**OBSAH**

[1. Vymezení některých pojmů a předmět přílohy 1](#_Toc63171979)

[2. Standardní smluvní ustanovení pro bezpečnost služeb poskytovaných přes internet (Cloud) 1](#_Toc63171980)

[3. Povinnosti vztahující se k bezpečnosti informačního systému a dat 2](#_Toc63171981)

[4. Povinnosti vztahující se na Subdodavatele 3](#_Toc63171982)

[5. Povinnosti vztahující se na CSP 3](#_Toc63171983)

[5.1. Lokace zpracování a uložení dat 3](#_Toc63171984)

[5.2. Governance / Dokumentace 3](#_Toc63171985)

[5.3. Backup 3](#_Toc63171986)

[5.4. Přístupové údaje / klíče 3](#_Toc63171987)

[5.5. Zabezpečení komunikace a dat 4](#_Toc63171988)

[5.6. Monitoring / kontrola 4](#_Toc63171989)

[5.7. Audit CSP 4](#_Toc63171990)

[5.8. Informační a ohlašovací povinnost (Security breach) 4](#_Toc63171991)

[5.9. CSP Reverzibilita / Exit strategie 4](#_Toc63171992)

[6. Bezpečnost produktů a služeb dodávaných Poskytovatelem služeb 4](#_Toc63171993)

[7. Závazky v případě, kdy Poskytovatel služeb přistupuje k informačnímu systému Objednatele 5](#_Toc63171994)

[8. Informační a ohlašovací povinnost 5](#_Toc63171995)

[9. Malware 5](#_Toc63171996)

[10. Povinnosti bezpečnostního útvaru Poskytovatele služeb 6](#_Toc63171997)

[11. Systém Vnitřní Kontroly 6](#_Toc63171998)

[12. Audit technické bezpečnosti 6](#_Toc63171999)

[13. Prevence Vendor lock-in 6](#_Toc63172000)

[14. Reverzibilita / Exit strategie 7](#_Toc63172001)

# Vymezení některých pojmů a předmět přílohy

„**CSP**“ nebo také „**Cloud Service Provider**“ je třetí osoba, která nabízí a poskytuje služby cloudové platformy, infrastruktury, aplikací nebo úložišť. CSP je většinou Subdodavatelem.

„**Subdodavatelem**“ se rozumí „**Subkontraktor**“, jak je definován ve Smlouvě a není-li Smlouvou tento pojem definován, pak je pro účely této Přílohy Subdodavatelem jakákoliv třetí osoba zajištěná Poskytovatelem, či v případě řetězení Subdodavatelů, některým ze Subdodavatelů, v souladu s touto Smlouvou pro potřeby poskytování služeb Objednateli.

Předmětem Přílohy je vymezení vzájemných práv a povinností Objednatele a Zhotovitele / Poskytovatele / Poskytovatele služeb (dále jen „**Poskytovatel**“ nebo „**Poskytovatel služeb**“) při poskytování služeb Poskytovatelem služeb Objednateli prostřednictvím internetu, tj. služeb v oblasti informačních technologií provozovaných na virtuální infrastruktuře Poskytovatelem prostřednictvím internetu a internetového prohlížeče umožňujícím přístup k rozšířitelnému a přizpůsobitelnému úložišti nebo výpočetním zdrojům, které je možné sdílet.

„**Zranitelnost**“ znamená jakoukoliv vadu, slabinu, chybu v provedení či malware ovlivňující příslušné produkty či služby poskytované na základě Smlouvy Objednateli.

„**Závažná zranitelnost**“ je taková zranitelnost, která může mít vážné dopady na informace, data a/nebo informační systém Objednatele.

# Standardní smluvní ustanovení pro bezpečnost služeb poskytovaných přes internet (Cloud)

Povinností Poskytovatele služeb je zajistit nezbytná technická a organizační opatření pro zajištění bezpečnosti služeb s dopadem na informační systém(y) a data Objednatele, za účelem:

* doložit a zajistit kontinuitu plnění legislativních a regulatorních požadavků souvisejících s předmětem Smlouvy a očekáváním všech regulatorních subjektů, jejichž kontrole či dohledu Objednatel podléhá např. České Národní Banky a Národního Úřadu pro Kybernetickou Bezpečnost, a to v celém řetězci subjektů poskytujících Objednateli služby, tedy včetně všech Subdodavatelů;
* povinně udržovat certifikaci služeb deklarovaných při pořizování dané služby na stejné, nebo vyšší úrovni v případě zpracování a/nebo přístupu ke klasifikovaným informacím Objednatele po celou dobu trvání Smlouvy;
* udržovat odpovídající úroveň bezpečnostní způsobilosti služby poskytované v souladu se smluvními podmínkami (kvalifikační, autorizační a certifikační podmínky) a být schopen na požádání jejich plnění prokázat. Poskytovatel služeb musí rovněž doložit, že má dostatečné znalosti o požadovaných technologiích a vlastní nezbytné know-how;
* zajistit důvěrnost, dostupnost, integritu a nepopíratelnost informačního systému Objednatele, a to do míry možných dopadů objednaných služeb na něj;
* chránit veškeré informace, data a údaje před vyzrazením, pozměňováním, zničením, ztrátou, zkreslením, neoprávněným zpřístupněním a zpracováním, a to ať již by šlo o činnosti náhodné, neoprávněné či nezákonné;
* zajistit monitoring a audit operací při zpracování informací a dat Objednatele, implementovat procesní a technická opatření, která vedou ke snížení rizika a vzniku bezpečnostních incidentů.

Poskytovatel služeb se zavazuje prokázat Objednateli, že výše uvedená opatření jsou zavedena po celou dobu trvání Smlouvy, a to bez zbytečného odkladu po obdržení výzvy Objednatele.

Bezpečnostní politika, postupy a opatření zaváděné Poskytovatelem služeb, případně i na základě pokynů Objednatele, musí být v každém případě řádně Poskytovatelem služeb zdokumentovány, zpřístupněny Objednateli a Poskytovatelem služeb upraveny při zohlednění citlivosti poskytovaných služeb, přičemž musí být po dobu trvání Smlouvy
v souladu s legislativou a praxí uplatnitelnou v dané oblasti.

# Povinnosti vztahující se k bezpečnosti informačního systému a dat

S ohledem na citlivost dat Objednatele, která mohou být v informačním systému Poskytovatele služeb zpracovávána, Poskytovatel služeb je povinen zvláštní pozornost tomu, aby zajistil fyzickou a logickou bezpečnost informačního systému, který pro zpracování dat Objednatele využívá.

Pokud informační systém Poskytovatele služeb zpracovává data Objednatele, pak je Poskytovatel služeb povinen zajistit následující:

* Zajistí ochranu důvěrnosti, dostupnost, integritu a nepopiratelnost informačního systému podílejícího se na dodávce služby;
* Zajistí přiměřené proškolení relevantního personálu podílejícího se na dodávce služby;
* Bezpečnostní opatření zavedená Poskytovatelem služeb musí být zdokumentována a být v souladu s legislativou a odvětvovou praxí uplatnitelnou v dané oblasti a na odpovídající úrovni;
* Zajistí zálohování dat nezbytných pro vlastní službu podle potřeby a na vyžádání Objednatele tak, že jak službu, tak i data bude možné obnovit dle smluvních podmínek. V případě, že součástí dodávané služby bude i zpracování dat Objednatele na straně Poskytovatele, Poskytovatel zajistí totéž pro data Objednatele;
* Postupy pro zálohování a obnovení budou nastaveny a předány Objednateli na začátku poskytování služby. Musí zahrnovat zejména odpovědnost, periodicitu, technické parametry, postupy k řízení přístupů, postupy pro obnovení dat, včetně kontrolních postupů. Poskytovatel služeb se zavazuje, že bude pravidelně, nejméně však jednou měsíčně / kvartálně / pololetně, provádět zkoušku obnovení dat a bude Objednateli na jeho vyžádání sdělovat výsledky této zkoušky;
* Pokud je to relevantní, Poskytovatel zajistí uložení a zpracování dat Objednatele, která musí být bezpečně logicky oddělena od vlastních dat Poskytovatele a/nebo dat náležejících třetím stranám;
* Zajistí zavedení systémů řízení oprávnění pro všechny uživatele (osobní účty, technické účty, apod.) kteří mají přístup k datům Objednatele prostřednictvím řízeného fyzického a logického přístupu;
* Zajistí předložení, na základě požadavku Objednatele a bezodkladně, všech stop a záznamů (např. auditních logů, událostí a bezpečnostních incidentů) a veškerých bezpečnostních analýz, prováděných Poskytovatelem služeb po celou dobu trvání smlouvy;
* Zavede a bude dodržovat bezpečnostní politiku určenou k tomu, aby byly uchovány použitelné záznamy dle související regulace, dále záznamy činností a/nebo pokusů o činnosti prováděné na vlastním informačním systému Poskytovatele služeb (např. toky příchozích/odchozích dat, nové verze aplikací, výsledky testování, počty chyb, odstranění duplicit, výmazy dat, atd.) pro účely kontrol (auditů) či pro důkazní účely. Záznamy musí zahrnovat: zdroj a cíl služby, typ události, identifikaci uživatele či systému a přesný časový údaj;
* Zajistí a zavede opatření do osmačtyřiceti (48) hodin od zjištění incidentu či hrozby v celém řetězci outsourcingu pro danou službu, které mohou ovlivnit dodávanou službu, mít přímý i nepřímý vliv na Objednatele (mj. reputační riziko). Poskytovatel zajistí řešení, které umožňuje účinně reagovat na daný incident či hrozbu. Poskytovatel služeb se rovněž zavazuje bez zbytečného odkladu informovat Objednatele o takových incidentech či hrozbách.

Pokud je předmětem plnění Smlouvy také zpracování osobních údajů, jak jsou definovány zvláštními právními předpisy, Poskytovatelem jako zpracovatelem, Poskytovatel doloží Objednateli v pravidelných intervalech minimálně jednou za dva roky správné provádění ochrany údajů, včetně provádění školení a to zprávou (papírovou nebo elektronickou) ve formě evidence.

Poskytovatel zajistí šifrování dat a komunikace end-to-end s použitím soudobě bezpečných algoritmů po celou dobu trvání Smlouvy.

Poskytovatel navíc zajistí, že zpracovávané údaje neopustí předem definovaný bezpečnostní perimetr pro:

* údaje zpracovávané mimo informační systém (například tištěné materiály);
* údaje zpracovávané v rámci informačního systému (definován ve Smlouvě).

Výjimka může být udělena jen na základě formální žádosti Poskytovatele služeb a písemné schválení Objednatele, a to při splnění následujících minimálních podmínek:

* údaje budou zabezpečeny proti případnému odcizení přenosných HW komponent šifrováním (viz článek 5.5), restriktivním řízením přístupových práv, a logováním;
* elektronické přenosy údajů mimo síť určenou k přenosu dat dohodnutou mezi Smluvními stranami je možné jen na základě přechozího písemného potvrzení Objednatele.

Poskytovatel služeb se zavazuje prokázat, že zaváděl výše uvedená opatření po celou dobu trvání Smlouvy, a bez zbytečného odkladu po vyžádání ze strany Objednatele.

Poskytovatel služeb se zavazuje po celou dobu trvání Smlouvy dodržovat regulatorní požadavky související s poskytovanou službou a neprodleně Objednatele informovat o případném nesouladu služby s regulatorními požadavky. Poskytovatel se zavazuje odstranit nedostatky a/nebo nesoulad v nezbytně krátkém čase, a to bez zbytečného odkladu po zjištění nesouladu a/nebo nedostatků. Objednatel v odůvodněných případech může určit/omezit geografické oblasti, kde mohou být data Objednatele uložena, zpracovávána a na jakém hostingu se nacházejí. Zmíněné geografické oblasti jsou v takovém případě definovány ve Smlouvě. Poskytovatel je oprávněn využít takovou lokalitu pouze v případě, pokud je dohodnuta ve Smlouvě nebo následně písemně schválena Objednatelem.

# Povinnosti vztahující se na Subdodavatele

Není-li Smlouvou sjednáno jinak, je Poskytovatel oprávněn plnit své povinnosti ze Smlouvy prostřednictvím Subdodavatelů, kteří byli Objednatelem předem písemně odsouhlaseni. Takovýto souhlas nebude Objednatelem Poskytovateli bez vážného důvodu odepřen. Za činnost Subdodavatele odpovídá Poskytovatel tak, jako by povinnost plnil sám. Poskytovatel je povinen zajistit, že smlouva, kterou uzavřel či uzavře se Subdodavatelem, případně jakékoliv smlouvy uzavřené mezi jednotlivými Subdodavateli, dochází-li k řetězení Subdodavatelů, nebudou v rozporu s obsahem Smlouvy včetně této Přílohy, ani nebudou obcházet její účel, a budou obsahovat zejména ustanovení Smlouvy upravující (i) audit, (ii) mlčenlivost, (iii) povinnost mít zavedeny odpovídající mechanismy vnitřní kontroly a řízení rizik, (iv) povinnost pravidelně prověřovat funkčnost a dostatečnost těchto mechanismů, (v) povinnosti uložené Poskytovateli touto Přílohou, (vi) povinnosti při zpracování osobních údajů, jsou-li zpracovávány a dále:

* V případě Subdodavatelů, kteří budou mít přístup k citlivým údajům nebo budou s citlivými daty manipulovat, musí být smluvně upraveno za jakých podmínek, jakým způsobem a v jakém rozsahu;
* Pro každého Subdodavatele bude určená kontaktní osoba po dobu trvání smluvního vztahu se Subdodavatelem;
* V případě úmyslu změny Subdodavatele, je povinen Poskytovatel o této skutečnosti Objednatele předem písemně informovat.

# Povinnosti vztahující se na CSP

Poskytovatel je povinen, kromě povinností stanovených Subdodavatelům, v případě CSP zajistit, aby CSP rovněž plnil veškeré povinnosti uvedené v tomto článku.

# Lokace zpracování a uložení dat

Všechna citlivá data musí být uložena a zpracovávána v prostoru Evropského hospodářského prostoru (EEA).). Poskytovatel je povinen zajistit, že data Objednatele budou uložena a/nebo zpracovávána v souladu se specifikací přípustných regionů.

# Governance / Dokumentace

Poskytovatel zajistí soupis a předání relevantní řídící a technická dokumentace, včetně auditní / compliance dokumentace, nezbytné pro dodávku služby. Zajistí aktuálnost a dostupnost této dokumentace Objednateli po celou dobu trvání Smlouvy.

# Backup

Poskytovatel zajistí správnou konfiguraci plánů obnovy a jejich pravidelné testování funkčnosti v souladu se specifikací danou Smlouvou, zejména s ohledem na ujištění o dostupnosti služby.

Poskytovatel na vyžádání Objednatele poskytne doklad o pravidelné revizi plánů obnovy včetně výsledků a přijatých opatření.

# Přístupové údaje / klíče

Uživatelské přístupové údaje a klíče související s poskytnutím služby musí být ve vlastnictví Objednatele. Poskytovatel je po celou dobu trvání Smlouvy povinen zajistit jejich dostupnost Objednateli, důvěrnost a integritu.

Poskytovatel zajistí tzv. *Lock mechanismus* (tzn. explicitní povolování administrátorského přístupu pro Poskytovatele jen pro konkrétní akci) vždy tam, kde to použitá Cloud platforma umožňuje. Poskytovatel je povinen mít přístupové údaje a klíče privilegovaných účtů ve svém výlučném vlastnictví související se správou služby bezpečně uchovány
a má povinnost je předat Objednateli při ukončení Smlouvy.

Poskytovatel nesmí přístupové údaje a klíče související s poskytnutím služby prodat, přenést, nebo licencovat či sub-licencovat na jiný subjekt bez předchozího písemného souhlasu Objednatele.

# Zabezpečení komunikace a dat

Poskytovatel zajistí šifrování dat a komunikace end-to-end s použitím soudobě bezpečných algoritmů po celou dobu trvání smlouvy.

Lze použít doporučení regulátora (nebo restriktivnější), například:

* [ČR] NÚKIB - Doporučení v oblasti kryptografických prostředků: Minimální požadavky na kryptografické algoritmy;
* [SR] NBÚ – Vyhláška 340/2004 Z. z., ktorou sa ustanovujú podrobnosti o šifrovej ochrane informácií

# Monitoring / kontrola

Poskytovatel v rámci vnitřního kontrolního systému zajistí pravidelnou kontrolu a monitoring dodávané služby.

Poskytovatel je dále Objednateli, pokud není možný online monitoring Objednatelem, je dodávat pravidelný měsíční report nad CSP. Součástí reportu jsou zejména tyto oblasti:

* Identity and access management;
* Patch / Vulnerability management;
* Incident / Problem management.

# Audit CSP

Poskytovatel je povinen u CSP zajistit právo Objednatele provést u CSP audit, a to jak Objednatelem, tak osobou určenou Objednatelem, případně osobou, které má právo kontrolovat a provádět dohled nad Objednatelem ve smyslu platných právních předpisů a zajistit Objednateli, případně jiným osobám oprávněným provést audit, přístup ke všem relevantním informacím nezbytným k tomu, aby bylo možné naplnit plnění povinností Objednatele při dohledu nad třetími stranami, které Objednatel vyžívá pro účely poskytování služeb.

# Informační a ohlašovací povinnost (Security breach)

Poskytovatel je povinen zajistit splnění oznamovací povinnosti, a to tak, že je povinen nejpozději do 24 hodin oznámit Objednateli všechny události s možným dopadem na poskytnutí služby Objednateli, včetně událostí reputačního rizika a/nebo nesouladu s právními a regulatorními požadavky.

V případě bezpečnostního incidentu je Poskytoval povinen oznámit bezpečnostní incident Objednateli bez zbytečného odkladu, nejpozději však do \_\_\_\_\_ od vzniku bezpečnostního incidentu.

# CSP Reverzibilita / Exit strategie

Poskytovatel je povinen zajistit Exit strategii alespoň v rozsahu požadovaném Smlouvou a je povinen předložit takovou Exit strategii Objednateli bez zbytečného prodlení po vyzvání Objednatelem.

# Bezpečnost produktů a služeb dodávaných Poskytovatelem služeb

Poskytovatel služeb se zavazuje:

* pokud je zjištěn nový případ závažné zranitelnosti: předložit Objednateli do osmi (8) pracovních hodin, od okamžiku zjištění zranitelnosti, rozbor dopadů a plán nápravných opatření v souladu s požadavky Objednatele,

- předložit Objednateli do dvou (2) pracovních dní od okamžiku zjištění zranitelnosti, jakékoliv zmírňující či dočasné řešení, které však žádným způsobem nemění cenu či funkčnost produktů
a služeb dodávaných podle Smlouvy;

- předložit Objednateli konečné řešení problému do pěti (5) pracovních dní od okamžiku zjištění zranitelnosti;

* pokud je zjištěn nový případ zranitelnosti, která není klasifikována jako závažná zranitelnost:

- předložit Objednateli do čtyř (4) pracovních dní od okamžiku zjištění zranitelnosti, jakékoliv zmírňující či dočasné řešení, které však žádným způsobem nemění cenu či funkčnost produktů a služeb dodávaných podle Smlouvy;

- tam, kde nebude vhodné nápravné opatření zajištěno do čtyř (4) pracovních dní od okamžiku zjištění zranitelnosti, bude Objednateli předloženo konečné řešení k odstranění problému do osmi (8) pracovních dní od zjištění zranitelnosti a Objednatel bude pravidelně informován o postupu Poskytovatele služeb;

- pokud je to relevantní, Poskytovatel se zavazuje dodat Objednateli softwarovou aplikaci a/nebo prostředky nezbytné pro odstranění zranitelnosti;

* v obecné rovině, informovat Objednatele o rizicích, souvisejících s dodávkou služby (vedoucích k případné degradaci důvěrnosti, dostupnosti, integrity či nepopiratelnosti) a nabídnout zavedení konkrétních opatření pro jejich mitigaci při uvedení souvisejících nákladů, které musí Objednatel předem písemně schválit.

# Závazky v případě, kdy Poskytovatel služeb přistupuje k informačnímu systému Objednatele

Poskytovatel (a relevantní zúčastněné třetí strany zřetězeného outsourcingu, tj. Subdodavatelé) se zavazuje používat jen takové zdroje a prostředky pro připojení k informačnímu systému Objednatele, které mu Objednatel poskytne, a to výhradně pro účely poskytování služeb sjednaných ve Smlouvě a v souladu s relevantními vnitřními předpisy Objednatele, které budou Poskytovateli Objednatelem předány. Poskytovateli služeb se bez předchozího písemného souhlasu Objednatele nepovoluje jakékoliv používání, sdělování, šíření či přenášení důvěrných informací a dat Objednatele mimo informační systém Objednatele.

Tam, kde pracovníci Poskytovatele služeb mohou mít přístup k informačnímu systému Objednatele a kde jsou Objednatelem k takovému přístupu výslovně a předem zmocněni, ať již jde o přístup při práci v prostorách Objednatele, nebo formou vzdáleného přístupu, musí být tito pracovníci řádně seznámeni s relevantními vnitřními předpisy Objednatele a řídit se jimi.

Poskytovatel služeb zajistí, že jeho zaměstnanci budou pravidelně seznámeni a proškoleni s materiály, které jsou pro ně určeny, a to ještě před jejich přidělením k daným úkolům (během prvních 5 pracovních dnů dle výjimky odsouhlasené Objednatelem), během nichž jim Objednatel tyto podklady poskytne.

# Informační a ohlašovací povinnost

Poskytovatel je povinen:

* bez zbytečného odkladu informovat Objednatele o jakémkoliv bezpečnostním incidentu, který vznikne v jeho informačním systému (včetně přístupu neoprávněné třetí strany, ztráty dat, poškození integrity dat, zavlečení malwaru a/nebo nestandardního použití informačních systémů používaných pro služby Objednatele), a to kdykoliv, kdy takový incident může ovlivnit informační systém, služby, informace a data Objednatele s ohledem na poskytovanou službu;
* zajistit, aby pracovníci pověření takovými úkoly dodržovali tyto povinnosti a zajistit jejich pravidelnou informovanost o nich;
* dodržovat ustanovený komunikační prostředek / komunikační kanál po celou dobu trvání Smlouvy;
* informovat Objednatele o jakýchkoliv organizačních a technických změnách, které by mohly mít negativní vliv na bezpečnost informací a dat Objednatele;
* zavést pravidelný monitoring, který určí Objednatel, s cílem snížit rizika ztráty důvěryhodnosti, celistvosti a dostupnosti, nepopíratelnosti dat Objednatele, jakoukoliv třetí stranou nebo jakýmkoliv uživatelem jednajícím za Poskytovatele služeb;
* zavést systém a metodiku řízení bezpečnostních incidentů, která bude popisovat proces pro detekci bezpečnostních incidentů, odezvy a spuštění procesů krizového managementu (metodika a její případné změny podléhají předchozímu písemnému souhlasu Objednatele);
* poskytovat součinnost Objednateli, a to bez nároku na dodatečnou odměnu, při přijímání nápravných opatření či vypořádání se s bezpečnostními incidenty, včetně informování příslušných orgánů a osob, které by takovým narušením mohly být poškozeny;
* bez zbytečného odkladu specifikovat záložní a nápravné postupy pro zvládnutí těchto incidentů, včetně jejich dopadů na ochranu informačního systému Objednatele a bezpečnost jeho informací a dat.

Poskytovatel služeb je povinen předložit Objednateli na požádání výsledky bezpečnostního auditu informačního systému Poskytovatele (zejména identifikována rizika a zranitelnosti) ve vztahu k poskytované službě prováděného minimálně jednou ročně provedeného třetí stranou u jakéhokoliv produktu a softwaru licencovaného Poskytovatelem služeb při přechodu na produkční provoz či při každé zásadní změně či aktualizaci. Poskytovatel služby se zavazuje implementovat bezpečnostní opatření v celém životním cyklu od vývoje, realizaci až po ostrý provoz, kde musí Objednateli doložit nastavení procesů a technologií, které vedou ke snížení rizika a zlepšení kvality kódu, produktů či služeb Poskytovatele.

# Malware

Poskytovatel služeb přijme veškerá nezbytná preventivní opatření proti zavlečení malwaru do informačního systému, který může obsahovat informace a data Objednatele a také taková odpovídající opatření, která existenci malwaru zjistí. Za tímto účelem, Poskytovatel služeb bude provádět odpovídající bezpečnostní testy a zavazuje se ke kontrole komponent informačního systému před tím, než je Objednateli dodá.

Pokud již k zavlečení malwaru do informační systému dojde, navzdory opatřením výše, Poskytovatel služeb a Objednatel se dohodli na tom, že budou pracovat ve vzájemné shodě k tomu, aby zjistili jeho zdroj a opravili vzniklé škody bez zbytečného prodlení. V případě zjištění, že:

* Nákazu či zavlečení malwaru lze přičítat Objednateli, nese náklady na diagnostiku a obnovení dotčených systému či služeb Objednatel.
* Nákazu a zavlečení malwaru lze přičítat Poskytovateli služeb, nese náklady na diagnostiku a obnovení dotčeného systému či služeb Poskytovatel služeb.
* Nelze jednoznačně identifikovat zavinění konkrétní strany / jednotlivce, bude se postupovat dle postupu pro řešení sporu uvedeného ve Smlouvě, je-li sjednán.

# Povinnosti bezpečnostního útvaru Poskytovatele služeb

Poskytovatel služeb je povinen určit manažera pro bezpečnost a řízení rizik, který bude jediným kontaktním místem Objednatele pro tuto problematiku.

# Systém Vnitřní Kontroly

Poskytovatel zajistí odpovídající nezávislost výkonu vnitřní kontroly vzhledem k povaze, předmětu a významu služby a zamezení střetu zájmů při zajišťování všech kontrolních mechanismů včetně kontroly řízení rizik a regulatorního souladu.

Poskytovatel služeb se zavazuje zajistit, aby úroveň kontroly rizik byla soustavně monitorována a aby bezpečnostní politika a pravidla uplatňovaná na služby byly dodržovány, včetně jeho Subdodavatelů.

Poskytovatel zajistí nápravu zjištěných nedostatků bez zbytečného odkladu v požadované lhůtě. V případě, že vnitřní kontrolní systém Poskytovatele nebude v souladu s očekáváním sektorové regulace [mj. Vyhláška č. 163/2014 Sb.], Objednatel je oprávněn vypovědět Smlouvu dle podmínek uvedených ve smlouvě, aniž by to přitom nějak ovlivnilo jeho nárok na jakékoliv odškodnění, které může v této souvislosti požadovat.

#  Audit technické bezpečnosti

[IF RELEVANT] Poskytovatel služeb zajistí, že Objednatel je oprávněn po celou dobu trvání Smlouvy v souladu s požadavky regulace provádět technické audity (včetně skenování, automatického testování zranitelnosti, zkoušek na infiltraci, auditů konfigurace a infrastruktury, případně dotazování, či ověřování) na informačním systému Poskytovatele a i u jakékoliv třetí strany včetně (CSP). Objednatel je oprávněn pověřit provedením auditu třetí stranu, se kterou bude uzavřena smlouva o mlčenlivosti, jejíž smluvní stranou bude i Poskytovatel. Bez této smlouvy je oprávněna audit provést Česká národní banka (nebo pověřenec).

Objednatel bude audity provádět primárně formou dotazování a vzdáleného ověřování, zejména v případě důvodného podezření z narušení či zranitelnosti informačního systému Poskytovatele i na místě.

Auditorovi bude umožněno provádět technický audit, či provádět nezbytné dotazování s cílem ověřit úroveň zabezpečení důvěrnosti, dostupnosti, integrity a nepopiratelnosti u poskytovaných služeb. Tyto zkoušky můžou sestávat ze souborů prováděných testů, ať automatizovaných či manuálních, zvnějšku či v informačním systému Poskytovatele služeb, či v informačním systému kteréhokoliv subdodavatele, který je zaangažován na poskytování daných služeb, a to s cílem zjistit jakékoliv zranitelnosti, které by umožnily uživatelům se infiltrovat do testovaného systému.

Poskytovatel služeb je povinen zajistit přístup auditorů k provádění technických auditů na daném informačním systému a informačních systémech všech třetích stran (včetně CSP), které mohou být zaangažovány či jinak dotčeny.

Tyto technické audity budou prováděny v souladu s platnou regulací a legislativou, ne častěji než jednou za kalendářní rok a budou předmětem předchozího upozornění sděleného Poskytovateli služeb a nenaruší poskytování služeb. Tímto se rozumí, že účelem těchto technických auditů není umožnit Objednateli přístup k datům jiných klientů Poskytovatele služeb, ale pouze ověřit bezpečnost systému a / nebo infrastruktury, v rámci kterých mu jsou služby poskytovány.

Zranitelnosti zjištěné auditem budou vyhodnoceny a bude s nimi nakládáno podle podmínek uvedených v článku 6., „Bezpečnost produktů a služeb dodávaných Poskytovatelem služeb“.

V případě, že Poskytovatel služeb nezajistí nápravu nedostatků zjištěných auditem v požadované lhůtě, potom bude Objednatel automaticky oprávněn vypovědět Smlouvu dle podmínek uvedených ve smlouvě, aniž by to přitom nějak ovlivnilo jeho nárok na jakékoliv odškodnění, které může v této souvislosti požadovat.

# Prevence Vendor lock-in

Není-li sjednáno Smlouvou jinak a v případě, že v rámci plnění Smlouvy předá Poskytovatel Objednateli zdrojové kódy, nebo, je-li sjednána úschova zdrojových kódu (escrow), je Poskytovatel povinen nabízet produkty či služby respektující principy interoperability a otevřených formátů, pokud není výslovně sjednáno jinak.

Poskytovatel je povinen nabízet Objednateli:

* řešení respektující principy mikroservisní architektury (decoupling) na jednotlivé celky, jež vzájemně komunikují standardizovanými, preferovaně veřejně dostupnými protokoly;
* formát datových souborů a metadat, preferovaně nezávislý na konkrétním technickém a programovém vybavení. Pokud daný formát není dostupný z veřejných zdrojů, musí Poskytovatel bezúplatně poskytnout Objednateli, po celou dobu trvání smlouvy, prostředek pro zpracování daného formátu.

# Reverzibilita / Exit strategie

Poskytovatel je povinen udržovat tzv. Exit strategii po celou dobu platnosti smlouvy, která musí zahrnovat alespoň:

* Podmínky, postup, termíny a odpovědnost za spuštění Exit strategie;
* kontaktní matici u Poskytovatele a relevantních Subdodavatelů (včetně CSP);
* definici způsobu a rozsahu předání dat týkajících se a/nebo vyplývajících z předmětu Smlouvy a jejich bezpečnou destrukci;
* Převod znalostí (*knowledge transfer*) a jejich rozsah, týkající se předmětu Smlouvy, z Poskytovatele na Objednatele tak, aby byla zajištěna kontinuita poskytované služby;
* odebrání uživatelských přístupů, HW a/nebo SW prostředků v majetku Objednatele.

Není-li na základě dohody Objednatele a Poskytovatele Exit strategie součástí Smlouvy, je Poskytovatel povinen Objednateli Exit strategii předložit bez zbytečného prodlení po vyzvání Objednatelem.

V případě výzvy Objednatele kdykoliv během trvání Smlouvy nebo v případě ukončení Smlouvy z jakéhokoli důvodu je Poskytovatel povinen umožnit Objednateli bez zbytečného odkladu bezpečné převzetí veškerých dat Objednatele umístěných v Cloudu. Za tímto účelem je Poskytovatel zejména povinen Objednateli poskytnout nezbytné licence, software a veškeré Objednatelem vyžadované zdroje, a to vše na náklady Poskytovatele.

V případě ukončení Smlouvy je po převzetí dat Objednatelem v souladu s tímto ustanovením ve lhůtě do 90 kalendářních dnů po převzetí dat Objednatelem Poskytovatel povinen zajistit nevratné vymazání všech dat Objednatele s formálním doložením této skutečnosti Objednateli, s výjimkou zákonně ustanovených archivačních povinností Poskytovatele.