PŘÍLOHA BEZPEČNOST INFORMACÍ

Tato příloha obsahuje CKTCH používané standardní ujednání o bezpečnosti informací. Vzhledem k předmětu smlouvy, který úzce souvisí s bezpečností informací, resp. kybernetickou bezpečností, ujednání této přílohy se použijí pouze v rozsahu, v jakém jsou relevantní vzhledem k předmětu smlouvy.

1 DEFINICE

Dále uvedené pojmy a zkratky mají v Příloze následující jednotný význam:

(a) „**KBU**“ je kybernetická bezpečnostní událost, tedy událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb a sítí elektronických komunikací.

(b) „**KBI**“ je kybernetický bezpečnostní incident, tedy narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb a sítí elektronických komunikací.

(c) „**Příloha**“ je tento dokument nadepsaný „Bezpečnost informací“.

(d) „**Smlouva**“ je smlouva, ke které je přiložena Příloha.

(e) „**VKB**“ je vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů.

(f) „**ZKB**“ je zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.

2 ÚČEL

2.1 V Příloze jsou stanoveny způsoby a úrovně realizace bezpečnostních opatření pro Dodavatele a určen vzájemný vztah odpovědnosti za zavedení a kontrolu bezpečnostních opatření mezi CKTCH a Dodavatelem v souladu se ZKB a VKB.

2.2 Veškeré činnosti podle Přílohy jsou kontrolovány v rámci pravidelného auditu, pokud není stanoveno jinak.

3 ZÁKLADNÍ POVINNOSTI V OBLASTI BEZPEČNOSTI INFORMACÍ

3.1 Dodavatel musí dodržovat požadavky řízení bezpečnosti informací uvedené ve Smlouvě a Příloze a současně příslušná ustanovení interních dokumentů CKTCH, zejména bezpečnostních politik, metodik a postupů, resp. platné řídící dokumentace CKTCH vycházející ze ZKB a VKB a běžných bezpečnostních standardů. V případě, že z interních dokumentů CKTCH vzejde Dodavateli

povinnost, která není výslovně stanovena ve Smlouvě, Příloze, právních předpisech nebo z nich jednoznačně odvoditelná, bude taková situace řešena prostřednictvím odpovídajících ustanovení o změnách obsažených ve Smlouvě, nebo, pokud taková ustanovení Smlouva neobsahuje, na základě dohody Stran.

3.2 Dodavatel musí provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění bezpečnosti informací (zajištění důvěrnosti, integrity a dostupnosti) v rámci aktiv souvisejících s plněním Smlouvy a vést o způsobu zabezpečení bezpečnostní dokumentaci.

3.3 Pokud je pro plnění Smlouvy nezbytný přenos dat z prostředí Dodavatele do prostředí CKTCH nebo naopak, musí Strany dostatečně zabezpečit takový přenos a vést dokumentaci o typech přenášených dat. Takový přenos se může uskutečnit pouze na výzvu nebo se souhlasem CKTCH v rozsahu a způsobem, který bude zvolen po vzájemné dohodě Stran.

3.4 Dodavatel dále musí:

(a) rozvíjet bezpečnostní povědomí svých zaměstnanců a jiných osob, které se podílejí na plnění Smlouvy, a průběžně je seznamovat s prováděnými nebo plánovanými změnami;

(b) přidělovat osobám, které se podílejí na plnění Smlouvy, oprávnění k výkonu činností a přísně při tom dodržovat bezpečnostní zásadu tzv. „potřeba vědět“ (*need-to-know principle*), tedy dbát o to, aby byla minimalizována rizika nežádoucího přístupu k těm aktivům CKTCH, která nesouvisí s plněním Smlouvy; jedná se například o přístupy cestou software systémů umožňujících vzdálený přístup;

(c) průběžně dokumentovat, kontrolovat a vyhodnocovat oprávněnost přístupu u všech osob na straně Dodavatele, které přistupují k aktivům souvisejících s plněním Smlouvy;

(d) průběžně detekovat obecné bezpečnostní hrozby a zranitelnosti v aktivech souvisejících s plněním Smlouvy

(e) bezodkladně informovat CKTCH o detekované bezpečnostní zranitelnosti, hrozbě nebo KBU a ve spolupráci s CKTCH zajistit odstranění nebo snížení rizika hrozby, zranitelnosti nebo KBU tak, aby bylo zabráněno vzniku KBI.

3.5 V případě, kdy CKTCH identifikuje KBU, která by mohla ohrozit Dodavatele, oznámí tuto skutečnost Dodavateli a společné naleznou řešení, aby nedošlo k KBI.

4 OPRÁVNĚNÍ UŽÍVAT DATA, PRAVIDLA PŘÍSTUPU

4.1 Dodavatel může při plnění Smlouvy užívat data předaná CKTCH za účelem plnění Smlouvy, avšak vždy pouze v rozsahu nezbytném k plnění Smlouvy. Veškerá předávaná data jsou klasifikována jako informace se střední důvěrností (viz odst. 15.3 písm. (b)), pokud CKTCH neurčí jinak.

4.2 Dodavatel nesmí instalovat ani používat žádné nástroje, které nebyly odsouhlaseny CKTCH a jejichž užívání by mohlo ohrozit kybernetickou bezpečnost.

4.3 Dodavatel musí při plnění Smlouvy nakládat s daty (včetně osobních údajů) pouze v souladu se Smlouvou, Přílohou a právními předpisy.

4.4 Dodavatel odpovídá za aktuálnost seznamu pracovníků oprávněných přistupovat do objektů CKTCH a aktiv CKTCH souvisejících s plněním Smlouvy.

4.5 Dodavatel bere na vědomí, že přidělení oprávnění zaměstnanci Dodavatele nebo osobě v jiném obdobném postavení ze strany CKTCH musí být řízeno principem nezbytného minima a není nárokové.

4.6 Dodavatel musí zajistit, aby žádný udělený přístup nebyl sdílen více zaměstnanci Dodavatele nebo jinými osobami a že pro přihlášení uživatele nebudou využívány účty typu *root* nebo *administrator*.

4.7 Dodavatel musí zajistit, že vzdálený přístup do aktiv souvisejících s předmětem plnění Smlouvy bude vždy uskutečněn pouze prostřednictvím zabezpečeného připojení VPN a na vyžádání ze strany CKTCH a na dobu nezbytně nutnou, pokud se Strany nedohodnou jinak.

4.8 Dodavatel nesmí vyvíjet, kompilovat nebo šířit v jakékoliv části aktiv CKTCH programový kód, který má za cíl nelegální ovládnutí, narušení aktiva nebo nelegální získání dat a informací. Dodavatel musí do interní sítě nebo k technologickým a komunikačním systémům CKTCH výhradně s využitím zařízení CKTCH, pokud se Strany nedohodnou jinak.

4.9 Dodavatel musí zajistit, aby osoby podílející se na plnění Smlouvy, kteří přistupují do interní sítě nebo technologického nebo komunikačního systému CKTCH:

(a) měly v externím zařízení (např. notebook, počítač) aplikovány bezpečnostní záplaty a aktualizovanou antivirovou ochranu;

(b) chránily autentizační prostředky a údaje k systémům CKTCH; Dodavatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako KBI;

(c) používaly v případě u administrátorských a servisních účtů hesla o délce minimálně 17 znaků obsahující velké písmeno, malé písmeno, číslici a speciální znak.

4.10 Postup v případě nutnosti využít TeamViewer (TV):

(a) Připojení přes TV je povoleno pouze na základě požadavku Dodavatele odsouhlaseného ze strany CKTCH v helpdeskovém systému Dodavatele, pokud nebude možno, tak telefonicky, což bude zaznamenáno ve výsledném reportu Dodavatele.

(b) Po odsouhlasení připojení je spuštěno nahrávání obrazovky na straně CKTCH. Dobu uložení videa určí garant aktiva. V případě řešení KBI má Dodavatel právo do záznamu na vyžádání nahlédnout, a to na základě písemného požadavku směřovaného na kontaktní osoby.

(c) Dodavatel musí po skočení činností vypracovat podrobný popis toho, co bylo provedeno, do svého helpdesk systému.

5 MONITOROVACÍ ČINNOST

5.1 Dodavatel bere na vědomí, že veškerá aktivita Dodavatele v rámci plnění Smlouvy nebo s ním úzce související bude ze strany CKTCH průběžně a pravidelně monitorována a vyhodnocována s ohledem na obsah Smlouvy, Přílohy a interních dokumentů CKTCH.

Dodavatel musí průběžně monitorovat a zaznamenávat veškerou svoji aktivitu v rámci plnění Smlouvy nebo s ním úzce související. Dodavatel musí na vyžádání předkládat CKTCH záznamy/logy obsahující výsledky monitorování, úspěšná a neúspěšná přihlášení do systému CKTCH (pokud nebude logováno v prostředí CKTCH) a záznamy o správě uživatelů prováděná na straně Dodavatele.

6 AUTORSTVÍ

6.1 Dodavatel musí při plnění Smlouvy postupovat v souladu s právními předpisy upravujícími ochranu duševního vlastnictví, zejména se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

7 KONTROLA A AUDIT

7.1 Dodavatel musí poskytnout CKTCH veškeré informace potřebné k doložení toho, že byly splněny povinnosti vyplývající ze Smlouvy, Přílohy, ZKB a VKB.

7.2 Dodavatel musí umožnit CKTCH provedení kontrol, včetně auditů v rozsahu minimálních požadavků podle ZKB a VKB, prováděných CKTCH či CKTCH určeným auditorem a poskytnout k těmto kontrolám nebo auditům veškerou potřebnou součinnost, včetně umožnění vstup do prostor Dodavatele nebo jeho poddodavatele, pokud je to relevantní z hlediska předmětu Smlouvy.

7.3 Kontrola a audit budou probíhat minimálně jednou ročně, zpravidla formou vyplnění kontrolního dotazníku, pokud se Strany nedohodnou jinak.

7.4 CKTCH musí písemně oznámit Dodavateli provedení kontroly nebo auditu, a to nejméně 30 předem. Součástí oznámení musí být i seznam osob, které byly CKTCH pověřeny k provedení kontroly nebo auditu.

7.5 Dodavatel souhlasí s prováděním hodnocení rizik, kontrolou nebo auditem zavedených bezpečnostních opatření Dodavatele ze strany CKTCH. CKTCH musí na žádost Dodavatele poskytnout výsledek proběhlé kontroly nebo auditu. Aktualizace procesu řízení rizik probíhá v pravidelném intervalu 1krát ročně, nebo v návaznosti na zjištění závažných rizik. Dodavatel musí na žádost CKTCH provést revizi a případné doplnění výsledku řízení rizik.

8 ŘETĚZENÍ A ŘÍZENÍ DODAVATELŮ

8.1 Pokud Dodavatel využívá při plnění Smlouvy poddodavatele, musí zajistit, aby:

(a) poddodavatel dodržoval bezpečnostní požadavky a požadavků na ochranu osobních údajů vyplývající ze Smlouvy a Přílohy;

(b) poskytl CKTCH veškerá nezbytnou součinnost v otázkách řízení bezpečnosti informací.

8.2 Dodavatel se musí řídit požadavky CKTCH na řízení bezpečnosti informací a poskytnout CKTCH veškerou nezbytnou součinnost v otázkách řízení bezpečnosti informací. Dodavatel odpovídá za to, že jeho subdodavatelé nebudou jednat v rozporu s bezpečnostními požadavky vyplývajícími

ze Smlouvy nebo Přílohy. Pokud poddodavatel takové požadavky nedodrží, považuje se takové nedodržení požadavků za porušení povinnosti Dodavatele.

9 DODRŽOVÁNÍ BEZPEČNOSTNÍ POLITIKY CKTCH

9.1 Dodavatel musí dodržovat bezpečnostní politiku CKTCH (viz odst. 3.1).

9.2 Bezpečnostní politiky CKTCH jsou měněny zpravidla pouze v případě změn právních předpisů.

10 ŘÍZENÍ ZMĚN

10.1 Dodavatel musí poskytnout CKTCH veškerou nezbytnou součinnost ke splnění povinností CKTCH vyplývajících z ustanovení § 11 VKB, zejména při analýze souvisejících rizik (postup přiměřeně podle Přílohy č. 2 a č. 3 VKB), přijímání opatření za účelem snížení všech nepříznivých dopadů spojených se změnami, aktualizaci bezpečnostní dokumentace souvisejícím testování a zajištění možnosti navrácení do původního stavu aktiva souvisejícího s plněním Smlouvy.

10.2 CKTCH musí informovat Dodavatele o výsledcích řízení změn, které mají dopady na plnění Smlouvy ze strany Dodavatele. Jde zejména o změny v bezpečnostní dokumentaci CKTCH (včetně aktiv souvisejících s plněním Smlouvy) a z toho se odvíjející změny v povinnostech Dodavatele. V případě nutnosti se Strany dohodnou na změně povinností Dodavatele postupem podle Smlouvy.

10.3 Veškeré změny, které mají vliv na funkčnost primárních aktiv, podpůrných aktiv, a které mají vliv na bezpečnost informací, musí být řízeny, kontrolovány a dokumentovány ze strany CKTCH. Dodavatel v této věci poskytuje součinnost. Jedná se především o následující změny:

(a) změny ovlivňující více uživatelů např. změna vzhledu systému, změna většího počtu funkcí systému, změna vyžadující dlouhodobou odstávku systém; do této kategorie nepatří pravidelné aktualizace systému;

(b) změny prováděné na základě změn platné právní úpravy;

(c) změny dle rozsahu poskytované služby;

(d) změny jednotlivých podpůrných aktiv.

10.4 Dodavatel musí v případě změn podpůrných aktiv poskytnout součinnost CKTCH v rámci přezkoumání dopadů požadovaných změn. Přezkoumání je provedeno před zahájením procesu změn a bere ohledy na následující aspekty:

(a) dopadu na funkčnost aktiv, kterých se změna týká;

(b) časová náročnost provedení změny;

(c) finanční náročnosti změny;

(d) požadavku na personální zdroje pro realizaci změny a pro provozování změněného aktiva, kterého se změna dotýká;

(e) dopadu změny na kvalitu poskytovaných služeb (SLA);

(f) dopadu na existující procesy, pracovní postupy a dokumentaci aktiva, kterého se změna dotýká;

(g) přidělení rolí a odpovědností při a po realizaci změny;

(h) identifikace a řízení rizik spojených se změnou;

(i) proces obnovy do původního stavu.

11 SOULAD S PRÁVNÍMI PŘEDPISY

11.1 Dodavatel musí při plnění Smlouvy postupovat v souladu s právními předpisy.

11.2 Dodavatel bere na vědomí, že v případě významné změny kontroly nad Dodavatelem nebo změny kontroly nad zásadními aktivy využívanými Dodavatelem, může CKTCH od Smlouvy odstoupit.

12 INFORMAČNÍ POVINNOST

12.1 Dodavatel musí informovat (například formou dotazníku v rámci auditu) CKTCH o tom, jakým způsobem řídí bezpečnostní rizika Dodavatele spojená s plněním Smlouvy a dále jaká jsou zbytková rizika s tím související (postup přiměřeně podle Přílohy č. 2 a č. 3 VKB).

12.2 Dodavatel musí CKTCH neprodleně, nejpozději do druhého pracovního dne, v případě závažného KBI ihned, informovat o všech nově KBU nebo KBI souvisejících s plněním Smlouvy, a to prostřednictvím kontaktních osob uvedených v odst. 12.3. Součástí oznámení musí být popis povahy KBU nebo KBI s ohledem na následující klasifikaci:

(a) **slabé místo nebo KBU** – nedošlo ke KBI, ale KBU související se systémem, procesem nebo organizací může dříve či později vést ke KBI;

(b) **méně závažný KBI** – KBI, který nemůže významně ovlivnit důvěrnost nebo integritu informací a nemůže způsobit dlouhodobou nedostupnost informací nebo procesů.

(c) **závažný KBI** – KBI, který může způsobit značnou škodu v důsledku ztráty důvěrnosti nebo integrity informací nebo může způsobit nepřijatelné časové období přerušení dostupnosti informací a/nebo procesů.

V případě nedodržení povinnosti informovat Objednatele dle tohoto odstavce do 24 hodin poté, co se o nežádoucí událostí dozví, je Poskytovatel povinen uhradit Objednateli smluvní pokutu ve výši 100.000,- Kč za každý případ porušení zajišťované smluvní povinnosti. Zaplacením smluvní pokuty není dotčen nárok Objednatele na náhradu škody vzniklé v důsledku nesplnění této povinnosti Poskytovatele.

12.3 Dodavatel musí oznámení zaslat e-mailem oběma kontaktním osoby. V případě, že by měl popis obsahovat informace s vysokou nebo kritickou důvěrností, musí být prostřednictvím e-mailu předán pouze obecný popis. Následný postup bude řešen individuálně. V případě závažného KBI musí Dodavatel oznámení provést také telefonicky minimálně na jednu z kontaktních osob.

Kontaktní osoby pro hlášení KBU/KBI:

[redacted]

E-mail: [redacted]
Tel.: [redacted]

[redacted]
E-mail: [redacted]
Tel.: [redacted]

CKTCH musí Dodavateli bezodkladně oznámit změnu kontaktních osob nebo jejich kontaktních údajů.

12.4 Dodavatel musí v souvislosti s plněním Smlouvy stanovit činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání KBU a KBI. Dodavatel musí podle takto stanovených a popsaných pravidel postupovat a hlásit všechny KBU a KBI související s plněním Smlouvy, včetně případů porušení zabezpečení osobních údajů ve výše stanovené lhůtě.

12.5 Dodavatel musí realizovat opatření pro snížení zranitelnosti aktiva souvisejícího s plněním Smlouvy vůči KBI a omezení dostupnosti způsobených Dodavatelem a vycházet při tom zejména z požadavků stanovených VKB.

12.6 Dodavatel musí CKTCH informovat o:

(a) významné změně ovládání Dodavatele nebo jeho poddodavatele;

(b) změně vlastnictví zásadních aktiv využívaných Dodavatelem k plnění Smlouvy nebo změně oprávnění nakládat s těmito aktivy,

a to nejpozději do 3 pracovních dnů od uskutečnění této změny.

13 POVINNOSTI PŘI UKONČENÍ SMLOUVY

13.1 V případě, že dojde k ukončení Smlouvy, musí Dodavatel i nadále dodržovat veškeré bezpečnostní požadavky stanovené právními předpisy, Smlouvou a Přílohy.

13.2 Dodavatel musí po ukončení Smlouvy v rozsahu pokynů CKTCH:

(a) vrátit CKTCH veškerou dokumentaci označenou jako důvěrnou, která mu byla předána;

(b) provést likvidaci dat, kterými disponuje v souvislosti se Smlouvou, pokud se nejedná o dokumenty, které musí Strana uchovávat podle právních předpisů;

(c) předat CKTCH prohlášení o vhodné likvidaci dat;

(d) předat CKTCH nezbytné informace, které:

(i) CKTCH umožní provedení migrace dat zpracovávaných na prostředcích dodaných či zajišťovaných podle Smlouvy na jiné systémy;

(ii) jsou do ukončení migrace nezbytné,

za účelem zajištění kontinuity služeb dodaných či zajišťovaných prostředky podle Smlouvy; rozsah a formu těchto informací musí Strany projednat v rámci ukončovacího období Smlouvy;

(e) účastnit se podle pokynů CKTCH jednání s CKTCH nebo třetí osobou za účelem plynulého a řádného převedení všech činností souvisejících s provozem, údržbou a rozvojem předmětu Smlouvy na CKTCH nebo třetí osobu.

14 ŘÍZENÍ KONTINUITY

14.1 CKTCH může zapojit Dodavatele do řízení kontinuity činností, zejména jej může zahrnout do:

(a) plánu kontinuity činností, který souvisí s aktivy souvisejícími s p plnění Smlouvy a souvisejících služeb;

(b) havarijního plánu CKTCH.

CKTCH musí Dodavatele o této skutečnosti informovat a poskytnou související dokumenty k připomínkám s dostatečným předstihem před jejich vydáním. Jakmile budou Stranami ujednány veškeré kroky, budou zapracovány do výpisu bezpečností dokumentace, jehož aktualizace bude předána Dodavateli podle odst. 3.1.

15 PODMÍNKY PŘEDÁVÁNÍ DAT

15.1 Veškeré provozní údaje, soubory, obsah logů, ostatní data a informace poskytnuté a zpracovávané v souvislosti s plněním Smlouvy (s výjimkou dat Dodavatele, která jsou jeho duševním vlastnictví) jsou ve výhradním vlastnictví CKTCH.

15.2 Předávání dat musí probíhat tak, aby je nemohly neoprávněné osoby číst, kopírovat, měnit ani mazat. Pokud CKTCH neurčí jinak, běžné informace, klasifikované jako informace s nízkou nebo střední důvěrností, budou zpravidla předávány prostřednictvím e-mailové komunikace, informace klasifikované jako informace s vysokou nebo kritickou důvěrností zpravidla prostřednictvím zabezpečeného cloudového úložiště CKTCH. CKTCH musí oznámit stupeň klasifikace informací oznámí Dodavateli před vlastním přenosem. Klasifikace informací CKTCH je specifikována v následujícím odstavci.

15.3 Klasifikace informací CKTCH:

(a) Informace s nízkou důvěrností:

(i) jsou veřejně přístupné bez omezení;

(ii) nenarušují důvěrnost primárních aktiv a neohrožují zájmy CKTCH;

(b) Informace se střední důvěrností:

(i) nejsou veřejně přístupné bez omezení;

(ii) jsou bez omezení přístupné zaměstnancům CKTCH;

(iii) jsou poskytovány nebo šířeny s definovaným omezením;

(iv) jsou přenášeny po veřejných komunikačních sítích jen určeným příjemcům;

(c) Informace s vysokou důvěrností:

(i) nejsou veřejně přístupné;

(ii) jsou sdíleny pouze mezi vymezeným oprávněným okruhem příjemců;

(iii) jsou sdíleny tak, že je vyhotoven záznam o přístupu nebo přenosu;

(iv) jsou přenášeny po veřejných komunikačních sítích jen určeným příjemcům s použitím ochranných kryptografických prostředků;

(d) Informace s kritickou důvěrností:

(i) nejsou veřejné přístupné;

(ii) jsou sdíleny pouze mezi taxativně vymezeným oprávněným okruhem příjemců;

(iii) jsou sdíleny tak, že je vyhotoven záznam o přístupu nebo přenosu;

(iv) jsou přenášeny po veřejných komunikačních sítích jen určeným příjemcům s použitím ochranných kryptografických prostředků a současně zabraňující zneužití jinými subjekty.

15.4 Pokud CKTCH neurčí jinak, Strany nesmí uchovávat předávaná data s výjimkou informací s nízkou důvěrností na přenosných datových nosičích.

16 PRAVIDLA PRO LIKVIDACI DAT

16.1 V případě, kdy Dodavatele disponuje daty CKTCH, musí se řídit pokyny CKTCH pro mazání dat a likvidaci technických nosičů, provozních údajů nebo informací a jejich kopií přiměřeně hodnotě a důležitosti aktiv a dále přiměřeně podle přílohy č. 4 VKB.

16.2 Likvidaci dat nepodléhají dokumenty, které musí Strana uchovávat podle právních předpisů.

17 DOKUMENTACE INFORMAČNÍHO SYSTÉMU ZÁKLADNÍ SLUŽBY

17.1 V případě, že je Dodavatel provozovatelem informačního systému základní služby, musí k němu vypracovat a předat CKTCH bezpečnostní dokumentaci alespoň v následujícím rozsahu:

(a) systémová příručka obsahující alespoň následující:

(i) popis funkcí, včetně bezpečnostních, které používá správce systému pro provádění určených činností a návod na používání těchto funkcí;

(ii) podrobný popis nebo odkaz na dokument, ve kterém je popis uveden a který je správci systému dostupný;

(iii) popis jednotlivých činností vykonávaných při správě a oprávnění nezbytných pro výkon těchto činností, definování uživatelů nebo skupin uživatelů a jejich oprávnění a povinnosti při využívání předmětu plnění;

(b) uživatelská příručka obsahující alespoň následující:

(i) popis funkcí, včetně bezpečnostních, které používá uživatel pro svou činnost a návod na použití těchto funkcí např. formou nápovědy v SW;

(c) potřebná provozní dokumentaci v rozsahu vyplývajícím z předmětu Smlouvy, zejména:

(i) dokumentace strategie obnovy (pokud není řešeno na straně CKTCH);

(ii) dokumentace skutečného provedení;

(iii) dokumentace obsahující popis autorizačního konceptu a oprávnění (pokud není řešeno na straně CKTCH);

(iv) dokumentace obsahující zálohovací a archivační postupy (pokud není řešeno na straně CKTCH);

(v) dokumentace obsahující instalační a konfigurační postupy (pokud se nejedná o know-how Dodavatele);

(vi) dokumentace obsahující bezpečností nastavení související s plněním Smlouvy.

PŘÍLOHA

ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Tato příloha obsahuje standardní ujednání o zpracování osobních údajů používané Centrem kardiovaskulární a transplantační chirurgie Brno.

Centrum kardiovaskulární a transplantační chirurgie Brno je v této příloze označeno jako „Zpracovatel" a dodavatel je v této příloze označen jako „Zpracovatel".

DEFINICE A VÝKLAD

Dále uvedené pojmy a zkratky mají v Příloze následující jednotný význam:

„**GDPR**" je Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 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).

„**Příloha**" je tento dokument nadepsaný „Zpracování osobních údajů".

„**Smlouva**" je smlouva, ke které je přiložena Příloha.

Pokud Příloha předpokládá písemný pokyn, souhlas nebo jinou komunikaci, musí být takové komunikace učiněna v elektronické podobě prostřednictvím e-mailu za použití uznávaného elektronického podpisu nebo prostřednictvím datové schránky nebo v listinné podobě osobním předáním nebo prostřednictvím držitele poštovní licence.

PŘEDMĚT

Předmětem Přílohy je úprava práva a povinností Správce a Zpracovatele při zpracování osobních údajů, se kterými Zpracovatel přišel, přijde nebo může přijít do styku při plnění Smlouvy, a to bez ohledu na to, zda se tak stalo záměrně s ohledem na předmět Smlouvy nebo z jiného důvodu, např. v důsledku omylu nebo kybernetického útoku.

Příloha se vztahuje na veškeré činnosti Zpracovatele vykonávané na základě Smlouvy, pokud to jejich povaha nevylučuje.

PŘEDMĚT, POVAHA, ÚČEL, MÍSTO A DOBA ZPRACOVÁNÍ

Předmětem zpracování jsou dále specifikované osobní údaje. Podrobnosti mohou být stanoveny ve Smlouvě.

Účelem zpracování je řádné plnění Smlouvy. Podrobnosti mohou být stanoveny ve Smlouvě.

Zpracovat může zpracovávat osobní údaje pouze v rozsahu nezbytném pro naplnění účelu Smlouvy.

Zpracovatel nesmí bez předchozího písemného souhlasu Správce zpracovávat osobní údaje za jiným účelem, než jaký vyplývá ze Smlouvy.

Zpracovatel nesmí bez předchozího písemného souhlasu Správce zpracovávat osobní údaje mimo území České republiky.

Doba zpracování trvá po dobu trvání Smlouvy, pokud Správce nevydá jiný pokyn nebo se Strany nedohodnou jinak.

TYP OSOBNÍCH ÚDAJŮ A KATEGORIE SUBJEKTU ÚDAJŮ

Příloha se vztahuje zejména na následující osobní údaje: jméno, příjemní, rodné číslo, datum narození, rok narození, genetické údaje, zdravotní stav, e-mailová adresa nebo jiný obdobný údaj, pokud lze na jeho základě identifikovat konkrétní fyzickou osobu.

Příloha se týká zejména následujících kategorií subjektů údajů: zaměstnanec Správce, pacient, osoby přistupující do informačních systémů Správce.

Pokud typ osobních údajů nebo kategorie subjektů údajů nevyplývají z právních předpisů, určuje jejich rozsah Správce. Zpracovatel nesmí zpracovávat Osobní údaje nad rámec pokynů Správce nebo nad rámec vyplývající z právních předpisů.

ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ, POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ

Zpracovatel musí přijmout v úvahu přicházející opatření požadovaná v článku 32 GDPR a musí být Správci nápomocen při zajišťování souladu s povinnostmi podle článků 32 až 36 GDPR, a to při zohlednění povahy zpracování a informací, jež má Zpracovatel k dispozici.

Zpracovatel musí s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob přijmout vhodná a dostatečná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku, které může být spojeno zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Zpracovatel musí Správci na jeho žádost předložit seznam přijatých opatření do 5 pracovních dnů od doručení takové žádosti. Zpracovatel garantuje stejnou nebo vyšší úroveň ochrany formou přijatých opatření uvedených v takovém seznamu po celou dobu trvání Smlouvy.

Zpracovatel musí bez zbytečného odkladu ohlásit Správci každé zjištěné porušení zabezpečení osobních údajů a poskytnout mu k tomu alespoň následující informace:

datum a hodina zjištění porušení;

popis povahy daného případu porušení;

kategorie a přibližný počet dotčených subjektů údajů;

kategorie a přibližné množství dotčených záznamů osobních údajů;

popis pravděpodobných důsledků porušení;

popis opatření, která Zpracovatel přijal nebo navrhl k přijetí s cílem vyřešit dané porušení, včetně případných opatření ke zmírnění možných nepříznivých dopadů;

zda má porušení za následek riziko nebo vysoké riziko pro práva a svobody fyzických osob;

zda Zpracovatel přijal následná opatření, která zajistila, že vysoké riziko pro práva a svobody subjektů údajů podle článku 34 odst. 1 GDPR se již pravděpodobně neprojeví.

Zpracovatel musí informovat Správce o pravděpodobnosti, že určitý druh zpracování, zejména při využití nových technologií, kterými Zpracovatel případně disponuje, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování mít za následek vysoké riziko pro práva a svobody fyzických osob. Takový druh zpracování nesmí Zpracovatel zahájit bez předchozího písemného souhlasu Správce.

VÝKON PRÁV SUBJEKTU ÚDAJŮ

Zpracovatel musí být Správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění Správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů stanovených v kapitole III GDPR.

Pokud se Zpracovatel dozví o uplatnění některého z práv subjektu údajů podle článků 12 až 23 GDPR, musí to oznámit Správci bez zbytečného odkladu, nejpozději však do 24 hodin od doby, kdy se o takovém dozvěděl.

UKONČENÍ ZPRACOVÁNÍ, VÝMAZ OSOBNÍCH ÚDAJŮ

Zpracovatel musí v souladu s rozhodnutím a pokyny Správce po ukončení plnění Smlouvy všechny osobní údaje vrátit Správci nebo je vymazat včetně všech existujících kopií, pokud nevyplývá z právních předpisů jinak.

Zpracovatel prohlašuje, že disponuje vhodným technickým opatřením, které umožňuje na základě rozhodnutí Správce výmaz vybraných osobních údajů.

POKYNY SPRÁVCE

Zpracovatel může zpracovávat osobní údaje pouze na základě doložených a zdokumentovaných pokynů Správce, a to i v případě předání osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu takové zpracování neukládají právní předpisy; v takovém případě Zpracovatel musí Správce informovat o takovém požadavku před samotným zpracováním, ledaže by právní předpisy takové informování zakazovaly z důležitých důvodů veřejného zájmu.

Pokyny Správce jsou obsaženy v Příloze a mohou být obsaženy také ve Smlouvě.

Správce může vydávat Zpracovateli i další písemné pokyny. Takové pokyny mají přednost před pokyny obsaženými v Příloze nebo ve Smlouvě.

Zpracovatel nesmí provádět pokyny vydané v rozporu s tímto článkem.

Správce musí po uzavření Smlouvy předložit Zpracovateli seznam osob oprávněných k vydání pokynů Správce. Správce je oprávněn prostřednictvím statutárního orgánu jednostranně písemně seznam oprávněných osob změnit.

Zpracovatel musí veškeré pokyny Správce na jeho vyžádání doložit a osvědčit tak oprávněnost jím prováděného zpracování.

Zpracovatel musí neprodleně informovat Správce, jestliže podle názoru Zpracovatele určitý pokyn Správce porušuje GDPR nebo jiné právní týkající se ochrany osobních údajů.

Zpracovatel nesmí zpracovávat osobní údaje pro Správce, pokud dojde k ukončení Smlouvy, neboť zpracování na základě uzavřené smlouvy je nezbytnou podmínkou pro naplnění požadavků vyplývajících z GDPR.

DALŠÍ ZPRACOVATELÉ

Zpracovatel nesmí bez předchozího písemného souhlasu Správce zapojit do zpracování dalšího zpracovatele.

Pokud Správce nepovolí použití dalšího zpracovatele, musí uvést důvody, pro které použití dalšího zpracovatele nepovolil a seznámit s nimi Zpracovatele.

Zpracovatel může opětovně požádat Správce o použití dalšího zpracovatele, pokud Správci předloží opatření, která přijal k odstranění námitek nebo obav Správce. Správce není povinen žádosti vyhovět.

Zpracovatel nesmí bez předchozího písemného souhlasu Správce zapojit do zpracování dalšího zpracovatele mimo území České republiky.

Pokud Zpracovatel zapojí dalšího zpracovatele, aby jménem Správce provedl určité činnosti zpracování, musí být tomuto dalšímu zpracovateli uloženy na základě smlouvy nebo jiného právního aktu stejné povinnosti na ochranu údajů, jaké jsou uvedeny v Příloze, a to zejména poskytnutí dostatečných záruk, pokud jde o zavedení vhodných technických a organizačních opatření tak, aby zpracování splňovalo požadavky GDPR. Neplní-li uvedený další zpracovatel své povinnosti v oblasti ochrany údajů, odpovídá Správci za plnění povinností dotčeného dalšího zpracovatele i nadále plně Zpracovatel. Další zpracovatel rovněž musí v plném rozsahu plnit povinnosti podle Přílohy, pokud Správce nevydá jiný pokyn nebo pokud to není objektivně vyloučeno.

POVINNOST MLČENLIVOSTI

Zpracovatel musí zachovávat mlčenlivost o všech skutečnostech, o kterých se dozvěděl v souvislosti se zpracováním. Stejnou povinnost mají i zaměstnanci Zpracovatele, další zpracovatelé a jejich zaměstnanci.

Povinnost mlčenlivosti trvá i po ukončení Smlouvy.

DALŠÍ POVINNOSTI ZPRACOVATELE

Zpracovatel musí poskytnout Správci veškeré informace potřebné k doložení toho, že Zpracovatel splnil povinnosti stanovené v čl. 28 GDPR, v Příloze a Smlouvě, a umožní audity, včetně inspekcí, prováděné Správcem nebo jiným auditorem, kterého Správce pověří, a k těmto auditům přispěje.

Zpracovatel musí umožnit Správci nebo jím určeným auditorům přístup do sídla Zpracovatele nebo na místa zpracování. Zpracovatel zajistí, aby měl Správce stejná oprávnění ve vztahu k dalším zpracovatelům.

Zpracovatel musí poskytnout na vyžádání Správci veškerou dokumentaci, kterou jsou dokumentována přijatá technická a organizační opatření k ochraně osobních údajů u Zpracovatele nebo dalších zpracovatelů.

Minimální technické požadavky

Úpravna vody pro laboratoře, 1 ks

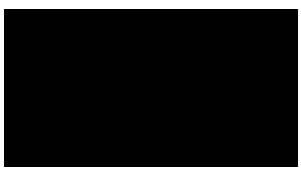
Popis parametru	Zadavatelem požadovaná hodnota	Uchazečem nabízená hodnota	Odkaz na konkrétní stránku v návodu k použití, nebo jinou oficiální dokumentaci výrobce	Závaznost
Dodavatel	**AquaOsmotic s.r.o.**	**87 800,- bez DPH 21%**	**www.aquaosmotic.cz**	
Výrobce	**AquaOsmotic s.r.o.**			
Typ/model	**AQ 50K**			
Výkon výrobníku 40-50 l/h.	Ano, uveďte (40-50 l/h)	45 l/h		Podmínka
Garantovaná čistota výstupní vody splňuje normu ČSN ISO EN 285.	Ano	ČSN ISO EN 285		Podmínka
Oplachový předfiltr 10“ s porozitou 50 mikronů.	Ano	10“ / 50 mikronů		Podmínka
Uhlíkový filtr 20“, CTC.	Ano	20“		Podmínka
Mechanický filtr 20“ s porozitou 1 mikron.	Ano	20“ / 1 mikron		Podmínka
Nerezové čerpadlo na zvýšení tlaku s frekvenčním měničem (přepravní).	Ano	E-Drive		Podmínka
Typ membrány – 3 ks reverzní osmóza.	Ano	3x RO MT-75		Podmínka
Uzavírání vstupní vody.	Ano	Regada		Podmínka
Snímání hladiny – 2x plovák.	Ano	2x plovák		Podmínka
Řídící jednotka (automatický provoz).	Ano	Ano, standart		Podmínka
Digitální vodivostiměr obdoba typu MW064MX.	Ano, uveďte	MW064MX		Podmínka
Ionexové dočištění 10 l typu Amberlite MB20.	Ano, uveďte	10L, Amberlite MB20		Podmínka
Průtokový rotametr typu GEMU – 1 ks.	Ano	1x Gemu		Podmínka
Plastový zásobník minimálně 90 l s výpustným ventilem.	Ano, uveďte (min. 90 l)	95L		Podmínka
Požadavky na napájení.	230 V, 16 A	230V, 16A		Podmínka
Další požadavky				
Třída rizika zdravotnického prostředku (ZP).	Uveďte třídu rizika ZP (I, IIa, IIb, III, nemá)	Není ZP		Informativní
Uveďte druh a četnost pravidelných kontrol doporučených výrobcem.	Uveďte	1x ročně		Informativní

Úpravna vody pro sterilizaci, 1 ks

Popis parametru	Zadavatelem požadovaná hodnota	Uchazečem nabízená hodnota	Odkaz na konkrétní stránku v návodu k použití, nebo jinou oficiální dokumentaci výrobce	Závaznost
Dodavatel	**AquaOsmotic s.r.o.**	**100 900,- bez DPH 21%**	**Www.aquaosmotic.cz**	
Výrobce	**AquaOsmotic s.r.o.**			
Typ/model	**AQ 150K**			
Výkon výrobníku 100-150 l/h.	Ano, uveďte (100-150 l/h)	100 – 150 l/h		Podmínka
Garantovaná čistota výstupní vody splňuje normu ČSN ISO EN 285.	Ano	ČSN ISO EN 285		Podmínka
Bypassem lze nastavit až na čistotu do 5 µS.	Ano	1 - 10us		Podmínka
Oplachový předfiltr 10“ s porozitou 50 mikronů.	Ano	10“ / 50 mikronů		Podmínka
Uhlíkový filtr 20“, CTC.	Ano	20“		Podmínka
Mechanický filtr 20“ s porozitou 1 mikron.	Ano	20“ / 1 mikron		Podmínka
Čerpadlo na zvýšení tlaku.	Ano	Fluitech		Podmínka
Typ membrány – reverzní osmóza.	Ano	RO-4021		Podmínka
Uzavírání vstupní vody elektromagnetickým ventilem.	Ano	Regada		Podmínka
Řídící jednotka (automatický provoz).	Ano	Ano, standart		Podmínka
Digitální vodivostiměr typu MW064MX.	Ano, uveďte	MW064MX		Podmínka
Ionexové dočištění 20 l typu Amberlite MB20.	Ano, uveďte	20L, Amberlite MB20		Podmínka
Plovákový rotametr typu GEMU – 3 ks.	Ano	3x Gemu		Podmínka
Plastový zásobník minimálně 250 l s výpustným ventilem.	Ano, uveďte (min. 250 l)	260L		Podmínka
Požadavky na napájení.	400 V, 16 A	230V, 16A		Podmínka
Další požadavky				
Třída rizika zdravotnického prostředku (ZP).	Uveďte třídu rizika ZP (I, IIa, IIb, III, nemá)	Není ZP		Informativní
Uveďte druh a četnost pravidelných kontrol doporučených výrobcem.	Uveďte	1x ročně		Informativní

Datum: 10. 10. 2025

Jméno, příjmení zodpovědné osoby: Petr Haška, jednatel



Cenová nabídka

Prosím zde uveďte rozepsané jednotkové ceny každé položky (cena jednotlivých samostatných položek/zařízení dodávky – příslušenství apod.) v Kč bez DPH a s DPH.

F-KB-03

Základní povinnosti v oblasti bezpečnosti informací v rámci servisního zásahu

Jméno, příjmení servisního technika: [redacted]
(dále jen „technický pracovník")

Externí technický pracovník je v případě osobního servisního zásahu (např. BTK) v prostorách CKTCH povinen dodržovat základní pravidla v oblasti kybernetické bezpečnosti a bezpečnosti informací. Informace obsažené v ICT (Informační a komunikační technologie) prostředcích a dalších zařízeních a dokumentech CKTCH smějí být využívány výhradně k plnění zadaných pracovních úkolů a jakékoliv jiné využití (například jejich neoprávněné kopírování nebo poskytování mimo CKTCH) se považuje za hrubé porušení povinnosti vyplývající z právních předpisů vztahujících se k vykonávané činnosti. Dále je technický pracovník povinen dodržovat následující zásady:

- Provádět servisní zásah pouze za vědomí biomedicínského inženýra a garanta oddělení/úseku, kde je servisní zásah prováděn.
- V případě nutnosti instalace software informovat s předstihem objednatele.
- Nepřipojovat žádné zařízení do neveřejné datové sítě CKTCH.
- V případě nutnosti výměny datového nosiče (harddisk) vyžádat součinnost zaměstnance Úseku IT a původní datový nosič ponechat v CKTCH.
- Neprovádět jakékoliv neoprávněné zásahy do operačního systému nebo programů (např. instalaci vlastního programu, změna konfigurace), není-li to nezbytně nutné z důvodu servisního zásahu.
- Provádět záznamy obrazovky a jakoukoliv další fotodokumentaci pouze v míře nezbytně nutné pro vykonání servisního zásahu. Veškeré takto provedené záznamy budou obsaženy v závěrečné zprávě. Provádět záznamy jakýchkoliv osobních dat a citlivých informací je přísně zakázáno.
- V případě nutnosti zapojení výměnného média, musí být toto médium před použitím prokazatelně zkontrolováno aktuálním antivirovým programem buď na PC technického pracovníka nebo na PC CKTCH k tomuto účelu určenému.
- Po dokončení servisního zásahu provést test funkčnosti a předat závěrečnou zprávu o provedení zásahu.

V Brně dne:

[redacted]

Technický pracovník

Podpis