2. 11. 2022

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Cloudy a právo 5: Kybernetická bezpečnost

Blížíme se ke konci našeho seriálu článků o právních aspektech využití cloudu. Již jsme se zabývali obecnou odpovědností organizace, která hodlá cloud využívat, popisem relevantních právních oblastí, typickými právními požadavky na poskytovatele cloudu i specifiky pro využití cloudu ve finančním sektoru.

V následujícím článku projdeme souvislosti a dopady právní úpravy kybernetické bezpečnosti, opět při využití cloudu. Tématem se budeme zabývat z pohledu klienta, který cloudové řešení využívá, i z pohledu jeho poskytovatele. Projdeme jak obecnou regulaci kybernetické bezpečnosti, tak specifika pro využití cloudu ve veřejné sféře. Na popisu ostatních aspekty, např. odpovědnost za zpracování osobních údajů, obecná soukromoprávní odpovědnost atd., jak jsme ji pojednali v předchozích článcích, se v tomto kontextu nic nemění.

Kybernetická bezpečnost při využití cloudu

V předchozích článcích jsme již upozorňovali, že při využití cloudu je nutné myslet mj. na ochranu informací, které budou v cloudu uloženy či které budou zpracovávány s využitím cloudových služeb. Osobní údaje, klientská data, obchodní tajemství, autorská díla.

Proč se tedy samostatně zabývat regulací kybernetické bezpečnosti?

Důvod je jednoduchý: Předmětem a důvodem právní úpravy kybernetické bezpečnosti je něco více než „pouhá“ ochrana dat. Smyslem této regulace je chránit informační systémy, informační technologie využívané pro poskytování důležitých služeb, a tím chránit bezpečnost státu. A právě z tohoto pohledu je nutné se dívat i na využití cloudových služeb, ať už se jedná o infrastrukturu nebo celou službu provozovanou někým jiným.

Pokud hodnotíme využití cloudu právě takto, a když přihlédneme k jasnému trendu zvyšujícího se využívání cloudových služeb, vzrůstajícího významu informačních technologií i počtu hrozeb, závažnost tématu kybernetické bezpečnosti je zjevná.

Koho zákon o kybernetické bezpečnosti týká?

Na prvém místě je vhodné vymezit, komu zákon o kybernetické bezpečnosti ukládá práva a povinnosti. A zde hned zdůrazněme rozdíl oproti úpravě v obecném nařízení o ochraně osobních údajů (GDPR) nebo finanční regulaci, které jsme diskutovali v předchozích článcích. Regulace kybernetické bezpečnosti totiž ukládá řadu povinností jak těm subjektům, které spravují z různých důvodů kritické či významné informační systémy, tak i přímo jejich dodavatelům, kteří se podílí na provozu těchto systémů. Včetně dodavatelů cloudových služeb, bez ohledu druh či kategorii cloudu (SaaS, IaaS atd.).

Zákon o kybernetické bezpečnosti totiž odlišuje činnost a odpovědnost **správce** a **provozovatele** informačního systému. Správcem je ten, kdo určuje účel zpracování informací a podmínky provozování informačního systému[1], provozovatel potom ten subjekt, který zajišťujíce funkčnost

technických a programových prostředků tvořících informační nebo komunikační systém[2]. V praxi může být správcem i provozovatelem jedna osoba. Jedná se o situaci, kdy k zajištění fungování informačního nebo komunikačního systému žádného dodavatele nevyužívá. Ale pokud dodavatele využívá, tak je provozovatelem právě tento dodavatel.

Jinak řečeno, pokud provozovatel cloudu své produkty poskytuje organizaci, která je správcem informačního systému ve smyslu zákona o kybernetické bezpečnosti, pak je i on přímo v režimu tohoto zákona. To platí i v případě, kdy toto není promítnuto do smlouvy se správcem informačního systému. Zákon o kybernetické bezpečnosti mu totiž ukládá řadu povinností a jejich nedodržování může být rovněž sankcionováno.

Správce informačního systému a cloudu

Zákon o kybernetické bezpečnosti vymezuje kategorie osob a organizací, které provozují kritické či významné informační systémy. A kterým je proto uložena povinna komplexně řídit kybernetickou bezpečnost.

Jsou jimi jak orgány státu, které provozují informační systémy, jejichž narušení může narušit nebo významně omezit výkon veřejné moci, subjekty provozující informační a komunikační systémy, ale i soukromoprávní společnosti, které jsou z pohledu své velikosti a pokrytí trhu významné pro poskytování některých ze zákonem vymezených základních služeb.[3] Těmito základními službami jsou např. energetika, doprava, ale i bankovnictví či infrastruktura finančních trhů a některé další.[4]

Konkrétní náležitosti systému pro zajištění kybernetické bezpečnosti, který musí výše uvedené subjekty zavést, jsou pak specifikovány v tzv. kybernetické vyhlášce[5].

Konkrétní požadavky při využití cloudu

Objednatel, který je povinným subjektem ve smyslu zákona o kybernetické bezpečnosti[6], se využitím dodavatele nezbavuje své odpovědnosti. Ani soukromoprávní, vůči klientů, odběratelům, zaměstnancům či dalším osobám, ani té veřejnoprávní. Pokud je tedy povinen přijmout opatření k ochrany jím provozovaných nebo využívaných informačních systémů, platí to i tehdy, pokud je v plném rozsahu neprovozuje sám, ale využívá je jako cloudovou službu.

Z pohledu zákona o kybernetické bezpečnosti to má dva důsledky: Za prvé, veškeré povinnosti, které na povinný subjekt dopadají, se uplatní i při využití cloudu. I při využití cloudového řešení tak povinná osoba musí zavést veškeré technická a organizační opatření pro ochranu svého informačního systému. Jejich detailní výčet či popis by přesáhl možnosti tohoto článku, proto pro příklad uveďme jen některé z nich: Zavedení systému (procesu) řízení kybernetické bezpečnosti včetně řízení informačních aktiv a souvisejících rizik, nastavení a popis pravidel v interní dokumentaci, rozdělení odpovědnosti za jednotlivé části systému, zajištění personální bezpečnosti, nastavení procesu pro zvládání kybernetických bezpečnostních incidentů, a rovněž řada konkrétních technických požadavků.[7]

Postupům a procesům pro řízení kybernetické bezpečnosti je nutno podrobit celý informační systém. V opačném případě, pokud by povinná osoba u částí informačního systému poskytované dodavatelem cloudu kybernetickou bezpečnost v plném rozsahu neřešila, by mohlo dojít k narušení celkového systému kybernetické bezpečnosti. Z pohledu práva pak k nedostatečné plnění požadavků regulace s rizikem uložení sankce či nápravného opatření ze strany Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) a s větším rizikem povinnosti nahradit škodu, která by v důsledku nesouladu s právními požadavky mohla vzniknout.

Regulace v oblasti kybernetické bezpečnosti však na objednatele cloudu, resp. některé povinné

osoby, která pro jakoukoliv část regulovaného informačního systému využívá dodavatele, klade i další, dodatečné povinnosti. Jedná se v prvé řadě o povinnost nastavit bezpečnostní opatření tak, aby pokrývala i rizika spojená s využitím dodavatele, vybrat dodavatele, který bude těmto požadavkům odpovídat, a zanést požadavky v nezbytném rozsahu i do smlouvy.

Druhým aspektem je požadavek na nastavení procesu pro řízení dodavatelů, jak je upraven v § 5 odst. 2 písm. e) zákona o kybernetické bezpečnosti, resp. v § 8 kybernetické vyhlášky. Tyto požadavky, které zahrnují především nastavení pravidel pro výběr a využití dodavatelů, jejich ověření, řízení souvisejících rizik, evidenci dodavatelů a požadavků na smlouvu[8], je nutno v plném rozsahu aplikovat i na dodavatele cloudových řešení.

Zákonné povinnosti poskytovatele cloudu

Poskytovatel cloudových řešení, mezi jehož zákazníky je správce informačního systému v režimu zákona o kybernetické bezpečnosti, je rovněž předmětem této regulace. Zákon o kybernetické bezpečnosti a kybernetická vyhláška mu přímo ukládají řadu povinností.

Je pravdou, že v GDPR, případně regulaci poskytování některých finančních produktů, můžeme nalézt některé povinnosti, které jsou dodavatelům (zpracovatelům osobních údajů, resp. poskytovatelům outsourcingu) ukládány přímo. Jedná se ale spíše o dílčí prvky či body, které jsou navíc vymezeny poměrně obecně. Zákon o kybernetické bezpečnosti však provozovatelům relevantních informačních systémů ukládá v zásadě stejné povinnosti, jako jejich správcům, samozřejmě s tím, že aplikace konkrétních organizačních a technických opatření musí odpovídat podmínkám daného provozovatele, jeho specifikům, rizikům, kterým čelí atd.

Poskytovatel cloudového řešení, který své služby nabízí správci informačního systému v režimu zákona o kybernetické bezpečnosti, tak rovněž musí nastavit celkový systém (proces) pro řízení kybernetické bezpečnosti, zřídit příslušné funkce či výbory, řídit kybernetické bezpečnostní incidenty, nastavit pravidla pro zajištění kontinuity poskytovaných činností (business continuity management), zavést odpovídající technická bezpečnostní opatření atd.

Takovýto poskytovatel cloudových řešení musí být rovněž schopen zavedená opatření doložit, jak svému klientovi, správci informačního systému, tak při kontrole NÚKIB. A k dodržování těchto opatření je také povinen se zavázat smluvně.

Směrnice NIS2 a cloud: větší záběr, vyšší pokuty

Regulaci kybernetické bezpečnosti čeká poměrně výrazná změna. Na úrovni Evropské unie byla dohodnuta revize, resp. přijetí nové směrnice, která tuto oblast upravuje, tzn. NIS2. Ta by měla být do českého práva transponována zhruba do poloviny roku 2024.

Jaké změny NIS2 přinese z pohledu našeho tématu, právních aspektů cloudových řešení?

Ačkoliv konečný text NIS2 zatím nebyl publikován[9], z posledního dostupného znění lze dovodit, že zásadně nové požadavky na povinné osoby při řízení dodavatelů, provozovatelů informačních systémů, ani při provozování těchto systémů klást nebude. Česká kybernetická vyhláška je již dnes poměrně detailní a odráží mezinárodní standardy a případy dobré praxe v oblasti řízení informační bezpečnosti. Vše výše uvedené, povinnost nastavit systém kybernetické bezpečnosti, určit odpovědnosti a role, řídit incidenty, řídit dodavatele, zavést technická opatření atd., zůstane v platnosti i nadále.

Poměrně zásadní změnou ale bude výrazně vyšší okruh povinných subjektů. Dnešní zákon o kybernetické bezpečnosti se týká zhruba 600 organizací. NÚKIB odhaduje, že po transpozici NIS2,

se jejich počet řádově zvýší na cca 6.000.[10] Povinnost komplexně řešit kybernetickou bezpečnost tak dopadne na mnoho dalších organizací, ať již v postavení správce informačního důležitého informačního systému, nebo v postavení jeho dodavatele, provozovatele systému.

NIS2 také zavede výrazně vyšší pokuty za nedostatky při řízení kybernetické bezpečnosti. Zatímco podle dnešního českého zákona o kybernetické bezpečnosti lze uložit pokutu nejvýše 5 milionů korun, a to v některých případech i přímo provozovateli informačního systému, NIS2 tuto hranici zvyšuje. Za ty nejzávažnější prohřešky by členské státy měly stanovit sankce do výše 10 milionů euro nebo 2 % z celosvětového obratu skupiny, do které daná organizace patří.

Cloudy ve veřejné správě: legislativní základ

Maje na vědomí vše výše uvedené ke kybernetické bezpečnosti, přejděme na veřejnou správu. Jedná se o oblast, kde je v posledních letech snaha digitalizovat své procesy i za využití dodavatelů ze soukromé sféry.

Česko dle zprávy Indexu digitální ekonomiky a společnosti Digital Economy and Society Index (DESI) zlepšilo svou pozici v oblasti digitálních veřejných služeb a postoupilo z 20. místa v roce 2021 na 17. místo v roce 2022. V roce 2021 přitom podíl uživatelů elektronické veřejné správy výrazně vzrostl, a to o 12 procentních bodů na 76 %.[11] I pozice designovaného místopředsedy vlády pro digitalizaci vypovídá nové vlády o záměru dále prohlubovat digitální fungování veřejné správy.

Pro ujasnění pravidel pro automatizované zpracování informací byl již v roce 2000 přijat zákon o informačních systémech veřejné správy (ZISVS). Ten založil pojem informačních systémů, jež zahrnují *„data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, a dále nástroje umožňující výkon informačních činností*". Pro vznik možnosti využívat cloudy ve veřejné správě je však klíčová tzv. digitální ústava, tedy zákon č. 12/2020 Sb., o právu na digitální služby. Ten do ZISVS přinesl definici cloud computingu. Cloud computing je definován jako *„způsob zajištění provozu informačních systémů veřejné správy nebo jejich části prostřednictvím dálkového přístupu ke sdíleným technickým či programovým prostředkům*". O cloud dle zákona se tedy jedná pouze tehdy, pokud je využit pro systémy veřejné správy – v ostatních případech jde o činnost ZISVS neregulovanou.

Vedle této definice digitální ústava tedy přinesla i možnosti využívání soukromých cloudů veřejnou správou, jakož i katalog jejich služeb. Jeho prostřednictvím může docházet k nabízení ověřených soukromých cloudových řešení a jejich následnému využití ve státní správě.

Katalogy poskytovatelů, poptávek a nabídek cloudových řešení

Katalog cloudů jakožto centrální bod celého využívání soukromých cloudových řešení ve veřejné správě obsahuje seznam nabídek ze strany soukromých dodavatelů, seznam poptávek ze strany veřejné správy (bohužel i nyní, v době psaní tohoto článku, v zásadě prázdný) a samotný seznam dodavatelů. Zápis do katalogu poskytovatelů (dodavatelů) je přitom klíčem pro možnost nabízet v budoucnu své (jiné než na nejnižší bezpečnostní úrovni) cloudové řešení státu.

Zápis probíhá na základě vyplněného a zaslaného excelu Ministerstvu vnitra spolu s nutnými přílohami, kterými dodavatel dokazuje, že je a) bezúhonný, b) způsobilý zajistit základní úroveň bezpečnosti informací, c) způsobilý řádně poskytovat cloud z hlediska veřejného pořádku, bezpečnosti a dodržování práv třetích osob. Součástí přihlášky jsou i reference za posledních 5 let. Ministerstvo vnitra má následně 45 dní na správní uvážení, zda dodavatele zapsat do katalogu: absence odpovídajících referencí přitom sama o sobě není důvodem k zamítnutí žádosti. Tato lhůta se navíc může prodloužit až o 3 měsíce, po které NÚKIB ověřuje naplnění požadavků ZISVS na

poskytovatele, tedy reálně může zápis trvat okolo 5 měsíců. Určitě proto doporučujeme podat přihlášku co nejdříve. Jinak poskytovateli hrozí, že se nebude moci účastnit nových zakázek na přesmluvnění všech cloudů do konce roku 2023 (k tomuto podrobněji níže).

Po úspěšném zapsání do seznamu dodavatelů může daný poskytovatel začít zapisovat do katalogu nabídek nabízené služby. Tyto zápisy vyřizuje ministerstvo během dalších 30 dní, přičemž si v některých případech musí vyžádat závazné stanovisko NÚKIB, které NÚKIB vydá do 30 dnů od podání žádosti. Dodavatel při něm dokládá seznam svých dodavatelů včetně informace, jak budou zpracovávat informace od veřejné správy, dokumentaci cloudu a následně požadavky dle vyhlášky č. 316/2021 Sb.

Vyhlášky stanovující bezpečnostní jádro pro dodávání cloudů

Katalyzátorem spící úpravy se stal ale až zákon č. 261/2021 Sb., který novelizoval zákony v souvislosti s další elektronizací postupů orgánů veřejné moci. Na základě tohoto zákona, známého též pod zkratkou DEPO, byly přijaty klíčové vyhlášky č. 315/2021 Sb. a 316/2021 Sb. DEPO také určilo 1. ledna 2024 jako datum, od kterého přestanou platit veškerá přechodná ustanovení a cloud ve veřejné správě se bude řídit zákonem v plném rozsahu. Pokud bylo využívání cloud computingu zahájeno před 1. 9. 2021, lze cloud computing, který nesplňuje požadavky ZISVS nebo je poskytován provozovatelem nezapsaným v katalogu, užívat do konce roku 2023. Pokud ale bylo užívání zahájeno později, lze takový cloud computing užívat jen do konce roku 2022.

Pro veřejnou správu je samozřejmě klíčové, aby dodavatel byl schopen zajistit odpovídající úroveň ochrany důvěrnosti, integrity a dostupnosti informací, které pro ni bude zpracovávat. Tato úroveň je nastavena dle vyhlášky č. 315/2021 Sb. ve čtyřech různých stupních: nízkém (1), středním (2), vysokém (3) a kritickém (4). Pro nejvyšší, kritický, stupeň platí, že nemůže být poskytován dodavatelem ze soukromého sektoru.

Pro každý z těchto stupňů představuje vyhláška č. 316/2021 Sb. ve svých přílohách požadavky, které musí dodavatel naplnit, aby se mohl zařadit do katalogu mezi poskytovatele v dané bezpečnostní úrovni a aby mohl dávat nabídky na poptávané cloudy. V tomto směru má zadavatel ze strany veřejné správy, který chce outsourcovat cloud, povinnost vyžadovat některé doklady, resp. ověřit, zda dodavatel splňuje požadavky pro danou bezpečnostní úroveň, a dodavatel má povinnost je doložit.

Na tomto místě se setkává úprava bezpečnostních požadavků stanovená vyhláškami s požadavkem na veřejnou správu, aby při využívání cloudů dodržovala požadavky kybernetické bezpečnosti. Oba tyto požadavky se obsahově prolínají, ale získávají obsah pro svou činnost z jiných předpisů.[12]

Veřejná správa tedy musí zajistit, aby dodavatel cloudu zavedl účinná bezpečnostní opatření a poskytoval o nich informace, informovat o bezpečnostních incidentech či podávat informace vyžádané orgány činnými v trestném řízení. Dodavatel zase musí sídlit v některém členském státě EU nebo zde mít alespoň zástupce ve smyslu čl. 27 obecného nařízení o ochraně osobních údajů (GDPR) a nesměl v posledních 5 letech být sankcionován za porušení ZKB. To vše pro dosažení nízké bezpečnostní úrovně.

Vyšší bezpečnostní třídy: certifikace a audity

To podstatné se ale děje v oblasti certifikací a auditů, které musí dodavatel získat a absolvovat, aby mohl dodávat (obvykle obchodně zajímavější) cloudová řešení ve vyšších bezpečnostních úrovních. Základním požadavkem pro střední bezpečnostní třídu je mít certifikát ČSN ISO/IEC 27001, přičemž certifikát se musí vztahovat na nabízené služby cloud computingu bez omezení, a pozor – musí z něj být patrné splnění celé řady požadavků (takže starší certifikát nemusí být samospásný). Datum

poslední revize na certifikátu nesmí být starší 15 měsíců (12 měsíců výročí plus 3 měsíce na dokončení auditních procesů).

Vedle samotného certifikátu musí orgán veřejné správy po dodavateli žádat doložení auditní zprávy a prohlášení o aplikovatelnosti k tomuto certifikátu, z které také musí být patrné splnění řady požadavků. Pro srovnání, na nízkou úroveň stačí dodavateli deklarovat minimální bezpečnostní opatření v kapitolách A7, A9, A12, A13, A15, A16 a A18 dle této normy. Totožná povinnost platí pro certifikáty ČSN ISO/IEC 27017 a ČSN ISO/IEC 27018, ty však mohou být součástí rozšířením výše uvedeného certifikátu.

Pro nejvyšší úroveň se pak začíná objevovat povinnost doložit Auditní zprávu SSAE18 SOC 2 Type II v doménách Security, Availability, Processing Integrity, Confidentiality, Privacy (z níž opět bude patrné splnění řady požadavků) či doložit nanejvýš tři roky starou zprávu o provedených penetračních testech, která se liší dle distribučního modelu cloudu, který má být dodáván.

Ačkoliv výše uvedené certifikace a auditní zprávy obsáhnou většinu požadavků dle tohoto odstavce, zmiňme si ještě jeden, velmi důležitý prvek pro dodávání cloudu veřejné správě, a to povinnosti týkající se datových center. Bez ohledu na bezpečnostní úroveň, datová centra, resp. údaje dotčených osob, mají být umístěna na území EU. Pokud mohou nastat případy zpracování zákaznických dat mimo EU, dodavatel má povinnost tuto informaci sdělit spolu se způsobem zajištění jejich bezpečnosti. Pro střední úroveň musí mít dodavatel připravena primární i záložní datacentra, která jsou alespoň 50 km od sebe: pro nejvyšší jsou pak buď obě v ČR nebo v různých státech EU a současně umožňují synchronní replikaci dat alespoň do jednoho (jiného) záložního datového centra, které je z hlediska kapacity a zajištěné konektivity dostatečné k převzetí všech služeb, poskytovaných z primárního datového centra.

Jak na zápis do katalogu dodavatelů a nabídek?

A jak se k přípravě na zápis nabídky postavit v praxi a neztratit se v nepřehledné změti technických požadavků, které často platí alternativně (tzn. stačí splnit jeden z nich)? Autorům se osvědčilo připravit si přehledný soubor (checklist) se všemi požadavky pro poskytovaný cloud a požadovanou bezpečnostní úroveň. Ideální je také požadavky zpracovat tak, aby se v případě splnění některého z alternativních požadavků ostatní označily jako splněné, resp. aby se v případě všech požadavků v daném ID požadavku označilo celé ID jako splněné. I když příprava takového dokumentu určitý čas zabere, můžete s ním rychle analyzovat výchozí připravenost (abyste věděli, co již máte splněno od počátku), namodelovat si nejvhodnější cestu ke splnění požadavků, a také si finálně ověřit, co již máte splněno. I když příprava takového dokumentu určitý čas zabere, v procesu přípravy na certifikaci ušetří spoustu času a minimalizuje chyby.

Závěr

Na rozmach cloudových řešení, jejich stále širší využívání a současně vzrůstající počet kybernetických útoků, reaguje i stát, který pro ochranu svého fungování přijal celou řadu výše popsaných požadavků. Byť splnění těchto požadavků není jednoduché, v řadě případů jej můžeme naopak označit za složité, věří autoři, že užití cloudových řešení a obecně outsourcing provozu IT systémů na specializované poskytovatele je správnou a efektivní cestou výkonu řady agend soukromých i veřejných subjektů.

Mgr. Bohuslav Lichnovský, LL. M.,
působící v Bohuslav Lichnovský GALI LEGAL, advokátní kancelář
e-mail: lichnovsky@galilegal.com

Mgr. František Nonnemann,
konzultant v oblasti ochrany osobních údajů a compliance, člen Výboru Spolku pro ochranu osobních údajů
e-mail: nonnemann@volny.cz

---

[*] **Cloudy a právo - 1 díl: Proč o nich uvažovat a na co se připravit**, dostupné na www, k dispozici >>> zde.
[**] **Cloudy a právo - 2 díl: Tisíc a jeden právní požadavek**, dostupné na www, k dispozici >>> zde.
[***] **Cloudy a právo - 3 díl: Povinnosti finančních institucí**, dostupné na www, k dispozici >>> zde.
[****] **Cloudy a právo - 4 díl: Jak se má připravit poskytovatel cloudu?**, dostupné na www, k dispozici >>> zde.

---

[1] Viz § 2 písm. e) zákona č. 181/2014 Sb.

[2] Viz § 2 písm. g) zákona č. 181/2014 Sb.

[3] Srov. § 3 zákona o kybernetické bezpečnosti.

[4] Konečný výčet je uveden v § 2 písm. i) zákona o kybernetické bezpečnosti.

[5] Resp. celým názvem 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).

[6] Jejich výčet je uveden v § 3 zákona o kybernetické bezpečnosti.

[7] Srov. § 5 zákona o kybernetické bezpečnosti, resp. vyhlášku č. 82/2018 Sb.

[8] Viz příloha č. 7 k vyhlášce č. 82/2018 Sb.

[9] Poslední dostupná verze je zveřejněna na stránkách NÚKIB zaměřených právě na osvětu k tématu nové regulace, k dispozici >>> zde.

[10] Srov. k dispozici >>> zde.

[11] Srov. k dispozici >>> zde.

[12] Požadavek na veřejnou správu dodržovat vyhlášku č. 82/2018 Sb. vychází z § 5b odst. 2 ZISVS, požadavky na odpovídající bezpečnostní úroveň a dodržování vyhlášky č. 316/2021 Sb. vychází (zjednodušeně) z požadavků dle § 6n a násl. ZISVS.

Další články:

- „Za každou kauzou je živý příběh“
- Ombudsman na Maltě – základní parametry a role. A v čem bychom se mohli poučit i my v Česku?
- DEAL MONITOR
- DEAL MONITOR
- Rozhovor s JUDr. Veronikou Janoušek Rudolfovou, samostatnou advokátkou specializující se na sportovní právo
- DEAL MONITOR
- DEAL MONITOR
- DEAL MONITOR
- Fotbaloví agenti vs. FIFA ve světle stanoviska generálního advokáta Soudního dvora Evropské unie
- Lichevní smlouva ve světle usnesení Nejvyššího soudu ze dne 3. 6. 2025, sp. zn. 28 Cdo 2378/2024
- DEAL MONITOR