnost

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §17 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:
    a. Dodržovat provozní řády budov (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny aktiva systémů ICT, anebo datové nosiče.
    b. V rozsahu předmětu plnění zajistit fyzické zabezpečení, zejména označení, uchování a likvidaci, instalačních, záložních nebo archivních médií a dokumentace v souladu s klasifikací aktiv Objednatele, pokud s ní byl Dodavatel seznámen.

§ 18 – 27 Bezpečnostní nástroje

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §18 až §27 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:
    a. Realizovat bezpečnostní opatření pro odstranění nebo blokování síťového spojení/síťových spojení, které/která neodpovídají požadavkům na ochranu integrity komunikační sítě.
    b. Realizovat přístup z mobilního zařízení do prostředí Objednatele pouze prostřednictvím zabezpečeného připojení virtuální privátní sítě (VPN) nebo zvolit adekvátní technické opatření.

c. Připojovat do prostředí Objednatele pouze ta síťová zařízení (switch, přístupový bod wifi, router, hub apod.), která prošla schvalovacím procesem a jejich připojení bylo schváleno oprávněnou osobu ve věcech technických na straně Objednatele určenou v této smlouvě.

d. Bez zbytečného odkladu deaktivovat všechna nevyužívaná zakončení sítě anebo nepoužívané porty aktivního síťového prvku, který je v rozsahu předmětu plnění a je ve správě Dodavatele.

e. Na aktiva Objednatele neinstalovat a nepoužívat v prostředí Objednatele tyto typy nástrojů, pokud nejsou součástí předmětu plnění:

   i. Keylogger – software nebo hardware, který neautorizovaně zaznamenává stisky kláves s cílem narušit důvěrnost zadávaných dat a informací.

   ii. Sniffer – software nebo hardware umožňující odposlouchávání síťového provozu.

   iii. Analyzátor zranitelností (scanner zranitelností) – softwarový nebo hardwarový nástroj umožňující vyhledávání zranitelností systémů ICT, detekování dostupných síťových služeb a portů, běžících procesů, běžících aplikací a jejich verzí apod.

   iv. Backdoor – skrytý softwarový nebo hardwarový nástroj, který umožňuje obejití schválených autentizačních procedur, instalovaný s cílem budoucího snadnějšího a neautorizovaného přístupu do systému ICT.

   v. Malware a jiný škodlivý software, který narušuje, obchází či jinak omezuje bezpečnostní opatření v prostředí Objednatele.

f. Připojovat do prostředí Objednatele pouze zařízení ICT, která jsou chráněna proti malware a jinému škodlivému softwaru, pokud to jejich technologie umožňuje.

g. Průběžně zaznamenávat a uchovávat data o provozu zařízení ICT (provozní a lokalizační údaje) v rozsahu předmětu plnění a v souladu s požadavky platné české a evropské legislativy.

h. Na vyžádání poskytnout Objednateli report obsahující výsledky monitorování veškerých uživatelských a administrátorských aktivit a jiných událostí v rozsahu předmětu plnění, a to po celou dobu trvání smlouvy a do 2 let po jejím ukončení.

i. Zajistit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění a ochranu získaných informací před jejich neoprávněným čtením nebo změnou.

j. Pro on-line transakce realizované prostřednictvím webových technologií implementovat TLS/SSL certifikáty s cílem zajistit jejich důvěrnost, integritu a identitu komunikujících protistran.

k. Veškeré neveřejné informace poskytnuté Objednatelem chránit vhodným šifrováním a proti neautorizovanému přístupu, a to zejména na mobilních zařízeních.

2. Dodavatel bere na vědomí, že v případě, kdy technické spojení Objednatele s Dodavatelem narušuje chod služeb Objednatele, může být toto spojení ihned ukončeno bez předchozího upozornění, pokud tato smlouva nestanoví jinak.

3. Dodavatel bere na vědomí, že veškeré aktivity Dodavatele a jeho plnění realizované v prostředí Objednatele jsou monitorovány a vyhodnocovány v rozsahu předměty plnění a v souladu s interními dokumenty Objednatele, se kterými byl Dodavatel seznámen.

Příloha č. 7

Dotazník Významného dodavatele dle vyhlášky 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidace dat

Splnění podmínek dle vyhlášky č. 82/2018 Sb.		
Hodnocení úrovně kybernetické bezpečnosti účastníka - O2 Czech Republic a.s.		
Postup vyplnění:		
	1. Účastník odpoví na všechny otázky v SEKCI A - E.	
	2. Účastník doloží splnění otázky označené hvězdičkou samostatným dokumentem nebo certifikátem	
	3. Účastník může vymazat hodnotu buňky klávesou DEL.	
	Každá otázka, resp. podotázka má stejnou bodovou hodnotu.	
		Zbývá vyplnit 0 otázek.
SEKCE A – STANDARDY A NEJLEPŠÍ PRAKTIKY		
1	**Které standardy a postupy nejlepší praxe organizace účastníka využívá v rámci poskytování služeb (tam, kde je to relevantní, na certifikované úrovni):**	[redacted]
a.	systém řízení kvality, například ISO 9001, CAF, TQM	
b.	systém řízení bezpečnosti informací, například ISO/IEC 27001 *	
c.	systém řízení ochrany osobních údajů dle ISO / IEC 27701	
d.	systém řízení kontinutiy podnikových procesů, například ISO 22301	
e.	systém řízení IT služeb, například ISO/IEC 20000-1, ITIL, CobIT	
2	**Audity provedené subjektem akreditovaným ČIA nebo obdobným subjektem v rámci EU pro poskytování certifikačních služeb**	
a.	Certifikační nebo dohledový audit, dle otázky Sekce A 1.a v posledních dvou letech	[redacted]
b.	Certifikační nebo dohledový audit dle otázky Sekce A 1.b v posledních dvou letech	
c.	Certifikační nebo dohledový audit dle otázky Sekce A 1.c v posledních dvou letech	
d.	Certifikační nebo dohledový audit dle otázky Sekce A 1.d v posledních dvou letech	
e.	Certifikační nebo dohledový audit dle otázky Sekce A 1.e v posledních dvou letech	
3	**Audit Významného dodavatele provedený správcem KII nebo VI**	

a.	Audit Významného dodavatele dle zákona 181/2014 Sb. Správcem KII	[redacted]
b.	Audit Významného dodavatele dle zákona 181/2014 Sb. Správcem VIS	
SEKCE B – ZÁKLADNÍ OPATŘENÍ		
1	Má organizace účastníka manažera kybernetické bezpečnosti nebo jinou určenou osobu s ekvivalentní odpovědností *	
2	Byl v organizaci v posledních 12ti měsících proveden třetí stranou audit či analýza, jejichž obsahem byla kontrola v oblasti kybernetické bezpečnosti	
3	Bylo v organizaci v posledních 12ti měsících provedeno hodnocení rizik v oblasti kybernetické bezpečnosti	
4	Je účastník vůči nějaké organizaci v postavení Významného dodavatele dle zákona 181/2014 Sb.*	
5	**Které oblasti pokrývá dokument bezpečnostní politiky, pokud v organizaci účastníka existuje?**	
a.	Procesy řízení rizik	[redacted]
b.	Klasifikace aktiv	
c.	Ochrana dat proti prozrazení, zničení, narušení integrity a dostupnosti *	
d.	Ochrana osobních dat *	
e.	Identifikace a autentizace uživatelů *	
f.	Přístup k datům na základě rolí (RBAC, Role Based Access Control)	
g.	Řízení privilegovaných přístupů *	
h.	Ochrana koncových stanic	
i.	Ochrana mobilních zařízení a vzdáleného přístupu	
j.	Ochrana emailu a vnitrofiremní komunikace (instant messaging)	
k.	Ochrana přístupu do internetu	
l.	Ochrana médií	
m.	Procesy řízení změn	
n.	Ochrana bezdrátových sítí a komunikace	
o.	Fyzická bezpečnost informačních aktiv	
p.	Bezpečnostní školení koncových uživatelů a administrátorů *	
q.	Ochrana proti škodlivému softwaru	
r.	Ochrana při výměně dat	
s.	Procesy zvládání kybernetických incidentů *	
t.	Procesy řízení rizik dodavatelů	
u.	Bezpečnost lidských zdrojů *	
v.	Bezpečnostní audity a analýzy	
w.	Řízení kontinuity činností a havarijní plánování	
SEKCE C – BEZPEČNOSTNÍ TECHNOLOGIE		
1	**Které níže uvedené bezpečnostní technologie organizace účastníka provozuje s cílem předcházet bezpečnostním hrozbám ve vztahu k datům a informačním systémům?**	

a.	Antivirový software na pracovních stanicích *	[redacted]
b.	Antivirový software na mobilních zařízeních	
c.	Nástroj pro detekci narušení sítě (IDS/IPS, Intrusion Detection/Prevention System)*	
d.	Nástroj pro řízení privilegovaných účtů a oprávnění (PIM/PAM, Priviledge Identity/Access Management)	
e.	Více-faktorová autentizace	
f.	Automatizovaný nástroj pro řízení technologických zranitelností	
g.	Nástroj pro řízení přístupu k síti (NAC, Network Access Control)	
h.	Nástroj pro ochranu před útoky DDoS (Distributed denial-of-service)	
i.	Šifrovací nástroje a techniky	
j.	Firewall kategorie Next Generation *	
k.	Nástroj pro vyhodnocování bezpečnostních událostí (SIEM, Security Informaton and Event Management)	
2	Byly interní systémy organizace účastníka v posledních 12ti měsících podrobeny penetračnímu testování?	
SEKCE D – PROCES ZVLÁDÁNÍ KYBERNETICKÝCH INCIDENTŮ		
1	Má organizace účastníka zaveden proces zvládání kybernetických incidentů? *	
2	Jsou všichni zaměstnanci organizace účastníka pravidelně (min. 1x ročně) vzdělávání v identifikaci kybernetických incidentů?	
SEKCE E – KOMUNIKACE BEZPEČNOSTI A VZDĚLÁVÁNÍ		
1	Má organizace účastníka zaveden proces vzdělávání a zvyšování bezpečnostního povědomí pro zaměstnance? *	
2	Jsou noví zaměstnanci organizace účastníka vyškoleni v oblasti kybernetické bezpečnosti dříve, než získají přístup k datům a informačním systémům? *	
3	Dokumentuje organizace účastníka účast pracovníků na bezpečnostních školeních a vzdělávacích programech?	
4	Vyžaduje organizace účastníka po zaměstnancích s přístupem k datům a informačním systémům podepsání individuální dohody o mlčenlivosti?	
5	Vyžaduje organizace účastníka po zaměstnancích podepsání etického kodexu?	
		Zbývá vyplnit 0 otázek.

Počet nevyplněných otázek: [redacted]

SEKCE A – STANDARDY A NEJLEPŠÍ PRAKTIKY
SEKCE B – ZÁKLADNÍ OPATŘENÍ
SEKCE C – BEZPEČNOSTNÍ TECHNOLOGIE
SEKCE D – PROCES ZVLÁDÁNÍ KYBERNETICKÝCH INCIDENTŮ
SEKCE E – KOMUNIKACE BEZPEČNOSTI A VZDĚLÁVÁNÍ

[redacted]

SEKCE A – STANDARDY A NEJLEPŠÍ PRAKTIKY

1 **Které standardy a postupy nejlepší praxe organizace účastníka využívá v rámci poskytování služeb (tam, kde je to relevantní, na certifikované úrovni):**

a. systém řízení kvality, například ISO 9001, CAF, TQM
b. systém řízení bezpečnosti informací, například ISO/IEC 27001 *
c. systém řízení ochrany osobních údajů dle ISO / IEC 27701
d. systém řízení kontinutiy podnikových procesů, například ISO 22301
e. systém řízení IT služeb, například ISO/IEC 20000-1, ITIL, CobIT

[redacted]

2 **Audity provedené subjektem akreditovaným ČIA nebo obdobným subjektem v rámci EU pro poskytování certifikačních služeb**

a. Certifikační nebo dohledový audit, dle otázky Sekce A 1.a v posledních dvou letech
b. Certifikační nebo dohledový audit dle otázky Sekce A 1.b v posledních dvou letech
c. Certifikační nebo dohledový audit dle otázky Sekce A 1.c v posledních dvou letech
d. Certifikační nebo dohledový audit dle otázky Sekce A 1.d v posledních dvou letech
e. Certifikační nebo dohledový audit dle otázky Sekce A 1.e v posledních dvou letech

3 **Audit Významného dodavatele provedený správcem KII nebo VIS**

a. Audit Významného dodavatele dle zákona 181/2014 Sb. Správcem KII
b. Audit Významného dodavatele dle zákona 181/2014 Sb. Správcem VIS

SEKCE B – ZÁKLADNÍ OPATŘENÍ

1 Má organizace účastníka manažera kybernetické bezpečnosti nebo jinou určenou osobu s ekvivalentní odpovědností *
2 Byl v organizaci v posledních 12ti měsících proveden třetí stranou audit či analýza, jejichž obsahem byla kontrola v oblasti kybernetické bezpečnosti
3 Bylo v organizaci v posledních 12ti měsících provedeno hodnocení rizik v oblasti kybernetické bezpečnosti
4 Je účastník vůči nějaké organizaci v postavení Významného dodavatele dle zákona 181/2014 Sb.*

[redacted]

5 **Které oblasti pokrývá dokument bezpečnostní politiky, pokud v organizaci účastníka existuje?**

a. Procesy řízení rizik

[redacted]

b. Klasifikace aktiv
c. Ochrana dat proti prozrazení, zničení, narušení integrity a dostupnosti *
d. Ochrana osobních dat *
e. Identifikace a autentizace uživatelů *
f. Přístup k datům na základě rolí (RBAC, Role Based Access Control)
g. Řízení privilegovaných přístupů *
h. Ochrana koncových stanic
i. Ochrana mobilních zařízení a vzdáleného přístupu
j. Ochrana emailu a vnitrofiremní komunikace (instant messaging)
k. Ochrana přístupu do internetu
l. Ochrana médií
m. Procesy řízení změn
n. Ochrana bezdrátových sítí a komunikace
o. Fyzická bezpečnost informačních aktiv
p. Bezpečnostní školení koncových uživatelů a administrátorů *
q. Ochrana proti škodlivému softwaru
r. Ochrana při výměně dat
s. Procesy zvládání kybernetických incidentů *
t. Procesy řízení rizik dodavatelů
u. Bezpečnost lidských zdrojů *
v. Bezpečnostní audity a analýzy
w. Řízení kontinuity činností a havarijní plánování

SEKCE C – BEZPEČNOSTNÍ TECHNOLOGIE

1 **Které níže uvedené bezpečnostní technologie organizace účastníka provozuje s cílem předcházet bezpečnostním hrozbám ve vztahu k datům a informačním systémům?**

a. Antivirový software na pracovních stanicích *
b. Antivirový software na mobilních zařízeních
c. Nástroj pro detekci narušení sítě (IDS/IPS, Intrusion Detection/Prevention System)*
d. Nástroj pro řízení privilegovaných účtů a oprávnění (PIM/PAM, Priviledge Identity/Access Management)
e. Více-faktorová autentizace
f. Automatizovaný nástroj pro řízení technologických zranitelností
g. Nástroj pro řízení přístupu k síti (NAC, Network Access Control)
h. Nástroj pro ochranu před útoky DDoS (Distributed denial-of-service)
i. Šifrovací nástroje a techniky
j. Firewall kategorie Next Generation *
k. Nástroj pro vyhodnocování bezpečnostních událostí (SIEM, Security Informaton and Event Management)

2 Byly interní systémy organizace účastníka v posledních 12ti měsících podrobeny penetračnímu testování?

SEKCE D – PROCES ZVLÁDÁNÍ KYBERNETICKÝCH INCIDENTŮ

1 Má organizace účastníka zaveden proces zvládání kybernetických incidentů? *

2 Jsou všichni zaměstnanci organizace účastníka pravidelně (min. 1x ročně) vzdělávání v identifikaci kybernetických incidentů?

SEKCE E – KOMUNIKACE BEZPEČNOSTI A VZDĚLÁVÁNÍ

1 Má organizace účastníka zaveden proces vzdělávání a zvyšování bezpečnostního povědomí pro zaměstnance? *

2 Jsou noví zaměstnanci organizace účastníka vyškoleni v oblasti kybernetické bezpečnosti dříve, než získají přístup k datům a informačním systémům? *

3 Dokumentuje organizace účastníka účast pracovníků na bezpečnostních školeních a vzdělávacích programech?

4 Vyžaduje organizace účastníka po zaměstnancích s přístupem k datům a informačním systémům podepsání individuální dohody o mlčenlivosti?

5 Vyžaduje organizace účastníka po zaměstnancích podepsání etického kodexu?

Splnění podmínek dle vyhlášky č. 82/2018 Sb.		
Hodnocení úrovně kybernetické bezpečnosti poddodavatele účastníka - CETIN a.s.		
Postup vyplnění:		
	1. Účastník odpoví na všechny otázky v SEKCI A - E.	
	2. Účastník doloží splnění otázky označené hvězdičkou samostatným dokumentem nebo certifikátem	
	3. Účastník může vymazat hodnotu buňky klávesou DEL.	
	Každá otázka, resp. podotázka má stejnou bodovou hodnotu.	
		Zbývá vyplnit 0 otázek.
SEKCE A – STANDARDY A NEJLEPŠÍ PRAKTIKY		
1	**Které standardy a postupy nejlepší praxe organizace účastníka využívá v rámci poskytování služeb (tam, kde je to relevantní, na certifikované úrovni):**	[redacted]
a.	systém řízení kvality, například ISO 9001, CAF, TQM	
b.	systém řízení bezpečnosti informací, například ISO/IEC 27001 *	
c.	systém řízení ochrany osobních údajů dle ISO / IEC 27701	
d.	systém řízení kontinutiy podnikových procesů, například ISO 22301	
e.	systém řízení IT služeb, například ISO/IEC 20000-1, ITIL, CobIT	
2	**Audity provedené subjektem akreditovaným ČIA nebo obdobným subjektem v rámci EU pro poskytování certifikačních služeb**	
a.	Certifikační nebo dohledový audit, dle otázky Sekce A 1.a v posledních dvou letech	[redacted]
b.	Certifikační nebo dohledový audit dle otázky Sekce A 1.b v posledních dvou letech	
c.	Certifikační nebo dohledový audit dle otázky Sekce A 1.c v posledních dvou letech	
d.	Certifikační nebo dohledový audit dle otázky Sekce A 1.d v posledních dvou letech	
e.	Certifikační nebo dohledový audit dle otázky Sekce A 1.e v posledních dvou letech	
3	**Audit Významného dodavatele provedený správcem KII nebo VIS**	
a.	Audit Významného dodavatele dle zákona 181/2014 Sb. Správcem KII	[redacted]
b.	Audit Významného dodavatele dle zákona 181/2014 Sb. Správcem VIS	
SEKCE B – ZÁKLADNÍ OPATŘENÍ		
1	Má organizace účastníka manažera kybernetické bezpečnosti nebo jinou určenou osobu s ekvivalentní odpovědností *	[redacted]

2	Byl v organizaci v posledních 12ti měsících proveden třetí stranou audit či analýza, jejichž obsahem byla kontrola v oblasti kybernetické bezpečnosti	[redacted]
3	Bylo v organizaci v posledních 12ti měsících provedeno hodnocení rizik v oblasti kybernetické bezpečnosti	
4	Je účastník vůči nějaké organizaci v postavení Významného dodavatele dle zákona 181/2014 Sb.*	
5	**Které oblasti pokrývá dokument bezpečnostní politiky, pokud v organizaci účastníka existuje?**	
a.	Procesy řízení rizik	[redacted]
b.	Klasifikace aktiv	
c.	Ochrana dat proti prozrazení, zničení, narušení integrity a dostupnosti *	
d.	Ochrana osobních dat *	
e.	Identifikace a autentizace uživatelů *	
f.	Přístup k datům na základě rolí (RBAC, Role Based Access Control)	
g.	Řízení privilegovaných přístupů *	
h.	Ochrana koncových stanic	
i.	Ochrana mobilních zařízení a vzdáleného přístupu	
j.	Ochrana emailu a vnitrofiremní komunikace (instant messaging)	
k.	Ochrana přístupu do internetu	
l.	Ochrana médií	
m.	Procesy řízení změn	
n.	Ochrana bezdrátových sítí a komunikace	
o.	Fyzická bezpečnost informačních aktiv	
p.	Bezpečnostní školení koncových uživatelů a administrátorů *	
q.	Ochrana proti škodlivému softwaru	
r.	Ochrana při výměně dat	
s.	Procesy zvládání kybernetických incidentů *	
t.	Procesy řízení rizik dodavatelů	
u.	Bezpečnost lidských zdrojů *	
v.	Bezpečnostní audity a analýzy	
w.	Řízení kontinuity činností a havarijní plánování	
SEKCE C – BEZPEČNOSTNÍ TECHNOLOGIE		
1	**Které níže uvedené bezpečnostní technologie organizace účastníka provozuje s cílem předcházet bezpečnostním hrozbám ve vztahu k datům a informačním systémům?**	
a.	Antivirový software na pracovních stanicích *	[redacted]
b.	Antivirový software na mobilních zařízeních	
c.	Nástroj pro detekci narušení sítě (IDS/IPS, Intrusion Detection/Prevention System)*	
d.	Nástroj pro řízení privilegovaných účtů a oprávnění (PIM/PAM, Priviledge Identity/Access Management)	
e.	Více-faktorová autentizace	

f.	Automatizovaný nástroj pro řízení technologických zranitelností	
g.	Nástroj pro řízení přístupu k síti (NAC, Network Access Control)	
h.	Nástroj pro ochranu před útoky DDoS (Distributed denial-of-service)	
i.	Šifrovací nástroje a techniky	
j.	Firewall kategorie Next Generation *	
k.	Nástroj pro vyhodnocování bezpečnostních událostí (SIEM, Security Informaton and Event Management)	
2	Byly interní systémy organizace účastníka v posledních 12ti měsících podrobeny penetračnímu testování?	
SEKCE D – PROCES ZVLÁDÁNÍ KYBERNETICKÝCH INCIDENTŮ		
1	Má organizace účastníka zaveden proces zvládání kybernetických incidentů? *	
2	Jsou všichni zaměstnanci organizace účastníka pravidelně (min. 1x ročně) vzdělávání v identifikaci kybernetických incidentů?	
SEKCE E – KOMUNIKACE BEZPEČNOSTI A VZDĚLÁVÁNÍ		
1	Má organizace účastníka zaveden proces vzdělávání a zvyšování bezpečnostního povědomí pro zaměstnance? *	
2	Jsou noví zaměstnanci organizace účastníka vyškoleni v oblasti kybernetické bezpečnosti dříve, než získají přístup k datům a informačním systémům? *	
3	Dokumentuje organizace účastníka účast pracovníků na bezpečnostních školeních a vzdělávacích programech?	
4	Vyžaduje organizace účastníka po zaměstnancích s přístupem k datům a informačním systémům podepsání individuální dohody o mlčenlivosti?	
5	Vyžaduje organizace účastníka po zaměstnancích podepsání etického kodexu?	
		Zbývá vyplnit 0 otázek.

Počet nevyplněných otázek: [redacted]

SEKCE A – STANDARDY A NEJLEPŠÍ PRAKTIKY
SEKCE B – ZÁKLADNÍ OPATŘENÍ
SEKCE C – BEZPEČNOSTNÍ TECHNOLOGIE
SEKCE D – PROCES ZVLÁDÁNÍ KYBERNETICKÝCH INCIDENTŮ
SEKCE E – KOMUNIKACE BEZPEČNOSTI A VZDĚLÁVÁNÍ

[redacted]

SEKCE A – STANDARDY A NEJLEPŠÍ PRAKTIKY

1 **Které standardy a postupy nejlepší praxe organizace účastníka využívá v rámci poskytování služeb (tam, kde je to relevantní, na certifikované úrovni):**

a. systém řízení kvality, například ISO 9001, CAF, TQM
b. systém řízení bezpečnosti informací, například ISO/IEC 27001 *
c. systém řízení ochrany osobních údajů dle ISO / IEC 27701
d. systém řízení kontinutiy podnikových procesů, například ISO 22301
e. systém řízení IT služeb, například ISO/IEC 20000-1, ITIL, CobIT

[redacted]

2 **Audity provedené subjektem akreditovaným ČIA nebo obdobným subjektem v rámci EU pro poskytování certifikačních služeb**

a. Certifikační nebo dohledový audit, dle otázky Sekce A 1.a v posledních dvou letech
b. Certifikační nebo dohledový audit dle otázky Sekce A 1.b v posledních dvou letech
c. Certifikační nebo dohledový audit dle otázky Sekce A 1.c v posledních dvou letech
d. Certifikační nebo dohledový audit dle otázky Sekce A 1.d v posledních dvou letech
e. Certifikační nebo dohledový audit dle otázky Sekce A 1.e v posledních dvou letech

3 **Audit Významného dodavatele provedený správcem KII nebo VIS**

a. Audit Významného dodavatele dle zákona 181/2014 Sb. Správcem KII
b. Audit Významného dodavatele dle zákona 181/2014 Sb. Správcem VIS

[redacted]

SEKCE B – ZÁKLADNÍ OPATŘENÍ

1 Má organizace účastníka manažera kybernetické bezpečnosti nebo jinou určenou osobu s ekvivalentní odpovědností *
2 Byl v organizaci v posledních 12ti měsících proveden třetí stranou audit či analýza, jejichž obsahem byla kontrola v oblasti kybernetické bezpečnosti
3 Bylo v organizaci v posledních 12ti měsících provedeno hodnocení rizik v oblasti kybernetické bezpečnosti
4 Je účastník vůči nějaké organizaci v postavení Významného dodavatele dle zákona 181/2014 Sb.*
5 **Které oblasti pokrývá dokument bezpečnostní politiky, pokud v organizaci účastníka existuje?**

a. Procesy řízení rizik

[redacted]

b. Klasifikace aktiv
c. Ochrana dat proti prozrazení, zničení, narušení integrity a dostupnosti *
d. Ochrana osobních dat *
e. Identifikace a autentizace uživatelů *
f. Přístup k datům na základě rolí (RBAC, Role Based Access Control)
g. Řízení privilegovaných přístupů *
h. Ochrana koncových stanic
i. Ochrana mobilních zařízení a vzdáleného přístupu
j. Ochrana emailu a vnitrofiremní komunikace (instant messaging)
k. Ochrana přístupu do internetu
l. Ochrana médií
m. Procesy řízení změn
n. Ochrana bezdrátových sítí a komunikace
o. Fyzická bezpečnost informačních aktiv
p. Bezpečnostní školení koncových uživatelů a administrátorů *
q. Ochrana proti škodlivému softwaru
r. Ochrana při výměně dat
s. Procesy zvládání kybernetických incidentů *
t. Procesy řízení rizik dodavatelů
u. Bezpečnost lidských zdrojů *
v. Bezpečnostní audity a analýzy
w. Řízení kontinuity činností a havarijní plánování

[redacted]

SEKCE C – BEZPEČNOSTNÍ TECHNOLOGIE

1 **Které níže uvedené bezpečnostní technologie organizace účastníka provozuje s cílem předcházet bezpečnostním hrozbám ve vztahu k datům a informačním**

a. Antivirový software na pracovních stanicích *
b. Antivirový software na mobilních zařízeních
c. Nástroj pro detekci narušení sítě (IDS/IPS, Intrusion Detection/Prevention System)*
d. Nástroj pro řízení privilegovaných účtů a oprávnění (PIM/PAM, Priviledge Identity/Access Management)
e. Více-faktorová autentizace
f. Automatizovaný nástroj pro řízení technologických zranitelností
g. Nástroj pro řízení přístupu k síti (NAC, Network Access Control)
h. Nástroj pro ochranu před útoky DDoS (Distributed denial-of-service)
i. Šifrovací nástroje a techniky
j. Firewall kategorie Next Generation *
k. Nástroj pro vyhodnocování bezpečnostních událostí (SIEM, Security Informaton and Event Management)

2 Byly interní systémy organizace účastníka v posledních 12ti měsících podrobeny penetračnímu testování?

[redacted]

SEKCE D – PROCES ZVLÁDÁNÍ KYBERNETICKÝCH INCIDENTŮ

1 Má organizace účastníka zaveden proces zvládání kybernetických incidentů? *

2 Jsou všichni zaměstnanci organizace účastníka pravidelně (min. 1x ročně) vzdělávání v identifikaci kybernetických incidentů?

SEKCE E – KOMUNIKACE BEZPEČNOSTI A VZDĚLÁVÁNÍ

1 Má organizace účastníka zaveden proces vzdělávání a zvyšování bezpečnostního povědomí pro zaměstnance? *

2 Jsou noví zaměstnanci organizace účastníka vyškoleni v oblasti kybernetické bezpečnosti dříve, než získají přístup k datům a informačním systémům? *

3 Dokumentuje organizace účastníka účast pracovníků na bezpečnostních školeních a vzdělávacích programech?

4 Vyžaduje organizace účastníka po zaměstnancích s přístupem k datům a informačním systémům podepsání individuální dohody o mlčenlivosti?

5 Vyžaduje organizace účastníka po zaměstnancích podepsání etického kodexu?

Příloha č. 8

Čestné prohlášení o neexistenci střetu zájmů

ČESTNÉ PROHLÁŠENÍ O NEEXISTENCI STŘETU ZÁJMU

Účastník *(Název, IČO a sídlo, zapsaný v obchodním rejstříku vedeném):*	O2 Czech Republic a.s., IČO 60193336 Praha 4 - Michle, Za Brumlovkou 266/2, PSČ 14022 Spisová značka: B 2322 vedená u Městského soudu v Praze
Název výběrového řízení:	**Datové centrum**
Zadavatel:	Ústav zdravotnických informací a statistiky České republiky
Sídlo zadavatele:	Palackého náměstí 4, 128 01 Praha 2
IČO:	00023833

tímto předkládá čestné prohlášení o neexistenci střetu zájmů v souladu s § 4b zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů a prohlašuje, že:

- není obchodní společností, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. c) zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů (člen vlády nebo vedoucí jiného ústředního správního úřadu, v jehož čele není člen vlády), nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti;

- poddodavatel, prostřednictvím kterého prokazuji kvalifikaci (existuje-li takový), není obchodní společností, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. c) zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů (člen vlády nebo vedoucí jiného ústředního správního úřadu, v jehož čele není člen vlády), nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti

V Praze, dne dle data el. podpisu

Příloha č. 9

Čestné prohlášení účastníka o splnění nařízení Rady EU 2022/576

ČESTNÉ PROHLÁŠENÍ ÚČASTNÍKA O SPLNĚNÍ NAŘÍZENÍ RADY EU 2022/576

Účastník *(Název, IČO a sídlo, zapsaný v obchodním rejstříku vedeném):*	O2 Czech Republic a.s., IČO 60193336 Praha 4 - Michle, Za Brumlovkou 266/2, PSČ 14022 Spisová značka: B 2322 vedená u Městského soudu v Praze
Název výběrového řízení:	**Datové centrum**
Zadavatel:	Ústav zdravotnických informací a statistiky České republiky
Sídlo zadavatele:	Palackého náměstí 4, 128 01 Praha 2
IČO:	00023833

tímto pro účely veřejné zakázky s názvem **„Datové centrum“** čestně prohlašuje, že splňuje podmínky stanovené nařízením Rady EU 2022/576 ze dne 8. dubna 2022 (dále také jen „**Nařízení**“), tedy že není:

a) ruským státním příslušníkem, fyzickou či právnickou osobou nebo subjektem či orgánem se sídlem v Rusku,
b) právnickou osobou, subjektem nebo orgánem, který je z více než 50 % přímo či nepřímo vlastněn některým ze subjektů uvedených v písmeni a) nebo
c) fyzickou nebo právnickou osobou, subjektem nebo orgánem, jednající jménem nebo na pokyn některého ze subjektů uvedených v písmeni a) nebo b), včetně poddodavatelů, dodavatelů nebo subjektů, jejichž způsobilost je využívána ve smyslu směrnic o zadávání veřejných zakázek, pokud představují více než 10 % hodnoty zakázky, nebo společně s nimi.

Toto čestné prohlášení činí účastník na základě své vážné a svobodné vůle a je si vědom všech následků plynoucích z uvedení nepravdivých údajů.

[redacted]

V Praze, dne dle data el. Podpisu