3. 11. 2016

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

Nová regulace ochrany osobních údajů aneb na jaké změny se připravit

Obecné nařízení o ochraně osobních údajů[1] bylo v Úředním věstníku EU zveřejněno začátkem května tohoto roku a správci osobních údajů tak mají necelé dva roky na to, aby zajistili soulad prováděných zpracování osobních údajů s novou regulací. Jaké základní změny nařízení přinese, kterým institutům je potřeba věnovat zvýšenou pozornost a jak se na nové povinnosti připravit, se alespoň ve stručnosti pokusíme nastínit v následujících řádcích.[2]

I přesto, že základní principy ochrany osobních údajů zůstávají zachovány, dochází v této oblasti k řadě zásadních změn. Vzhledem k tomu, že právní úprava platná od roku 1995 již přestala vyhovovat současnému stavu moderní globalizované společnosti, rychlému vývoji technologií a digitálního trhu, regulátoři působící v oblasti ochrany údajů přistoupili k úpravám současných práv a povinností a po téměř čtyřech letech navrhování a vyjednávání je k dispozici finální text. Řada stávajících povinností byla podstatným způsobem modifikovaná nebo k nim přibyly povinnosti nové, jež primárně posilují práva subjektu údajů a jeho postavení vůči správcům. Všechny subjekty, ať již soukromoprávní či veřejnoprávní, v rámci jejichž činnosti dochází k nakládání s osobními údaji tak musí do dvou let přizpůsobit své interní politiky a procesy tak, aby vyhovovaly novým požadavkům na ochranu osobních údajů a eliminovaly nejen riziko výrazně vyšších sankcí, ale rovněž poškození své reputace v souvislosti s případným porušením zabezpečení osobních údajů. Jaké změny se nejvíce dotknou společností působících na finančním trhu v České republice? Jak se na nařízení připravit, a jaké kroky lze podniknout již dnes? S čím počítat do budoucna, a jaké prostředky si pro implementaci vyčlenit? To jsou otázky, na které se pokusíme níže odpovědět.

Jednotné uplatňování nařízení

Nařízení, které nahrazuje doposud platnou směrnici, která byla do právních řádů jednotlivých členských států transponovaná prostřednictvím národních zákonů o ochraně osobních údajů, svou přímo účinnou povahou zavádí jednotný režim pro všechny členské státy, přičemž transpozice do národních zákonů již v zásadě není potřeba. K jednotnému uplatňování tohoto nařízení v celé Unii, by měl rovněž přispět tzv. mechanismus jednotnosti, který nastavuje pravidla pro spolupráci mezi jednotlivými národními dozorovými úřady. I přesto, že se jedná o bezprostředně aplikovatelný předpis EU, nařízení členským státům u řady institutů umožňuje v rámci určitých mantinelů zachovat nebo zavést konkrétnější úpravu. Zda se tak skutečně stane, je zatím otázkou. V každém případě by významnou úlohu při jednotném uplatňování nařízení měl hrát nově vzniklý Sbor pro ochranu osobních údajů (nahrazuje současnou pracovní skupinu, tzv. WP 29), prostřednictvím vydávání pokynů, doporučení či osvědčených postupů.

Působnost nařízení

Nařízení bude nově dopadat i na správce a zpracovatele, kteří vůbec nejsou v EU usazeni. Postačovat bude, pokud se v EU nachází dotčený subjekt údajů a zpracování souvisí s nabídkou zboží či služeb (bez ohledu na to, zda je spojena s platbou) nebo s monitorováním chování subjektu údajů, v rozsahu v němž k tomuto chování dochází v EU. Pokud například bude možné v členském státě EU objednat službu přes internet v anglickém či německém jazyce a platbu bude možné realizovat v eurech, zpracování osobních údajů bude podléhat režimu nařízení. To samé bude platit, pokud budou

například americkou společností sledovány internetové činnosti fyzických osob nacházejících se v EU.

Zásady a základní pojmy

Co se týče základních zásad pro zpracování osobních údajů nebo již zaužívaných institutů či pojmů, tyto doznaly pouze minimálních změn. Zpracování musí být nadále prováděno korektně, zákonným a transparentním způsobem a pro účely, které jsou určité, výslovně vyjádřené a legitimní. Konkrétní účely by měly být stanoveny v okamžiku shromáždění osobních údajů a ke zpracování by mělo docházet pouze, pokud účelu nemůže být přiměřeně dosaženo jinými prostředky. Zpracovávat je možné pouze údaje přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k deklarovanému účelu. Je nutné dbát na přesnost údajů i dobu, po kterou jsou uloženy a v neposlední řadě na jejich zabezpečení, tedy integritu a důvěrnost. Správce musí celé zpracování provádět v souladu s těmito zásadami, přičemž za jejich zpracování nejen, že odpovídá, ale soulad musí být také schopen doložit – princip accountability.[3] Princip accountibility se stává novým principem ochrany osobních údajů explicitně v nařízení vyjádřený. Nařízení oproti současné směrnici tak zásadním způsobem rozšiřuje prostředky vedoucí k podněcování větší odpovědnosti správce, mezi které patří např. posouzení vlivu na ochranu osobních údajů, stanovení závazných politik v oblasti ochrany údajů (BCR), jmenování pověřence pro ochranu osobních údajů, vytváření etických kodexů, vnitřních mechanismů pro vyřizování stížností, zavedení vnitřních postupů pro zvládání porušení zabezpečení osobních údajů, záměrná a standardní ochrana.

Většina základních definic, jako správce, zpracovatel či subjekt údajů zůstává proti směrnici nezměněná. Co se rozumí osobním údajem či zpracováním osobních údajů zůstává v principu rovněž stejné jako doposud. Definice osobního údaje se sice dočkala určitého rozšíření či upřesnění, ale jedná se pouze o změny, jež vzhledem k výkladovým stanoviskům dozorových orgánů platí i dnes. Aby byly informace předmětem ochrany osobních údajů podle nařízení, musí se vztahovat k osobě identifikované nebo identifikovatelné, přičemž za určitých okolností, lze za osobní údaje považovat i síťové identifikátory jako například adresy internetového protokolu či cookies. Také osobní údaje, u kterých byla uplatněna pseudonymizace, budou podléhat režimu nařízení. Pseudonymizace se tak stala jedním z významných prostředků sloužící k zabezpečení údajů, podobně jako např. šifrování. Nařízení se nebude týkat pouze zcela anonymních údajů, tedy těch, které se nevztahují k identifikované či identifikovatelné osobě

Souhlas subjektu údajů či jiný právní základ pro zpracování

Souhlas se zpracováním osobních údajů byl již za současné právní úpravy problematickým institutem a lze předpokládat, že pro řadu správců osobních údajů jím zůstane také za účinnosti nové právní úpravy. Proti původnímu, značně strohému vymezení tohoto právního titulu, nařízení podstatně rozšiřuje zejména podmínky jeho vyjádření. Kromě toho, že souhlas musí být svobodný, konkrétní a informovaný, je v nařízení kladen důraz také na jeho jednoznačnost, tedy že by měl být dán jednoznačným potvrzením. Pokud je souhlas vyjádřen písemným prohlášením explicitně umožněným také v elektronické podobě, musí být jasně odlišitelný od jiných skutečnosti, jich se může týkat a ve smyslu zásady transparentnosti musí být srozumitelný a snadno přístupný za použití jasných a jednoduchých jazykových prostředků. V opačném případě takové prohlášení nebo jeho část není závazná. Správce takto získaný souhlas musí být schopen doložit. Nařízení výslovně umožňuje souhlas udělit například zaškrtnutím políčka při návštěvě internetové stránky, volbou technického nastavení služby informační společnosti nebo jiným prohlášením jasně symbolizujícím souhlas s navrhovaným zpracováním osobních údajů. Naopak mlčení či předem zaškrtnuta políčka za souhlas považovat nelze. Nařízení také nově stanoví právo subjektu údajů svůj souhlas kdykoliv odvolat, což musí být stejně snadné jako poskytnutí souhlasu a ještě před udělením souhlasu, musí být subjekt

údajů o tomto právu informován. Speciální podmínky jsou stanoveny, pokud se jedná o souhlas dítěte nebo zvláštní kategorie osobních údajů, dnes známé jako citlivé údaje.

Co se týče dalších legitimních a legálních základů neboli tzv. právních titulů, na základě kterých je možné rovněž osobní údaje zpracovávat, zůstává jejich původní koncept beze změn. V soukromém sektoru lze předpokládat, že zpracování bude možné bez souhlasu provádět především, pokud to bude nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu. Dále také pokud je zpracování nezbytné pro splnění právní povinnosti, která se na správce vztahuje a v neposlední řadě také pro účely oprávněných zájmů správce či třetí strany, za předpokladu, že před těmito zájmy nemají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů. U posledního zmíněného právního titulu je zvláštní zřetel kladen na případy, kde je subjektem údajů dítě, přičemž speciální přístup k ochraně osobních údajů dětí je vlastní celému nařízení a jedná se o jednu z hlavních změn proti původní úpravě.

Práva subjektů údajů

Nařízení výrazným způsobem posiluje práva fyzických osob – subjektů údajů, jimž mají změny umožnit lepší kontrolu nad jejich osobními údaji a usnadnit jim přístup k nim, a to bez ohledu na místo, kde se nacházejí. Nařízení má zajistit větší transparentnost tak, aby pro subjekty údajů byly dostupné informace o tom, jak jsou jejich osobní údaje shromažďovány, používány, konzultovány nebo jinak zpracovávány, jakož i to, v jakém rozsahu se tak děje. Kromě již zaužívaných práv, nařízení klade ještě větší důraz na to, aby každý subjekt údajů disponoval snadnějším přístupem k těmto informacím, a to ve stručné a srozumitelné podobě. Nad rámec toho je správci uložen úkol používat jasných a jednoduchých jazykových prostředků. V případě, kdy si fyzická osoba nepřeje, aby byly její osobní údaje dále zpracovávány, je nově výslovně zakotveno její právo „být zapomenut“, které je rozšířením dosavadního práva na výmaz o povinnost správce, jenž osobní údaje zveřejnil, informovat další správce, kteří tyto údaje zpracovávají, aby vymazali veškeré odkazy na dané osobní údaje či jejich kopie nebo replikace. Plnění této povinnosti bude v praxi pro správce jistě poměrně složitou a nákladnou operací, která z povahy věci nemůže být nikdy beze zbytku naplněna. Nicméně je nutné upozornit, že institut práva být zapomenut není zcela nový, ale do praxe se již dostal v návaznosti na rozhodnutí Evropského soudního dvora EU z května 2014 ve věci sporu mezi Googlem a M. C. Gonzálesem.[4] Nařízení nově explicitně stanoví také právo na přenositelnost údajů, jež má zajistit snadnější možnost převádění osobních údajů mezi různými poskytovateli služeb. Opomenout nelze ani právo subjektu údajů být informován o neoprávněném přístupu ke svým údajům. Z podstatně podrobnějšího textu nařízení tak lze dovodit, že rozšíření práv subjektu údajů se odrazí v nárůstu korespondujících povinností správců, kteří budou muset plnění těchto práv náležitě zajistit a v souladu s principem accountability to také doložit.

Povinnosti správců

Kromě povinností souvisejících se zajištěním výkonu práv subjektů údajů, stanoví nařízení řadu dalších povinností přímo správcům či zpracovatelům osobních údajů. Jedním z nejvíce diskutovaných institutů v rámci vypracovávání nařízení byl institut pověřence pro ochranu osobních údajů. Jedná se o osobu, která pro správce zajišťuje, aby jeho činnosti byly v souladu se všemi požadavky v oblasti ochrany osobních údajů, a vykonává s tím související úkoly. Správce musí pro pověřence zajistit, aby mohl svou funkci vykonávat řádně a nezávisle, byl zapojen do veškerých záležitosti souvisejících s ochranou osobních údajů a měl dostatečné zdroje k plnění svých úkolů. Pověřence pro ochranu osobních údajů sice nemusí jmenovat každý správce, ale řada z nich se této povinnosti nevyhne (ve většině případů se bude jednat o zpracování zvláštních kategorii osobních údajů, případně osobních údajů velkého rozsahu i velkého počtu subjektů údajů). Nařízení ovšem neřeší procedurální

záležitosti institutu pověřenců. Proto stále zůstávají otevřené některé otázky týkající se např. stanovení kritérií pro jmenování pověřenců, určení role dozorového orgánu, který by pravděpodobně měl vést evidenci pověřenců, případně i veřejně přístupnou, dále otázka jejich jmenování a přezkušování, zda mají v oblasti ochrany osobních údajů dostatečné odborné znalosti apod. Konečná podoba institutu pověřenců včetně vymezení role Úřadu pro ochranu osobních údajů tak bude muset být pravděpodobně ještě nějakým způsobem konkretizována.

Další povinností, kterou bude muset podle nařízení plnit většina správců je vedení záznamů o činnostech zpracování. Tyto záznamy budou muset obsahovat nařízením předepsané náležitosti a nebudou je muset plnit pouze správci, kteří zaměstnávají méně než 250 osob a splňují další předpoklady pro vyjmutí z této povinnosti. Výjimka z této povinnosti je fakticky omezena pouze na taková zpracování, která nelze kvalifikovat jako riziková, resp. nezasahující závažným způsobem do práv a svobod jednotlivců. Limitem je zde rizikovost zpracování, které se ovšem neomezuje pouze na zpracování citlivých údajů ale má širší rozsah např. na údaje velkého objemu či údaje velkého počtu subjektů údajů, dále údaje, jejichž zneužití může mít za následek způsobení fyzické újmy, krádež identity nebo údaje, jejichž zneužití může způsobit hmotnou či nehmotnou újmu subjektu údajů.

Jak z výše uvedeného vyplývá, bude nově správce vést dokumentaci, jejímž obsahem bude v zásadě podobné penzum informací, které je v současné době správce povinen sdělovat dozorovému orgánu v rámci oznamovací povinnosti, a které dozorový orgán následně zapisuje do veřejného registru zpracování. Na rozdíl od současné právní úpravy nebude již povinností správců dokumentaci obsahující informace o zpracování zasílat dozorovým orgánům za účelem jejich registrace, nicméně správci budou povinni záznamy o zpracování dozorovému orgánu na jeho žádost zpřístupnit.

U tzv. vysoce rizikových zpracování uvedených v seznamu zveřejněném dozorovým úřadem bude také nutné provádět posouzení vlivu na ochranu osobních údajů. Nařízení uvádí demonstrativní situací, kdy posouzení vlivu bude s největší pravděpodobností nutné provést, resp. kdy zpracování může představovat vysoké riziko, jako například zpracování, které by mohlo vést k fyzické, hmotné nebo nehmotné újmě (např. k diskriminaci, krádeži identity, finanční ztrátě, poškození pověsti atd.), rozsáhlé operace zpracování (např. zpracování velkého množství osobních údajů jednotlivců či zaměstnanců zpracovávajících osobní údaje), zpracování zcela nového druhu nebo zpracování, při nichž jsou používány nové technologie či rozsáhlé zpracování zvláštních kategorií údajů. Na základě výše uvedeného obecného výčtu zpracovatelských operací (konkrétní výčet rizikových i vysoce rizikových zpracování bude ještě upraven dozorovými úřady ve spolupráci se Sborem pro ochranu osobních údajů), lze usuzovat, že povinnost provádět posouzení vlivu na ochranu osobních údajů dopadne např. na finanční instituce. Na druhou stranu nejedná se o institut zcela nový. Například zmíněné finanční instituce již dnes provádějí tzv. analýzu rizik, jejíž struktura a obsah by měly být v zásadě totožné s posouzením vlivu. Kromě popisu zpracování musí posouzení obsahovat i posouzení nezbytnosti a přiměřenosti zpracování z hlediska účelu, posouzení rizik pro práva a svobody subjektu údajů a plánovaní opatření k řešení těchto rizik včetně záruk, bezpečnostních opatření a mechanizmů k zajištění ochrany osobních údajů a k doložení souladu s nařízením. Správce, který bude provádět posouzení vlivu, bude muset v prvé řadě posoudit konkrétní pravděpodobnost a závažnost vysokého rizika a následně pak, na základě výsledku posouzení, stanovit opatření, záruky a mechanismy pro eliminaci tohoto rizika, zajistit ochranu osobních údajů a prokázat soulad s nařízením. Pokud s ohledem na dostupné technologie správce usoudí, že vysoké riziko nelze vhodnými opatřeními zmírnit, má navíc povinnost konzultovat dozorový úřad. Pozitivní informací je skutečnost, že posouzení vlivu je možné provést buď pro jedno zpracování ale také pro soubor podobných zpracování a může být provedeno dokonce společně i pro celé průmyslové odvětví, pro určitý segment nebo pro široce užívanou horizontální činnost. Pro některé instituce provádějící zpracování se stejnými parametry, u nichž lze předpokládat aktivní využití nových institutů (kodexů chování, osvědčení), se tak v tomto ohledu nabízí určité možnosti vzájemné spolupráce v případě

vytváření společných posouzení vlivu, etických kodexů, případně dalších standardů zajišťující soulad s nařízením. Posouzení vlivu na ochranu osobních údajů se tak stává důležitým nástrojem, prostřednictvím kterého správce dokládá, že zamýšlené zpracování je v souladu s nařízením – viz výše princip accountability.

Nařízení dále ukládá správci povinnost přijmout vhodná technická a organizační opatření, aby byla zaručena úroveň zabezpečení osobních údajů odpovídající konkrétnímu riziku. Navzdory tomu může dojít, vlivem záměrné činnosti, hackerského útoku, nedbalosti, omylu nebo živelní události, k porušení zabezpečení osobních údajů, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů. Nařízení ukládá správci povinnost, za stanovených podmínek, porušení zabezpečení osobních údajů oznámit Úřadu pro ochranu osobních údajů případně i dotčeným subjektům údajů (tzv. data breaches). Ani v tomto případě se však nejedná o povinnost zcela novou. Novelou zákona o elektronických komunikacích[5] s účinností od 1. ledna 2012 byla do našeho právního řádu zavedena povinnost oznamovat porušení zabezpečení osobních údajů poskytovatelů veřejně dostupných služeb elektronických komunikací. Nařízení de facto pouze rozšiřuje oznamovací povinnost i na další odvětví. Správci, na které se bude ohlašovací povinnost vztahovat, si budou muset zavést vnitřní postupy a mechanismy pro případ, že by k takovému porušení došlo (jak v takovém případě postupovat – zjištění bezpečnostního incidentu a podrobností o něm, způsob, rozsah, závažnost porušení, kdo je odpovědný za bezpečnost dat, procesní a technické zabezpečení toho, aby nedošlo k opětovnému porušení apod.). Navíc má správce povinnost veškeré případy porušení zabezpečení osobních údajů dokumentovat tak, aby bylo Úřadu pro ochranu osobních údajů umožněno ověření plnění povinností uložených nařízením. I v případě vyřizování agendy porušení zabezpečení osobních údajů, by měl hrát klíčovou roli pověřenec pro ochranu osobních údajů.

Společně s účinností nařízení sice dojde ke zrušení oznamovací povinnosti vůči dozorovému úřadu, jež se často jevila jako zbytečná administrativní zátěž, avšak vzhledem k množství nových povinností, jež správcům přibydou, se jedná pouze o nepatrné odlehčení. Kromě výše uvedených institutů nařízení obsahuje řadu dalších novinek jako například kodexy chování, osvědčení o ochraně osobních údajů, změny týkající se předávání osobních údajů a podobně.

Jaké kroky podniknout

Správcům osobních údajů lze vzhledem k výše uvedenému doporučit následující kroky:

- řádně se seznámit s nařízením, a pokud možno již nyní určit osobu či osoby, které se budou této regulaci podrobněji věnovat, neboť zajištění souladu bude představovat dlouhodobý a soustavný proces;
- posoudit a nejlépe i zdokumentovat všechny současné procesy společnosti, které zahrnují zpracování osobních údajů. Vzhledem k tomu jak se zpracování údajů prolíná s množstvím obchodních aktivit, se bude zřejmě jednat o časově a personálně náročnou analýzu zahrnující nejen útvary přímo pracující s daty klientů (vč. obchodní sítě), ale i personální agendu, marketing, IT, security či správu budov, která má zřejmě v gesci archiv či kamerový systém. Pro každé zpracování by měl být jasně definován účel a posléze právem uznaný důvod, na základě kterého je zpracování prováděno;
- provést důkladnou analýzu interních předpisů a posouzení, zda současný stav vyhovuje novým požadavkům a v návaznosti na výsledky začít s přepracováváním. Nebude se zřejmě jednat pouze o jediný předpis, neboť ke zpracování osobních údajů dochází také při řadě běžných činností (poskytování služeb, správa smluv, řízení některých rizik apod.). Proto posouzení nelze

omezit pouze na jediný předpis týkající se ochrany osobních údajů;
- kromě interních předpisů bude zřejmě nutná i revize informací poskytovaných klientům (např. v rámci smluv či na internetu), a revize procesů k zajištění uplatňování a výkonu práv subjektů údajů (např. formulář pro žádost o informace o zpracování osobních údajů, žádost o opravu, výmaz nebo i interní sladění jak v těchto situacích postupovat);
- vhodné je také vytvořit školící program, na základě kterého budou jednotliví pracovníci vzhledem ke své funkci proškoleni ohledně svých povinností.

Závěr

Není pochyb, že nová regulace ochrany osobních údajů bude mít na soukromý sektor značný dopad a vypořádání se se všemi novými regulatorními požadavky nebude snadné. I když již je nařízení platné a pro jeho implementaci do běžné praxe zbývají pouze necelé dva roky, je pořád spojeno s řadou nejasností, s kterými se budou muset postupně vypořádat evropské i národní dozorové úřady, zejména v rámci prováděcích předpisů. Žádný správce by neměl opomenout riziko výrazně vyšších sankci, než ty které byly umožněny doposud. Nově správcům hrozí správní pokuty až do výše 20 000 000 eur nebo jedná-li se o podnik, až do výše 4 % celkového ročního obratu celosvětově za předchozí rozpočtový rok. Je tak zcela na místě věnovat novým regulatorním požadavků zvýšenou pozornost a již zahájit první kroky k zajištění a doložení souladu s nařízením.

Mgr. Zuzana Radičová,
právník/compliance v Raiffeisen stavební spořitelně

Mgr. David Burian,
vedoucí oddělení registračních činností Úřadu pro ochranu osobních údajů

---

[1] 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, dostupné na www, k dispozici >>> zde.
[2] Další články autorů k novému nařízení o ochraně osobních údajů naleznete např. - dostupné na www, k dispozici >>> zde či zde.
[3] Princip accountability (čl. 5 odst. 2 nařízení) pochází z anglosaského prostředí. Jeho smysl spočívá v tom, že správce/zpracovatel je schopen prokázat a doložit, že zpracování provádí v souladu s nařízením. Do češtiny je termín nepřesně překládán jako „odpovědnost“, místo přesnějšího termínu „přičitatelnost“. Nařízení totiž operuje dále s pojmy „responsibility“ (čl. 24) a „liability“ (čl. 82),

které jsou rovněž překládány do českého jazyka jako „odpovědnost“. Jedná se tedy o tři významově různá anglická slova, která jsou do češtiny překládány jednotně jako „odpovědnost“.
[4] C 131/12 Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González
[5] Zákon č. 127/2005 Sb., o elektronických komunikacích a změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů

Další články:

- Právo na přístup ke kamerovým záznamům: střet GDPR, informačního zákona a praxe veřejných institucí
- Postoupení pohledávky na výživné jako novinka právní úpravy účinné od 1. 1. 2026
- Jak zahájit provoz mezinárodní letecké linky do České republiky (EU): právní požadavky pro aerolinky ze třetích zemí
- Mimořádné vydržení a vývoj judikatury Nejvyššího soudu
- Preventivně-sankční funkce náhrady nemajetkové újmy za porušení osobnostních práv pohledem Ústavního soudu
- Odštěpný závod zahraniční společnosti optikou NIS2: Jak správně určit velikost podniku?
- Zápis ochranné známky bez komplikací. Klíčem k úspěchu je kvalitní předběžná rešerše
- Zneužití práva na přístup podle GDPR
- Byznys a paragrafy, díl 31. - létající pořizovatel ve světle nového stavebního zákona
- Právní povaha sítě elektronických komunikací – režim náhrady škody
- Náhrada ušlého nájemného při předčasném ukončení nájemní smlouvy na nebytové prostory