OBSAH

1. STANDARDNÍ SMLUVNÍ USTANOVENÍ V OBLASTI OCHRANY INFORMAČNÍCH SYSTÉMŮ A DAT

1.1. POVINNOSTI V RÁMCI VŠEOBECNÉ BEZPEČNOSTI

Povinností poskytovatele služeb (zhotovitele díla apod.) je zavádět nezbytná technická a organizační opatření pro zajištění bezpečnosti služeb včetně informačních systému a dat objednatele, s cílem:

- udržovat odpovídající úroveň bezpečnostní způsobilosti informačních systémů pro 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 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, že tato opatření zavedl v celém období trvání smlouvy, a to bez zbytečného odkladu na požádání ze strany objednatele.

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

1.2. POVINNOSTI VZTAHUJÍCÍ SE K OCHRANĚ INFORMAČNÍHO SYSTÉMU POSKYTOVATELE SLUŽEB

S ohledem na citlivost dat objednatele, která mohou být v informačním systému poskytovatele služeb zpracovávána, poskytovatel služeb bude věnovat 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, potom musí poskytovatel služeb zajistit následující:

- Zajistí ochranu důvěrnosti, dostupnost a integritu svého informačního systému;

  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 a dat objednatele, podle potřeby a na vyžádání objednatele tak, že jak službu, tak i data bude možné obnovit dle smluvních podmínek;
- 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, provádět zkoušku obnovení dat a bude objednateli na jeho vyžádání sdělovat výsledky této zkoušky;

- Zajistí uložení a zpracování dat objednatele, která musí být uložena oddělené od vlastních dat poskytovatele anebo 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 bezpečnostní politiku určenou k tomu, aby byly udržovány použitelné záznamy po dobu jednoho roku, 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, které mohou ovlivnit vlastní informační systém poskytovatele služeb, vhodné posílení bezpečnostních opatření či jakéhokoliv jiné řešení, které umožňuje účinně reagovat na incident či hrozbu. Poskytovatel služeb se zavazuje bez zbytečného odkladu informovat objednatele o takových incidentech či hrozbách.

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 informovat objednatele o lokalitách (stát, město, ulice), kde jsou jeho informace a data uložena, zpracovávána a na jakém hostingu se nacházejí. Objednatel může určit/omezit geografické oblasti, kde mohou být jeho data uložena, zpracovávána a na jakém hosting se nacházejí. Zmíněné geografické oblasti jsou definovány ve smlouvě.

Poskytovatel a/nebo subdodavatel písemně schválený objednatelem je oprávněn využít takovou lokalitu pouze v případě, pokud je dohodnuta ve smlouvě nebo následně písemně schválena objednatelem v rámci dodatku ke smlouvě.

1.3. BEZPEČNOST PRODUKTŮ A SLUŽEB DODÁVANÝCH POSKYTOVATELEM SLUŽEB

Zranitelnost *znamená jakoukoliv vadu, slabinu, chybu v provedení či malware ovlivňující příslušné produkty či služby, na které se vztahuje smlouva.*

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

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 zahrnutých v rámci 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,
  - ze strany výrobce/vývojáře dodat objednateli softwarovou aplikaci nezbytnou pro odstranění zranitelnosti,
- v obecné rovině, informovat objednatele o rizicích, souvisejících s bezpečností a ochranou informačních systémů a nabídnout zavedení konkrétních opatření pro detekci pokusů o narušení a bezpečnostních incidentů při uvedení souvisejících nákladů, které musí objednatel schválit.

1.4. ZÁVAZKY V PŘÍPADĚ, KDY POSKYTOVATEL SLUŽEB POUŽÍVÁ INFORMAČNÍ SYSTÉM OBJEDNATELE

Poskytovatel služeb 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 dohodnutých v rámci smlouvy a v přísném souladu s bezpečnostními politikami informačního systému objednatele, které budou poskytovateli služeb předány. V tomto ohledu, se poskytovateli služeb, bez výslovného oprávnění ze strany 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, vyžaduje bezpečnostní politika informačního systému objednatele, aby se takoví pracovníci seznamovali s materiály, vztahujícími se k oblasti bezpečnosti informačních systémů, které jsou pro ně určeny a řídili 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 či během několika prvních dní, během nichž jim objednatel tyto podklady poskytne.

1.5. INFORMAČNÍ A OHLAŠOVACÍ POVINNOST

Poskytovatel služeb 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,
- 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 odcizení informací a dat objednatele, nebo neoprávněného přístupu k nim jakoukoliv třetí stranou nebo jakýmkoliv uživatelem jednajícím za poskytovatele služeb;
- zavést 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 má za povinnost 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 s nížení rizika a zlepšení kvality kódu, produktů či služeb poskytovatele.

1.6. MALWARE

*Pojem **Malware** znamená škodlivý strojový kód, včetně specifických virů, logických bomb, červů, trojských koní, či jakýchkoliv jiných kódů či instrukcí infikujících či napadajících jakékoliv programy, software, data, soubory, databáze, počítače či jiný hardware a jeho komponenty a které poškozují či vyzrazují utajení dat či ohrožují jejich integritu, přičemž ruší některé či všechny operace, obsazují veškeré či některé části informačního systému a umožňují, aby se činnosti systémů odchylovaly od jejich určeného účelu.*

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, 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 prodlení.

Pokud se zjistí, že nákazu či zavlečení malwaru lze přiřadit objednateli, potom objednatel ponese náklady na diagnostiku a obnovení dotčených systému či služeb.

Pokud se zjistí, že nákazu a zavlečení malwaru lze přiřadit poskytovateli služeb, potom poskytovatel služeb ponese náklady na diagnostiku a obnovení dotčeného systému či služeb.

Pokud se na identifikaci zavinění kontaktní osoby smluvních stran nedohodnou, bude se postupovat dle postupu pro řešení sporu uvedeného ve smlouvě.

1.7. 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 (možný kontakt i na DPO (pověřenec pro ochranu osobních údajů) dle Nařízení EU č. 2016/679).

1.8. KONTROLA A AUDIT

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.

1.8.1. AUDITY TECHNICKÉ BEZPEČNOSTI

Poskytovatel služeb souhlasí, že objednatel je oprávněn 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 – subdodavatelů, včetně těch společností, které hostují částečně či celý informační systém poskytovatele služeb. 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.

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 bezpečnosti příslušných systémů. Tyto zkoušky budou 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.

V tomto ohledu poskytovatel služeb zaručuje, že je držitelem nezbytných a dostatečných práv a oprávnění k provádění shora uvedených technických auditů na daném informačním systému a informačních systémech všech třetích stran, které mohou být zaangažovány či jinak dotčeny.

Tyto technické audity budou prováděny v souladu s platnou regulací a legislativou 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 infrastruktury, v rámci kterých mu jsou služby poskytovány.

1.8.2. VYPOŘÁDÁNÍ NEDOSTATKŮ

Zranitelnosti zjištěné auditem budou vyhodnoceny a bude s nimi nakládáno podle podmínek uvedených v oddílu „Bezpečnost“, v článku „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 odstoupit od smlouvy bez předchozího upozornění, aniž by to přitom nějak ovlivnilo jeho nárok na jakékoliv odškodnění, které může v této souvislosti požadovat.

1.9. POVINNOSTI V RÁMCI TESTOVÁNÍ BEZPEČNOSTI ZDROJOVÉHO KÓDU SOFTWARE

V případě, že je předmětem plnění dle příslušné smlouvy (např. smlouva dílo, smlouva o poskytování služeb, licenční smlouva) dodání či vývoj software poskytovatelem objednateli, je poskytovatel povinen provádět na vlastní náklady bezpečnostní analýzu a test zdrojového kódu software (tzv. *Security Code Review*) podle verifikačních požadavků OWASP Application Security Verification Standard (ASVS), a to před předáním zdrojového kódu software objednateli. Poskytovatel je rovněž povinen na výzvu objednatele doložit objednateli dostatečné důkazy o důkladném testování zdrojového kódu software. V případě sporu o kvalitě provedeného testování je poskytovatel povinen objednateli na výzvu objednatele předložit dostatečné důkazy o skutečnostech, že každý relevantní požadavek, který může mít vliv na bezpečnost a řádnou funkci zdrojového kódu software, byl poskytovatelem otestován, a pokud nebyl, je poskytovatel povinen objednateli zdůvodnit jeho netestování. Objednatel je oprávněn v případě pochybností o kvalitě provedeného testování požadovat na poskytovateli dodatečné otestování zdrojového kódu software na náklady poskytovatele.

V případě, že poskytovatel nesplní povinnosti na *Security Code Review*, nebo v případě zjištění vad, a to zjevných zjištěných v rámci převzetí software, které zabraňují dle názoru objednatele nasazení zdrojového kódu software do produkčního prostředí objednatele, či skrytých, které se objeví až po převzetí software objednatelem, je poskytovatel povinen objednateli uhradit náklady vzniklé objednateli v souvislosti se zjištěním a odstraněním takovýchto vad.

1.10. DALŠÍ UJEDNÁNÍ V OBLASTI OCHRANY INFORMACÍ A DAT

Pracovníci poskytovatele jím budou proškoleni v oblasti ochrany údajů (informace, data, osobní údaje apod.), zejména pak s ohledem na platné a účinné právní a regulatorní předpisy (například Zákon č. 21/1992 Sb., o bankách, 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 - GDPR)).

Poskytovatel je povinen sledovat aktuálnost uvedených legislativních předpisů a případně reagovat na jejich novelizaci.

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, že zpracovávané údaje neopustí bezpečnostní perimetr objednatele:

a. bezpečnostní perimetr pro údaje zpracovávané mimo informační systém (například tištěné materiály) je definován výčtem budov, místností, které jsou pod bezpečnostní ochranou objednatele/poskytovatele, kde dochází ke zpracování údajů, viz zejména místo plnění dle smlouvy;

b. bezpečnostní perimetr pro údaje zpracovávané v rámci informačního systému je definován zařízeními ve správě objednatele, výjimka může být udělena jen na základě formální žádosti a písemné schválení objednatele a při splnění následujících minimálních podmínek:

    i. údaje budou zpracovávány jen na HW zařízeních plně pod správou poskytovatele (zpracování v cloud computing se nepřipouští);

    ii. údaje budou zabezpečeny proti případnému odcizení přenosných HW komponent šifrováním;

    iii. na HW poskytovatele pro zpracování údajů je implementována standardní bezpečnost založená na důsledném aplikování přístupových práv, o důležitých událostech jsou tvořeny bezpečnostní záznamy;

    iv. místnost s ostatním HW vybavením je uzamčena a přístup je omezen jen na vybrané pracovníky poskytovatele, místnost tvoří režimové pracoviště;

    v. údaje jsou zálohovány standardními procedurami poskytovatele;

    vi. elektronické přenosy údajů předávaných objednatelem nejsou možné mimo síť určenou k přenosu dat dohodnutou mezi smluvním i stranami.

Cloud computing - model uplatňovaný v oblasti informačních a komunikačních systémů a technologií, který umožní získat síťový přístup ke konfigurovatelným výpočetním prostředkům (např. sítě, servery, datová úložiště, aplikace a služby), které jsou sdíleny větším množstvím uživatelů a jejichž kapacita je poskytována a opět uvolňována s minimálními nároky na jejich správu anebo na intervenci poskytovatele cloud computingu.

Použití evropských předpisů o předávání údajů mimo Evropskou unii

Poskytovatel zajistí, že žádné údaje od objednatele, tj. včetně osobních údajů fyzických osob, nebudou předávány mimo státy Evropské unie poskytovatelem a/nebo jakoukoliv osobou jednající jeho jménem a/nebo subdodavatelem. Objednatel je oprávněn si plnění této povinnosti ověřit.

Poskytovatel, pokud tak bude dohodnuto s objednatelem, je oprávněn v rozsahu nezbytně nutném pro plnění smlouvy, využít zdroje zpracování dat ve státě, který nezajišťuje adekvátní úroveň ochrany údajů dle Nařízení EU č. 2016/679 (GDPR), za podmínky uzavření standardních smluvních doložek, jak jsou stanoveny ve smyslu článku 46. GDPR. Na žádost objednatele budou tyto doložky podepsány poskytovatelem, subdodavatelem, pokud je zahrnut do zpracování, a objednatelem. Poskytovatel zajistí podepsání a plnění těchto doložek ze strany subdodavatele. V případě požadavku schválení takového předávání Úřadem pro ochranu osobních údajů či jiným obdobným regulatorním orgánem bude možné nechat zpracovávat údaje ve třetím státě pouze v případě obdržení souhlasu takového orgánu, vedle podpisu výše uvedených doložek, pokud jsou dle GDPR nutné (více zejména čl. 46. GDPR).