ČESKÁ REPUBLIKA

ROZSUDEK JMÉNEM REPUBLIKY

Nejvyšší správní soud rozhodl v senátu složeném z předsedy JUDr. Karla Šimky a soudkyň Mgr. Evy Šonkové a JUDr. Miluše Doškové v právní věci žalobkyně: **Vězeňská služba České republiky,** se sídlem Soudní 1672/1a, Praha 4, proti žalovanému: **Úřad pro ochranu osobních údajů,** se sídlem Pplk. Sochora 27, Praha 7, proti rozhodnutí předsedy žalovaného ze dne 20. 5. 2013, č. j. UOOU-00182/13-27, o kasační stížnosti žalobkyně proti rozsudku Městského soudu v Praze ze dne 5. 8. 2016, č. j. 10 A 154/2013 – 27,

takto:

I. Kasační stížnost **se zamítá.**

II. Žalobkyně **nemá** právo na náhradu nákladů řízení o kasační stížnosti.

III. Žalovanému **se** náhrada nákladů řízení o kasační stížnosti **nepřiznává.**

Odůvodnění:

I. Vymezení věci

[1] Se žalobkyní bylo zahájeno správní řízení pro podezření ze spáchání správního deliktu podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů“), v jehož důsledku mělo dojít k neoprávněnému přístupu k osobním údajům osmi osob umístěných ve vazebních věznicích v souvislosti s kauzou a zatčením MUDr. D. R. a následnému zveřejnění fotografií těchto osob v deníku Blesk v červnu 2012.

[2] Žalovaný rozhodnutím ze dne 25. 3. 2013, č. j. UOOU-00182/13-21 (dále jen „prvostupňové rozhodnutí“), shledal, že žalobkyně porušila § 13 odst. 1 zákona o ochraně osobních údajů, tedy povinnost přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití

osobních údajů. Za to jí byla uložena pokuta ve výši 50 000 Kč. Rozklad podaný proti prvostupňovému rozhodnutí zamítl předseda žalovaného v záhlaví označeným rozhodnutím (dále jen „napadené rozhodnutí“).

[3] Proti napadenému rozhodnutí podala žalobkyně žalobu, kterou Městský soud v Praze zamítl v záhlaví uvedeným rozsudkem (dále jen „městský soud“ a „napadený rozsudek“). Městský soud předně nesouhlasil se žalobní námitkou spočívající v tom, že žalobkyně jako organizační složka státu nespadá mezi deliktně způsobilé subjekty podle § 45 odst. 1 zákona o ochraně osobních údajů. K samotnému naplnění skutkové podstaty správního deliktu pak uvedl, že došlo k neoprávněnému přístupu k osobním údajům ve vězeňském informačním systému (dále jen „VIS“), resp. k jejich zneužití, čemuž měla žalobkyně jako správce a zpracovatel povinnost zabránit nastavením přístupových oprávnění k systému automatizovaného zpracování osobních údajů v rozsahu, v němž ta která fyzická osoba oprávněná k přístupu potřebovala příslušné osobní údaje užít, a to v souladu s účelem vymezeným v § 5 odst 1 písm. a) zákona o ochraně osobních údajů. Pokud žalobkyně provozovala VIS s takovým nastavením přístupových oprávnění, že všechny osoby oprávněné s ním pracovat měly přístup ke všem údajům bez vztahu ke konkrétnímu úkolu těchto osob, porušila povinnosti plynoucí jí z § 13 zákona o ochraně osobních údajů. Žalobkyně nerespektovala zásadu, aby přístupová oprávnění v systému automatizovaného zpracování osobních údajů v maximální míře zabraňovala riziku neoprávněného (tj. v rozporu s účelem zpracování informací) užití osobních údajů. Pro výkon činnosti žalobkyně nebylo nezbytné mít takto široce nastavená přístupová oprávnění do VIS, což jasně prokazuje sama skutečnost, že žalobkyně tato oprávnění v návaznosti na kontrolu žalovaného restriktivním způsobem upravila. Městský soud shrnul, že žalobkyni nebylo vytýkáno, že měl do systému přístup nadměrný počet osob, ani to, že dva její zaměstnanci porušili tehdy platná opatření k zajištění bezpečnosti osobních údajů, ale skutečnost, že přístupová oprávnění byla nastavena způsobem, který nerespektoval skutečnou potřebu osobních údajů o vězních k plnění pracovních (služebních) úkolů těchto osob. Její opatření byla z hlediska zákonného požadavku vyjádřeného v § 13 odst. 4 písm. b) zákona o ochraně osobních údajů nedostatečná.

[4] Městský soud se dále ztotožnil s názorem správních orgánů, že aplikace § 46 odst. 1 zákona o ochraně osobních údajů, podle něhož právnická osoba za správní delikt neodpovídá, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila, nebyla namístě. Ze skutkových zjištění plyne, že jednotlivá přístupová oprávnění bylo možno nastavit daleko cíleněji a restriktivněji, než odpovídalo původní praxi žalobkyně. Žalobkyně se nemohla zprostit odpovědnosti za nedůsledné nastavení přístupových oprávnění ani tím, že osobám, které objektivně měly nepřiměřená přístupová oprávnění, zakázala vnitřním předpisem osobní údaje zneužít.

II. Obsah kasační stížnosti a vyjádření žalovaného

[5] Žalobkyně (dále jen „stěžovatelka“) brojí proti napadenému rozsudku kasační stížností, kterou opírá o důvod dle § 103 odst. 1 písm. a) zákona č. 150/2002 Sb., soudní řád správní (dále jen „s. ř. s.“), a tedy namítá nesprávné posouzení právní otázky městským soudem.

[6] Stěžovatelka rozporuje závěr, že porušila generální klauzuli ochrany bezpečnosti osobních údajů dle § 13 odst. 1 zákona o ochraně osobních údajů. Je toho názoru, že v obecné rovině jsou dostatečným prostředkem ochrany osobních údajů vnitřní organizační opatření, tj. závazné interní normy či pokyny stanovící odpovědnost konkrétních osob za bezpečnost zpracovávaných osobních údajů (nařízení generálního ředitele č. 20/2005), a všichni její zaměstnanci navíc

podepisují prohlášení o mlčenlivosti. V projednávané věci došlo k morálnímu selhání dvou osob, které se dopustily protiprávního jednání, což však stěžovatelce nelze přičítat k tíži, neboť tomu nikdy nelze zcela zabránit. Stěžovatelka se domnívá, že vyvinula veškeré úsilí, aby náležitě zabezpečila zpracovávané osobní údaje, proto měl být aplikován liberační důvod dle § 46 odst. 1 zákona o ochraně osobních údajů. Připomíná také, že jí užívaný systém měl mechanismus, který umožnil vyhledání osob, které se provinění dopustily, což umožnilo zahájení trestního stíhání proti nim.

[7] Podle stěžovatelky musí mít přístup k údajům o vězněných osobách všichni zaměstnanci, kteří vkládají do VIS údaje. Těmi nemohou být pouze pracovníci věznice, v níž je umístěna vězněná osoba. Žalovaný přitom mylně dospěl k závěru, že zveřejnění fotografií osob umístěných ve vazebních věznicích v souvislosti s případem MUDr. R. se odrazilo ve změně tohoto principu. Pokud by byl tento princip opuštěn, nemohli by se pracovníci přijímající věznice ani příslušníci provádějící eskorty seznamovat s profily vězňů a získat o nich konkrétní informace. Stěžovatelka je přesvědčena, že přístupová oprávnění do VIS byla nastavena korektně. Závěrem podotýká, že od zavedení VIS v roce 2004 došlo k úniku informací pouze v tomto jediném případě.

[8] Žalovaný se ve svém vyjádření ke kasační stížnosti ztotožňuje s právním posouzením městského soudu a odkazuje na odůvodnění prvostupňového i napadeného rozhodnutí. Přijetí interních předpisů nemá za dostatečný prostředek předcházení zásahu do osobních údajů, pokud správce osobních údajů dodržování přijatých norem nekontroluje. Liberační důvod dle § 46 odst. 1 zákona o ochraně osobních údajů nelze dle žalovaného aplikovat. K otázce, zda všichni zaměstnanci stěžovatelky potřebují přístup k údajům o vězněných osobách, žalovaný podotýká, že stěžovatelka během kontroly ani v průběhu správního řízení neodůvodnila, proč musí mít řadoví zaměstnanci přímý a nepřetržitý přístup k údajům o vězních z jiných věznic. Takový důvod dle žalovaného ani neexistuje. Že šlo o jediný incident od zavedení systému v roce 2004, bylo vedle jiných skutečností zohledněno ve výši sankce.

III. Posouzení kasační stížnosti Nejvyšším správním soudem

[9] Nejvyšší správní soud nejprve zkoumal formální náležitosti kasační stížnosti. Konstatoval, že stěžovatelka je osobou oprávněnou k jejímu podání, neboť byla účastníkem řízení, z něhož napadený rozsudek vzešel (§ 102 s. ř. s.). Kasační stížnost byla podána včas (§ 106 odst. 2 s. ř. s.) a za stěžovatelku v souladu s § 105 odst. 2 s. ř. s. jedná její zaměstnanec, který má požadované vysokoškolské právnické vzdělání, které je podle zvláštních zákonů vyžadováno pro výkon advokacie.

[10] Důvodnost kasační stížnosti vážil Nejvyšší správní soud v mezích jejího rozsahu a uplatněných důvodů a zkoumal přitom, zda napadený rozsudek netrpí vadami, k nimž by musel přihlédnout z úřední povinnosti (§ 109 odst. 3 a 4 s. ř. s.).

III. 1. K porušení povinností dle § 13 odst. 1 zákona o ochraně osobních údajů

[11] Podle § 13 odst. 1 zákona o ochraně osobních údajů „*[s]právce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů.*“ Dle důvodové zprávy k tomuto zákonu (dostupné např. z ASPI) se citovaným ustanovením stanoví obecné povinnosti pro všechny správce co do zajištění ochrany osobních údajů a jejich

bezpečnosti. „*Opatřeními, která je správce povinen učinit, se rozumí opatření technická, organizační, právní a jiná. Jimi se má zabránit neoprávněnému i nahodilému přístupu, zpracování a zneužívání /využívání/ osobních údajů. Údaje musí být chráněny jak vůči zaměstnancům, tak jiným osobám, které s nimi oprávněně přicházejí do styku, tak např. vůči tzv. průnikářům (hackerům)*“ (důraz přidán).

[12] Původně obecná úprava § 13 zákona o ochraně osobních údajů, který dříve obsahoval pouze jeden, shora citovaný odstavec, doznala změn mimo jiné s přijetím zákona č. 170/2007 Sb. Do třetího a čtvrtého odstavce byly přidány povinnosti správce a zpracovatele, které obecné povinnosti dle prvního odstavce konkretizují. Podle § 13 odst. 3 tohoto zákona má správce nebo zpracovatel posuzovat rizika týkající se mimo jiné „*a) plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům, b) zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování*“. V oblasti automatizovaného zpracování osobních údajů jsou dle § 13 odst. 4 zákona o ochraně osobních údajů povinni také „*a) zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby, b) zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby*“.

[13] Nejvyšší správní soud v rozsudku ze dne 30. 1. 2013, č. j. 7 As 150/2012 – 35, publ. pod č. 2845/2013 Sb. NSS (dostupném stejně jako ostatní zde citovaná rozhodnutí z www.nssoud.cz), poznamenal, že pokud jde o obecné povinnosti stanovené v § 13 odst. 1 zákona o ochraně osobních údajů, je volba konkrétních opatření, která mají správce nebo zpracovatel přijmout, ponechána na nich. V případě konkrétních opatření dle odstavce třetího a čtvrtého tak tomu ovšem není, ta je nutno přijmout bezvýhradně.

[14] Ustanovení § 13 odst. 3 zákona o ochraně osobních údajů ukládá správci nebo zpracovateli povinnost hodnotit rizika, neboť přijetí adekvátních bezpečnostních opatření dle odstavce prvního předpokládá nejprve posouzení hrozeb. Dle písm. a) tohoto ustanovení mají posoudit v rámci opatření přijímaných dle prvního odstavce rizika spojená s plněním pokynů pro zpracování osobních údajů osobami, které k nim mají bezprostřední přístup. Nedílnou součástí bezpečnostních opatření by tak mělo být rozdělení pracovních úkolů a jednoznačné určení odpovědnosti za kroky spojené se zpracováním osobních údajů na určitém pracovišti. Pokud zpracovatel či správce zjistí, že zde existují rizika pramenící z toho, že plněním úkolů pověřuje další osoby (zejména zaměstnance), je dle § 13 odst. 1 tohoto zákona povinen přijmout odpovídající opatření tak, aby je snížil na minimum. Vhodným nástrojem nepochybně mohou být interní pokyny či směrnice pro zaměstnance (které současně budou reflektovat povinnost mlčenlivosti zakotvenou v § 15 zákona), správce či zpracovatel je však zároveň povinen plnění interních pokynů kontrolovat. Dle písm. b) jsou povinni dále zvažovat, jak zabránit neoprávněným osobám v přístupu k osobním údajům, přičemž neoprávněnými osobami je třeba i s ohledem na důvodovou zprávu rozumět nejen osoby vně organizační struktury zpracovatele nebo správce, ale také osoby pro ně pracující, které ovšem vzhledem k náplni své činnosti nejsou oprávněny se s danými osobními údaji seznamovat, neboť to pro plnění jejich úkolu není nutné (srov. také komentářovou literaturu KUČEROVÁ, A. a kol. *Zákon o ochraně osobních údajů. Komentář*. Praha: C. H. Beck, 2012, s. 231 – 232, nebo NOVÁK, D. *Zákon o ochraně osobních údajů a předpisy související. Komentář*. Praha: Wolters Kluwer, 2014, s. 237 - 239). Výklad, který k těmto ustanovením podal městský soud v napadeném rozsudku (zejména str. 12), odpovídá shora řečenému a nelze mu tedy ničeho vytknout.

[15] Co se týče § 13 odst. 4 zákona o ochraně osobních údajů, ten dopadá výhradně na automatizované zpracování osobních údajů, tedy zpracování za použití výpočetní techniky, z něhož „*plynou vyšší rizika úniku osobních údajů, jejich neoprávněné změny, zničení, ztráty,*

zpracování či jiného zneužití. Je tomu tak proto, že výpočetní technika umožňuje rychlé a detailní zpracování velkého množství dat (zejména jejich strukturované uspořádání a analýzu podle zadaných kombinací kritérií), jakož i jejich snadné a bez zvláštních opatření následně jen obtížně zjistitelné kopírování, včetně kopírování nepovoleného. V e své podstatě jsou to právě informační systémy provozované pomocí výpočetní techniky, jež svojí podstatou jsou typický potenciální objekt zneužití osobních údajů v masovém měřítku, a to způsobem, co do komerčních i jiných možností využití takto získaných dat vysoce společensky nebezpečným" (již citovaný rozsudek Nejvyššího správního soudu č. j. 7 As 150/2012 – 35). Podle písm. a) tohoto ustanovení je povinností správce nebo zpracovatele zajistit přístup k osobním údajům jen oprávněným osobám, kterými je dle mínění zdejšího soudu třeba stejně jako v případě předešlého odstavce rozumět osoby, které se s danými osobními údaji potřebují seznamovat a pracovat s nimi vzhledem ke svému pracovnímu úkolu, resp. pozici, kterou zastávají. Tyto oprávněné osoby pak musí mít dle písm. b) upravena přístupová oprávnění tak, aby mohly pracovat jen s pro ně potřebnými osobními údaji, a nikoli i s osobními údaji dalšími. Přístupová oprávnění je tedy nutno individualizovat, k čemuž zpravidla bude docházet jednak podle agendy a jednak podle postavení dané osoby (nadřízený bude mít přístup k více datům než podřízený).

[16] Jedním z preventivních prostředků ochrany osobních údajů tedy mohou být vnitřní organizační opatření (závazné interní pokyny), nelze však souhlasit s názorem stěžovatelky, že se v jejím případě jednalo o prostředek dostatečný. Stěžovatelka jakožto provozovatel VIS byla povinna učinit i další kroky k tomu, aby vyhověla požadavkům dle § 13 odst. 1 zákona o ochraně osobních údajů. V tomto ohledu je nutné mít na zřeteli, že na ni dopadalo konkretizující ustanovení odst. 4, a tudíž byla povinna bezvýhradně přijmout bezpečnostní opatření zde uvedená. V souzené věci přitom není sporu o tom, že přístup do VIS, konkrétně k fotografiím vězněných osob, měl v rozhodnou dobu každý zaměstnanec stěžovatelky, který byl jakýmkoliv způsobem oprávněn pracovat s daty vězněných osob. Jednalo se o osoby na pozicích ředitel, zástupce ředitele, správní referent správního úseku, dozorce výkonu vazby a trestu, vychovatel výkonu vazby a trestu, sociální pracovník, pedagog, psycholog, strážník vězeňské stráže, příslušník prevence a stížností, zaměstnanec zdravotního střediska, materiálový intendant pro vězněné osoby, zaměstnanec na úseku zaměstnávání vězněných osob, účetní, duchovní zaměstnanec, včetně příslušných vedoucích funkcionářů (viz sdělení stěžovatelky ze dne 22. 1. 2013, č. l. 7 správního spisu). K fotografiím jednotlivých vězňů mělo přístup cca 5000 zaměstnanců povolaných s daty pracovat (viz sdělení stěžovatelky ze dne 12. 2. 2013, č. l. 18 správního spisu). Tyto skutečnosti svědčí o tom, že přístupová oprávnění nemohla být v rozhodnou dobu nastavena individuálně při zohlednění pracovní náplně jednotlivých zaměstnanců, čímž bylo riziko neoprávněného nebo nahodilého přístupu k osobním údajům, jejich změně, zničení, ztrátě, přenosu, zpracování či jinému zneužití zvýšeno, a nikoli sníženo na minimum, jak vyžaduje § 13 odst. 1 zákona o ochraně osobních údajů.

[17] Stěžovatelka své tvrzení, že přístupem k údajům o vězněných osobách musí disponovat všichni zaměstnanci, kteří údaje do VIS vkládají, a nejen ti, kteří v dané věznici působí, nijak nekonkretizuje. Nejvyššímu správnímu soudu tak není vůbec zřejmé, proč by například materiálový intendant nebo účetní potřeboval mít k plnění svých pracovních úkolů neustálý přístup k informacím o vězních (např. fotografiím), natožpak o vězních umístěných v jiné věznici než té, ve které sami působí. Stěžovatelčino kusé konstatování tak není schopno jakkoliv zpochybnit závěry o nedostatečných opatřeních, které v této věci zaujaly již správní orgány a městský soud.

[18] Nejvyšší správní soud ze shora uvedených důvodů sdílí názor městského soudu, že stěžovatelka porušila § 13 odst. 1 zákona o ochraně osobních údajů tím, že nedostála povinnostem, které pro ni plynuly zejména z § 13 odst. 4 písm. a) a b) téhož zákona.

III. 2. K liberaci dle § 46 zákona o ochraně osobních údajů

[19] Podle § 46 odst. 1 zákona o ochraně osobních údajů „*[p]rávnická osoba za správní delikt neodpovídá, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila*“. Toto ustanovení vychází z toho, že odpovědnost za správní delikt je podle zákona o ochraně osobních údajů objektivní, a tedy se nezkoumá zavinění. Z dikce citovaného ustanovení je patrné, že je třeba prokázat vynaložení veškerého (maximálního) možného úsilí, které lze spravedlivě požadovat (srov. také rozsudek Městského soudu v Praze ze dne 26. 5. 2014, č. j. 11 A 107/2013 – 28). Pokud tedy pachatel správního deliktu tvrdí, že nějaké úsilí vynaložil, ale současně lze dospět k závěru, že mohl a měl učinit více, aby negativnímu následku zabránil, nelze o aplikaci tohoto ustanovení vůbec uvažovat.

[20] Názoru stěžovatelky, že bylo namístě aplikovat liberační důvod dle § 46 odst. 1 zákona o ochraně osobních údajů, přisvědčit nelze. Stěžovatelka nebyla sankcionována za selhání dvou jejích zaměstnanců, kteří porušili své pracovní závazky a předali médiím několik fotografií z VIS zachycujících osoby umístěné ve vazebních věznicích, nýbrž za nesplnění vlastních povinností, které pro ni plynuly ze zákona o ochraně osobních údajů. Skutečnost, že došlo k úniku osobních údajů z VIS, byla pouze indikátorem přítomnosti nedostatků při spravování osobních údajů o vězních a podnětem k zahájení kontroly u stěžovatelky. Pokud bylo v rámci této kontroly prokázáno, že stěžovatelka nesplnila povinnosti, které jí ukládal § 13 zákona o ochraně osobních údajů, neboť neupravila přístupová oprávnění svých zaměstnanců s ohledem na jejich pracovní pozici a úkoly, nemohlo z její strany dojít k vynaložení veškerého možného úsilí. Existenci konkrétních okolností, které by jí objektivně bránily potřebné úsilí vynaložit, přitom stěžovatelka netvrdila. To, že stěžovatelka v návaznosti na provedenou kontrolu přístupová oprávnění diverzifikovala, naopak svědčí o tom, že v rozhodné době nebylo nastavení VIS provedeno správně.

[21] Tvrzení stěžovatelky, že žalovaný nezohlednil skutečnost, že od roku 2004, kdy byl VIS zaveden, došlo k úniku osobních údajů jen v tomto jediném případě, nemůže na závěru o její odpovědnosti za nesplnění povinností dle § 13 zákona o ochraně osobních údajů ničeho změnit. Pro naplnění skutkové podstaty správního deliktu, kterého se stěžovatelka dopustila, není podstatné to, zda nebo ke kolika únikům informací došlo. Rozhodující je, že stěžovatelka nepřijala dostatečná opatření pro zajištění bezpečnosti osobních údajů. Rozsah a četnost konkrétních škodlivých následků pramenících z nesplněné povinnosti lze zohlednit jako polehčující či přitěžující okolnost až při stanovení výše pokuty. Ojedinělost úniku informací měla v případě stěžovatelky vliv na výši pokuty, která činila pouhé jedno procento maximální zákonné sazby, neboť žalovaný přihlédl k tomu, že v důsledku nepřijetí dostatečných opatření došlo k prokazatelnému úniku informací jen o osmi osobách (tj. v rámci jediného incidentu z června 2012), jejichž totožnost již veřejnosti v souvislosti s medializovanou kauzou stejně byla známa.

IV. Závěr a rozhodnutí o nákladech řízení

[22] Nejvyšší správní soud dospěl ze shora uvedených důvodů k závěru, že kasační stížnost není důvodná, a proto ji dle § 110 odst. 1 *in fine* s. ř. s. zamítl.

[23] O náhradě nákladů řízení o kasační stížnosti rozhodl Nejvyšší správní soud v souladu s § 60 odst. 1 s. ř. s. ve spojení s § 120 s. ř. s. Stěžovatelka neměla ve věci úspěch, a proto nemá

právo na náhradu nákladů řízení. Úspěšný žalovaný vznik nákladů řízení o kasační stížnosti netvrdil a ani ze spisu Nejvyššího správního soudu neplyne, že by mu nějaké náklady nad rámec jeho běžné činnosti vznikly, proto mu právo na jejich náhradu nemohlo být přiznáno.

P o u č e n í : Proti tomuto rozsudku **n e j s o u** opravné prostředky přípustné.

V Brně dne 5. ledna 2017

JUDr. Karel Šimka
předseda senátu