Ptáme se právníka

JUDr. Lukáš Michna, LL.M., Ph.D.

Advokát
Advokátní kancelář Lukáš Michna
Vojtěšská 212/8
110 00 Praha 1
+420 777 189 480
lukas.michna@aklm.cz

Firmy mají velice často šablonu formuláře, který právně ošetřuje přístup do sítě, k datům a interním zdrojům třetími stranami. Zajímalo by mne, jaká je vlastně právní vymahatelnost takového dokumentu, co všechno by měl obsahovat a kým by měl být podepsán?

Takové formuláře skutečně existují, sám jsem jich řadu vytvořil i podepsal. Přestože je dotaz položen spíše obecně, rozumím, o co se tazateli jedná. Než se pustím do samotné odpovědi, dovolím si nicméně jednu drobnou výhradu. Předpokládám, že se tazatel netáže na různé klikací souhlasy na formulářích pro přístup k veřejné nebo návštěvnické wi-fi. Kromě toho bych ještě předeslal, že se na předmětnou problematiku podívám z perspektivy společnosti, která přístup ke své infrastruktuře poskytuje, nikoli z pohledu třetí strany.

Především je třeba uvést, že podobné formuláře nemají žádnou pevně danou strukturu a jejich obsah záleží na podmínkách konkrétní společnosti, zpravidla v závislosti na tom, k jaké infrastruktuře a případně i datům třetí stranu pouštějí. Obecně se jedná o smlouvu mezi naší společností a třetí stranou. Obsah může být vysoce individualizován, není upraveným smluvním typem a jedná se o smlouvu inominátní. Forma není předepsána, postačí i smlouva ústní, s ohledem na případné pozdější prokazování jejího obsahu lze ovšem písemnou formu jedině doporučit. Dále se tedy k formuláři budu vyjadřovat jako ke smlouvě.

Je rovněž možné, pokud hodláme obdobná pravidla závazně uložit i zaměstnancům, vydat je formou vnitřního předpisu, např. jako součást pracovního řádu podle zákoníku práce. V takovém případě je třeba, aby byl vnitřní předpis podepsán statutárním orgánem společnosti a aby zaměstnanci byli s jeho vydáním či změnou seznámeni ve lhůtě 15 dní.[1]

Lze si představit, že společnost udělí třetí straně přístup bez uzavření jakékoli smlouvy, nicméně důvodů bezpečnostních i právních, proč takový přístup není moudrý, by se našlo mnoho. V zásadě si dovedu představit, že jediné omezeně životné použití takového řešení by mohlo být např. při udělení přístupu k návštěvnické wi-fi, a to pouze s výhradou, že i tak může vzniknout problém – někde (např. na sociálních sítích či v diskusích pod články na zpravodajských serverech) se objeví příspěvky se závadným obsahem a IP adresa povede právě do této společnosti, která přístup do návštěvnické wi-fi poskytla, což pro ni může představovat rizika právní i reputační.

Pokud ale uvažujeme v intencích postupů, které lze očekávat od společnosti, jež ke správě svých záležitostí přistupuje standardním[2] způsobem, pak se domnívám, že lze definovat jisté okruhy, které by měly být v rámci příslušné smlouvy ošetřeny.

Jak tazatel správně uvádí, třetí strana může získat přístup k infrastruktuře a datům. Tomu, co je zpřístupňováno, by pak měl být přizpůsoben obsah smlouvy. Jedná-li se o přístup k infrastruktuře, považuji za žádoucí definovat především podmínky a limity jejího využití ze strany třetí osoby:

- *Účel* – přístup je zpravidla povolován za určitým účelem, typicky kvůli plnění nějaké smlouvy, a na takové plnění by měl být omezen i přístup k infrastruktuře.
- *Limity* – zpravidla ani nebudeme chtít třetí straně zpřístupnit naši infrastrukturu neomezeně. Může se jednat o procesorový čas, šířku pásma, objem dat či místo

[1] V případě společností, u kterých působí odbory, se nám situace dále komplikuje tím, že vydání nebo změna musí být předem schválena odborovou organizací.
[2] Jakkoli používání termínu „standardní“ nemám rád, protože je na další dlouhou a výživnou diskusi, co to má vlastně znamenat.

na disku, případně další parametry. Kromě toho, že přijmeme odpovídající technická opatření, je dobré limity nastavit i smluvně.

- *Zakázaná užití* – pokud víme, co přesně nechceme, aby třetí strana dělala (a umíme to popsat), je dobré to výslovně uvést. Pokud tedy nechceme, aby si třetí strana na našem hardwaru např. řešila své soukromé projekty nebo si na náš síťový disk ukládala svá soukromá data, je vhodné to smluvně ošetřit. Obdobně sem bude patřit zákaz přistupovat na určité stránky či adresy, případně zákaz použít soukromé periferie či prostřednictvím vlastních zařízení přistupovat do naší sítě, mapovat, zaznamenávat a ovlivňovat náš síťový provoz, ukládat a šířit nelegální obsah apod.

- *Ochrana zájmů* – i když se budeme snažit sebevíc, asi nikdy se nám nepodaří postihnout výslovnými ujednáními vše, co chceme nebo nechceme. Je proto dobré zařadit rovněž obecné ustanovení o povinnosti třetí strany chránit naše zájmy a postupovat způsobem, který nebude v rozporu s našimi zájmy, které třetí strany byly nebo měly být známy.

- *Kontrola* – zpravidla je vhodné zařadit i ujednání, že jsme oprávněni přiměřeně kontrolovat, jakým způsobem třetí strana naši infrastrukturu používá. Inspiraci je možné čerpat např. z § 316 zákona č. 262/2006 Sb., zákoník práce (ZP), který upravuje možnosti zaměstnavatele přiměřeným způsobem kontrolovat využívání výpočetní techniky ze strany zaměstnanců. K uvedené problematice existuje hezká judikatura česká[3] i Evropského soudu pro lidská práva[4] se závěrem, že to spíše možné je.

[3] Např. Nejvyšší soud ČR, sp. zn. 21 Cdo 1771/2011, sp. zn. 21 Cdo 747/2013.
[4] Např. Rozsudek ESLP ve věci č. 61496/08.

Jedná-li se o přístup k datům, je dobré upravit zejména následující otázky:

- *Účel* – obdobně jako v případě přístupu k infrastruktuře, nyní však ve vztahu k využití dat. V praxi se zpravidla nerozlišuje.

- *Zakázaná užití* – obdobně jako v případě přístupu k infrastruktuře, nyní však ve vztahu k využití dat. V praxi se zpravidla nerozlišuje.

- *Ochrana zájmů* – obdobně jako v případě přístupu k infrastruktuře, nyní však ve vztahu k využití dat. V praxi se zpravidla nerozlišuje.

- *Obchodní tajemství* – ve smyslu zákonné definice obsažené v § 504 zákona č. 89/2012 Sb., občanský zákoník (OZ), se obchodním tajemstvím rozumějí veškeré konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních kruzích běžně nedostupné skutečnosti, které souvisejí s obchodním závodem a jejichž vlastník zajišťuje ve svém zájmu odpovídajícím způsobem jejich utajení. Je tedy vhodné uvést, které skutečnosti považujeme za své obchodní tajemství, a zavázat třetí stranu, že naše obchodní tajemství bude chránit.

- *Důvěrné informace* – jsou širší kategorií než obchodní tajemství, jedná se o veškeré informace, ohledně nichž si přejeme, aby třetí strana zachovávala mlčenlivost. Zřej-

mě všichni jsme se již setkali v nějaké formě s NDA (Non Disclosure Agreement), který v češtině překládáme jako dohodu o ochraně důvěrných informací. NDA zpravidla zahrnuje jak ochranu důvěrných informací v širším smyslu, tak ochranu obchodního tajemství.

- *Osobní údaje* – v rámci přístupu k datům se zřejmě třetí strana bude moci dostat i do kontaktu s osobními údaji. V závislosti na tom, v jakém rozsahu a jakým způsobem bude třetí strana přistupovat k osobním údajům, bude třeba ošetřit příslušné vztahy např. uzavřením dohody o zpracování osobních údajů nebo jiným vhodným způsobem.

- *Sdílení a kontrola* – obdobně jako v případě přístupu k infrastruktuře, nyní však ve vztahu k využití dat. V praxi se zpravidla nerozlišuje. Specificky ve vztahu k datům lze nicméně sjednat, že např. data vkládaná třetí stranou se okamžikem vložení stávají naším majetkem,[5] případně že okamžikem vložení na naši infrastrukturu k nim máme plný přístup, nebo co se stane s voženými daty, pokud následně třetí straně odebereme přístup.

Z obecných ujednání bych dále doporučil upravit:

- *Odpovědnost za subdodavatele* – třetí strana odpovídá za subdodavatele tak, jako kdyby přístup využívala sama (nevíme, zda bude činnosti pro nás provádět svými zaměstnanci nebo dalšími externími dodavateli – zde pozor, i „IČaři" jsou z pohledu práva subdodavatelem, nikoli zaměstnancem, i když často fungují v rámci společnosti téměř nerozeznatelně od zaměstnanců) a sjedná závazek třetí strany zavázat své zaměstnance a subdodavatele k dodržování povinností vyplývajících ze smlouvy v maximálním možném rozsahu.

- *Pojištění, záruky* – dále se nabízí zvážit možnost, zda budeme po třetí straně požadovat pojištění, v jaké výši a zda budeme požadovat vinkulaci pojistného plnění v náš prospěch, případně zda budeme požadovat bankovní záruku za splnění závazků vyplývajících ze smlouvy.

- *Odškodnění* – budeme-li vidět jako ne zcela zanedbatelné riziko, že by při činnosti třetí strany mohlo dojít k poškození práv třetích osob, typicky v souvislosti se zpracováním osobních údajů nebo porušením práv duševního vlastnictví, vyplatí se sjednat slib odškodnění (tzv. hold harmless klauzule) – v případě porušení práv dalších osob třetí strana převezme odpovědnost za škody způsobené svou činností a odškodní nás.

- *Naše zpracování osobních údajů třetí strany* – dále bych doporučil upravit naši možnost zpracovávat osobní údaje třetí strany (zde bych to hodnotil jako náš oprávněný zájem, přičemž třetí stranu přiměřeně informujeme o účelu a rozsahu zpracování).[6]

- *Smluvní pokuty* – v neposlední řadě – a s ohledem na tazatelův zájem dozvědět se, jak je to s vymahatelností – bych věnoval pozornost smluvním pokutám za porušení jednotlivých ujednání. Výhodou smluvní pokuty je, že není potřeba prokazovat vznik škody, pouze porušení takto utvrzené povinnosti. Smluvní pokuta by měla být přiměřená, nicméně pokud nebude, až tak moc nás to trápit nemusí, protože soud má možnost moderace (snížení). Riziko, že bychom kvůli „přepálení" výše přišli o celou smluvní pokutu, je spíše nízké. Dále můžeme zvážit, zda chceme celou smluvní pokutu vedle náhrady škody, případně jen smluvní pokutu nebo náhradu škody nad rámec smluvní pokuty. Je rovněž na zvážení, zda chceme případný spor řešit před soudy nebo rozhodci.

Řada výše uvedených ujednání samozřejmě může být součástí jiných ujednání, např. samotné smlouvy o dílo, případně smlouvy o spolupráci nebo jiné obdobné smlouvy, která se k danému projektu vztahuje.

Kdo by to měl podepsat, to je poslední věc, na kterou se tazatel ptá. Obecně platí, že jakákoli právní jednání může učinit statutární orgán. Je-li příslušná smlouva podepsána statutárem naší společnosti, je vše v naprostém pořádku. S ohledem na pracovní pozici a typickou agendu bych se asi nebál, pokud by za společnost takový dokument podepsal např. vedoucí IT, případně i běžný IT. Zřejmě se bude jednat o dokument, který byl předem připraven a odsouhlasen vedením.

Za třetí stranu by měl podepisovat rovněž statutárním orgán (ideálně) nebo osoba, u níž lze s ohledem na její postavení (ředitel, vedoucí) předpokládat, že je oprávněna v daném rozsahu třetí osobu zavazovat. Problematický by zřejmě mohl být podpis výkonného technika na místě, pokud bychom z něj následně chtěli dovozovat odpovědnost třetí strany jako celé společnosti.

Pokud jste tou třetí stranou, která formulář podepisuje, měli byste si z tohoto příspěvku odnést informaci, že pokud takový formulář podepíšete, velmi pravděpodobně uzavíráte platnou smlouvu, ze které pro vás plynou práva a povinnosti včetně možného postihu v případě jejich porušení. Rozhodně byste si tedy to, co podepisujete, měli alespoň přečíst (to ovšem platí naprosto obecně vždy).

[5] Předmětné ujednání může být v závislosti např. na možné povaze vkládaných dat jako autorského díla formulované i jinak, např. jako udělení licence k jejich užití.
[6] Jinými slovy následujeme čl. 13 GDPR.