



XXXXXXXXXXXXX
XXXXXXXXXX
bytem: XXXXXXXXXXXXXXXX
XXXXXXXXXXXXX
/dále také jako „Žadatel“/

naše č. j. TSK/006/2025
vyřizuje: XXXXXXXXXXXX
V Praze dne 31. 01. 2025

ROZHODNUTÍ O ODMÍTNUTÍ ŽÁDOSTI

Technická správa komunikací hl. m. Prahy, a.s. (dále také jako „TSK“), se sídlem: Veletržní 1623/24, Holešovice, 170 00 Praha 7, IČO: 03447286, zapsaná v OR vedeném MS v Praze v odd. B, vl. 20059 jako povinný subjekt dle § 2a, odst. 1, písm. b) zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále jen „InfZ“) rozhodl v souladu s ustanovením § 15, odst. 1 InfZ o žádosti pana XXX, ze dne 16. 01. 2025, doručené povinnému subjektu dne 16. 01. 2025 (dále také jako Žádost), o poskytnutí informace, specifikované v Žádosti, konkrétně takto:

- a) „žádám o zpřístupnění API pro systém CIS parkování za účelem možnosti ověřování, zda vybrané automobily disponují parkovacím oprávněním“

takto:

Žádost žadatele pana XXX, ze dne 16. 01. 2025, doručená povinnému subjektu dne 16. 01. 2025, o poskytnutí informace spočívající ve sdělení/poskytnutí „*zpřístupnění API pro systém CIS parkování za účelem možnosti ověřování, zda vybrané automobily disponují parkovacím oprávněním*“,

SE ODMÍTÁ,

neboť s odkazem na ust. § 11b InfZ za současného využití ust. § 11, odst. 1, písm. d) InfZ, protože se jedná o informaci, kterou povinný subjekt nemá, když mu taková povinnost nevyplyvá ani ze zákona, resp. jejíž poskytnutí, byť v omezeném a Žádostí ne zcela přesně vyžádaném rozsahu, přímo ohrožuje účinnost bezpečnostních opatření stanovených na základě zvláštního právního předpisu pro účel ochrany osob, majetku a veřejného pořádku.



Odůvodnění:

Technické správě komunikací hl. m. Prahy, a.s., se sídlem: Veletržní 1623/24, Holešovice, 170 00 Praha 7, IČO: 03447286, zapsané v OR vedeném MS v Praze v odd. B, vl. 20059, jako povinnému subjektu dle ust. § 2a, odst. 1, písm. b) InfZ byla dne 16. 01. 2025 doručena Žádost žadatele pana XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX, ze dne 16. 01. 2025, o poskytnutí informací podle zákona o svobodném přístupu k informacím, požadující „zpřístupnění API pro systém CIS parkování za účelem možnosti ověřování, zda vybrané automobily disponují parkovacím oprávněním“.

Ust. § 15, odst. 1 InfZ stanoví, že pokud povinný subjekt nevyhoví žádosti, byť i jen zčásti, vydá ve lhůtě pro vyřízení Žádosti o informace rozhodnutí o odmítnutí Žádosti (být i částečném), což je tento případ.

Povinný subjekt úvodem konstatuje, že v Žádosti uváděné zkratky „API“ a „CIS“ ve smyslu dalšího obsahu Žádosti Žadatele definoval pro potřeby vyřízení Žádosti následovně takto:

v případě zkratky „API“ jako *Application programming interface* - tedy rozhraní pro programování aplikací, kdy se jedná o programový nástroj, který umožňuje přímý přístup k obsahu databáze na úrovni jednotlivých programů;

v případě zkratky „CIS“ jako *Centrální informační systém* tedy soustavu softwarových aplikací ve vlastnictví Hlavního města Prahy (dále také jako „MHMP“), využívanou tímto subjektem pro celou škálu zajištění svých činností, mimo jiné i na úseku ochrany bezpečnosti osob, majetku a veřejného pořádku, to vše na základě příslušných autorských licenčních oprávnění, když správa CIS byla svěřena povinnému subjektu.

Povinný subjekt dále konstatuje, že NÚKIB v srpnu 2021 určil Technickou správu komunikací hl. m. Prahy, a.s., IČO: 03447286, se sídlem: Veletržní 1623/24, 170 00 Praha 7, jakožto povinný subjekt a jako provozovatele základní služby dle ZoKB. Povinný subjekt, jakožto povinná osoba dle ZoKB je proto povinen realizovat celou řadu bezpečnostních opatření, řídit se příslušnou legislativou a provádět činnosti dle nařízení vydávaných NÚKIB. Jedna ze základních povinností povinného subjektu je ochrana informací a dat (primárních aktiv), kterou má povinný subjekt realizovanou v souladu s metodikami NÚKIB a získanou certifikací ISO27001:2022, a to na základě jejich klasifikace důvěrnosti rozdělených do čtyř úrovní. K informacím s úrovní důvěrnosti „střední“, „vysoká“ či „kritická“ mají u povinného subjektu přístup pouze osoby, které tyto informace potřebují ke své pracovní činnosti. Za vysoce důvěrné informace považuje povinný subjekt mimo jiné i informace o konkrétních bezpečnostních opatřeních, používaných technologiích, HW a SW prostředcích, způsobu přístupů k SW aplikacím, ochrany, využití a zabezpečení dat a datových souborů/databází, technické podpory informačních systémů spravovaných povinným subjektem včetně HW vybavení, na který jsou informační systémy ve správě povinného subjektu provozovány. V souvislosti s kybernetickou bezpečností bylo na straně povinného akceptováno a současně implementováno písemné Doporučení NÚKIB k (ne)poskytování informací v oblasti kybernetické bezpečnosti a bezpečnosti systémů nakládajících s utajovanými informacemi, ze dne 22.12.2022.

Dále se jeví jako účelné poukázat i na definici vymezení pojmu „osobní údaj“ z hlediska obecně závazných právních předpisů, týkajících se ochrany osobních údajů. Lze potvrdit, jak správně uvádí Žadatel, se za osobní údaj především považuje jakýkoli údaj/informace, který lze „propojit“ s konkrétní fyzickou osobou, nicméně takovéto vymezení ze strany Žadatele není úplné. Za osobní údaj je nutno považovat nejen takovou informaci, která identifikuje konkrétní subjekt údajů, ale též i údaj/informaci, která způsobila



identifikovat subjekt údajů. Jinými slovy osobním údajem je jakákoli informace o identifikované fyzické osobě nebo identifikovatelné fyzické osobě, kterou tak lze přímo či nepřímo identifikovat.

V neposlední řadě povinný subjekt upozorňuje na tu skutečnost, že z hlediska jeho správy CIS v rámci jeho využití pro kontrolu zón placeného stání (dále jen ZPS) na území Hlavního města Prahy v návaznost na vydaná platná parkovací oprávnění (dále jen POP) jednotlivých subjektů využívajících ZPS, nedisponuje jakýmkoli oprávněním či přístupem k databázím údajů shromažďovaným CIS, ze kterých by bylo možno ověřit, zda vybraná motorová vozidla disponují POP či nikoli. Povinný subjekt opakovaně ve vyřizování dotazů dle InfZ spadajících do této oblasti informuje žadatele o informace o tom, že sběr dat v podobě registračních značek motorových vozidel parkujících v ZPS je zaznamenáván monitorovacími vozidly zcela automaticky. Takto nasbíraná data jsou s databází CIS automaticky porovnávána jak v reálném čase, tak i z důvodu kontroly v rámci automatického vyhodnocování opakovaně s časovým odstupem. I při kontrole oprávněnosti parkování motorových vozidel v ZPS vykonávané strážníky Městské policie hlavního města Prahy přímo v terénu, tito z důvodu právní jistoty prokázání spáchání přestupku neoprávněného stání motorového vozidla v ZPS provádějí kontrolu konkrétního vozidla opakovaně po uplynutí přiměřeného časového odstavu. Následné vyhodnocování automaticky sestavených datových sad/balíčků záznamu jednání stran důvodného podezření ze spáchání přestupku neoprávněného parkování motorových vozidel v ZPS, pořízených z monitorovacích vozidel, včetně jejich doplňování o další údaje co do podezření z naplnění skutkové podstaty příslušného přestupku provádí pouze Městská policie hl. m. Prahy. Městská policie hl. m. Prahy je jediným oprávněným subjektem ke zpracování datových údajů o motorových vozidlech parkujících v ZPS v rámci jejich komparace s vydanými platnými POP. Údaje o platných POP stejně tak údaje o vozidlech parkujících v ZPS povinný subjekt jakkoli nezpracovává a nevyhodnocuje. Povinný subjekt není vlastníkem takovýchto databází, ani je jakkoli nezpracovává, povinný subjekt je toliko správcem hardwarového a softwarového systému, jejichž prostřednictvím jsou údaje zaznamenávány a poskytovány k dalšímu využití. S ohledem na tuto skutečnost nemá povinný subjekt jakékoli zákonné oprávnění s daty, a to ani s přístupem k těmto datům jakkoli nakládat, využívat, nebo je poskytovat k dalšímu zpracování či využití třetím subjektům.

V návaznost na výše uvedené má povinný subjekt za to, že není, vzhledem k tomu, že vykonává toliko správu informačního systému, jehož prostřednictvím jsou data o ZPS zaznamenávána, oprávněn jakékoli třetí osobě zřídit přístup k takto zaznamenávaným datům. To vše za situace, kdy povinný subjekt není vlastníkem ani správcem zaznamenaných databází údajů, ale toliko vykonává správu hardwarových zařízení a softwarových systémů, jejichž prostřednictvím jsou data zaznamenávána. Tímto vlastníkem a správcem dat je Hlavní město Praha. Povinný subjekt má dále za to, že Žadatelem vyžádaná informace je způsobilá být nástrojem pro opatřování osobních údajů ve smyslu zvláštních právních předpisů, resp. jejím prostřednictvím lze opatřovat údaje, jimž lze identifikovat konkrétní fyzické osoby – subjekt údajů. Těmito údaji jsou zejména registrační značka motorových vozidel, časový úsek a místo parkování takového motorového vozidla. Osobní údaje smí být zpracovávány (a to jak správcem - tj. tím, kdo je získal od subjektu údajů nebo od jiného správce), pouze k tomu účelu, ke kterému byly získány, popř. s kterým subjekt údajů předem a výslovně souhlasil. V případě, že by osobní údaje byly zpracovávány k jinému účelu, než ke kterému je subjekt údajů poskytl, jednalo by se o porušení zásady zákonnosti (dle čl. 6 GDPR). Je třeba upozornit, že pokud by správce (HMP) nedisponoval řádným důvodem ke zpracování osobních údajů, bylo by dále nerozhodné, zdali plní ostatní povinnosti, jelikož by osobní údaje zpracovával nezákonně a musel by osobní údaje zlikvidovat anebo ukončit jejich nezákonné zpracování. Pakliže správce zpracovává osobní údaje za účelem udělení a správy dlouhodobého parkovacího oprávnění není možné, aby takové údaje veřejně zpřístupnil široké veřejnosti, a to ani jejich část nebo jinak např.



prostřednictvím povinného subjektu, umožnil k nim přístup. Tedy není možné, a v daném případě by se jednalo o nezákonné zpracování, aby správce umožnil široké veřejnosti vyhledávat RZ vozidla s informací, zda mají oprávnění parkovat v dané zóně. Takové neoprávněné zveřejnění - resp. umožnění neoprávněného přístupu k těmto informacím/údajům, by zcela jistě bylo porušením zásady zákonnosti. To vše navíc umocněno tím, že Žadatelem vyžádaným přístupem k databázi údaje by bylo, dle právního názoru povinného subjektu, možno identifikovat konkrétní subjekt údajů/konkrétní fyzickou osobu, neboť z databáze shromážděné údaje o typu, druhu, barvě, registrační značce motorového vozidla, konkrétním místě a konkrétním čase jeho parkování v ZPS lze důvodně předpokládat zjištění konkrétní fyzické osoby/subjektu údajů, který dané vozidlo provozuje, resp. vlastní.

Nadto povinný subjekt současně sděluje, že nedisponuje API pro systém CIS pro ZPS, jenž by umožňovalo přístup k databázím takových údajů, ze kterých by bylo způsobilé bez dalšího zpracování naznat, které vozidlo disponuje platným POP. Jak již bylo výše uvedeno, kontrolu oprávnění parkovat motorová vozidla na území Hlavního města Prahy v zónách placeného stání, a to i v návaznost na vydání platných parkovacích oprávnění má Městská policie hlavního města Prahy v rámci jí prověřovaného možného přestupkového jednání provozovatelů motorových vozidel, parkujících vozidla v konkrétních parkovacích zónách, nikoli povinný subjekt. Nelze tedy poskytnout Žadateli API do CIS k údajům/datům-databázím, ze kterých by bez jejich dalšího zpracování vyplývalo, zda konkrétní zaznamenaná registrační značka, v daném čase a v dané ZPS měla platné POP či nikoli. Takováto databáze v CIS není přítomna, a tedy k ní nelze API poskytnout. Oprávněnost či neoprávněnost parkování konkrétního vozidla v ZPS je zjišťována Městskou policií hl. města Prahy až následným zpracováním údajů ze systému CIS automaticky poskytovaných, a to jejich komparací, tedy zpracováním údajů z různých databází a jejich vyhodnocením pouze pro potřebu a ze strany Městské policie hl. m. Prahy na úsek výkonu jí zajišťované přestupkové agendy. Současně je třeba zdůraznit, že povinný subjekt není smluvně zavázán, stejně jako i nemá zákonnou povinnost disponovat API pro systém CIS za účelem možnosti ověření, zda vybrané automobily disponují parkovacím oprávněním. Povinný subjekt je toliko správcem majetku Magistrátu hlavního města Prahy a v oblasti CIS zajišťuje jeho provozuschopnost, není nadán právem vydávání oprávnění POP, jejich správou, kontrolou z hlediska jejich užití v rámci ZPS a ani sankcionováním pro případ porušení pravidel parkování v ZPS. Zjišťování a vyhodnocování, zda konkrétní vozidlo, v konkrétním čase a místě ZPS má či nemá platné oprávnění POP není v gesci povinného subjektu. Navíc takovouto samostatnou databází CIS, jak už bylo výše řečeno, nevytváří, když tato je výsledkem dalšího zpracování údajů z CIS ze strany Městské policie hlavního města Prahy.

Dále v návaznost na shora uvedené shledává povinný subjekt vysoká a reálná rizika spojená s poskytnutím a zveřejněním jakékoli API do systému CIS, neboť jejich poskytnutím a zveřejněním lze umožnit dojití k cílenému zaměření škodlivých aktivit (kybernetických útoků, sociálního inženýrství apod.) s cílem získat údaje k přístupům do CIS, nebo jakkoli poškodit či omezit činnost CIS. Lze tak uvést, že jakákoli specifikace API do systému CIS je na základě klasifikace informací v rámci hodnocení aktiv podle vyhlášky č. 82/2018 Sb., vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, klasifikována a zařazena do úrovně důvěrnosti „vysoká“. Povinný subjekt postupuje v tomto případě i dle principů předběžné opatrnosti, vědom si budoucích rizik spojených s velmi sofistikovanými útoky pomocí technologií AI, a důsledně chrání svá primární i podpůrná aktiva zařazená do úrovně důvěrnosti „vysoká“ nebo „kritická“.

V této souvislosti povinný subjekt sděluje, že i z aktuálně získaného stanoviska Národního úřadu pro kybernetickou a informační bezpečnost (dozorový orgán v oblasti působnosti zákona č. 181/2014 Sb.,



zákon o kybernetické bezpečnosti a o změně souvisejících zákonů k poskytování) ze dne 16. ledna 2025 vyplývá, že v případě klasifikace informace z pohledu důvěrnosti na úrovni „vysoká“ nebo „kritická“, je podle názoru NÚKIB žádoucí neposkytnout tuto informaci v souladu s § 10a zákona č. 181/2014 Sb., zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) (dále jen „ZKB“), resp. postupovat dle ust. § 11, odst. 1, písm. d) InfZ.

Lze shrnout, že povinný subjekt je povinen (ostatně jako i dalších právní subjekty) řídit se obecně závaznými právními předpisy. V této souvislosti pak zejména právními předpisy z hlediska ochrany a zabezpečení majetku povinného subjektu, resp. majetku Hlavního města Prahy, který byl svěřen povinnému subjektu do správy, předcházet případným škodám na majetku povinného subjektu, resp. spravovaného povinným subjektem a v neposlední řadě se řídit právními předpisy těch veřejných norem práva, které dopadají do jeho činnosti. Za situace, kdy povinný subjekt provozuje hardwarové zařízení (server) a na něm funkční softwarové aplikace/programy nutné nejen pro výkon podnikatelské činnosti povinného subjektu, ale též pro výkon státní správy, navíc za právní situace, kdy je ústředním orgánem státní správy – NÚKIB výslovně určen a pověřen povinnostmi stran zabezpečení kybernetické bezpečnosti takovýchto zařízení, lze jednoznačně dovodit jeho povinnost se příslušnými právními předpisy striktně řídit. To vše navíc umocněno geopolitickou situací, kdy kritická infrastruktura nejen státní institucí v podobě serverů je denně napadána hackerskými útoky, motivovanými ať již kriminální činností nebo snahou o politickou a sociální destabilizaci (např. hackerským útokem na počítačové systémy Ředitelství silnic a dálnic ČR, obdobně kybernetický útok na nemocnice v ČR, útoky na bankovní systémy komerčních bank v ČR apod. v neposlední řadě též bezprecedentním hackerským útokem na servery slovenského katastrálního úřadu). Za takto vymezeného právního rámce a bezpečnostní situace došlo předně k projednání konkrétní žádosti o informace Žadatele s příslušnými zaměstnanci úseku informatiky povinného subjektu za současného vyhodnocení s aktuálním písemným stanoviskem NÚKIB, metodikami NÚKIB a získanou certifikací ISO27001:2022. Povinným subjektem bylo v souladu s vnitřními bezpečnostními předpisy, vydanými na základě ZoKB, vyhodnoceno, že poskytnutí informace v podobě API pro systém CIS nikoli v podobě vyžádané Žadatelem (jak již bylo výše uvedeno touto povinný subjekt nedisponuje), ale i pro databázi zaznamenávaných registračních značek vozidel parkujících v ZPS, může být ve výsledku reálně způsobilým vodítkem (minimálně však přímo usnadnit) možnosti narušení zabezpečení CIS. Navíc, jak již bylo výše uvedeno, poskytnutí takové informace by představovalo rozpor s právními předpisy, jimiž je povinný subjekt povinen se při své činnosti řídit, jakož i vnitřními bezpečnostními předpisy povinného subjektu.

Porušení povinnosti zajistit kybernetickou bezpečnost CIS pak ve svém důsledku může povinnému subjektu přivodit škody v řádech miliónů korun českých a být způsobilé narušit softwarovou bezpečnost nejen u povinného subjektu, ale ve svém důsledku i kritickou infrastrukturu dle zvláštních právních předpisů. Zároveň může přivodit povinnému subjektu právní odpovědnost ve vztahu k HMP, neboť povinný subjekt vykonává správu svěřeného majetku a vybrané činnosti s tím související na základě smluvního vztahu s HMP a je povinen dle smluvního vztahu plnit své povinnosti vedoucí k řádnému výkonu správy, s čímž by poskytnutí vyžádané informace Žadateli, byť i v omezeném rozsahu s jakou s ní povinný subjekt disponuje, nekorespondovalo.

S odkazem na vše shora uvedené povinný subjekt neposkytuje požadované informace tak, jak tyto byly Žadatelem Žadostí vyžádány (viz. výroková část tohoto rozhodnutí), s odkazem na ust. § 15, odst. 1 InfZ ve spojení s ust. § 11b InfZ za současného využití ust. § 11, odst. 1, písm. d) InfZ, protože se jedná o informaci, kterou povinný subjekt nemá, když mu taková povinnost nevyplývá ani ze zákona, resp. jejichž poskytnutí, byť v omezeném a Žadostí přesně nevyžádaném rozsahu přímo ohrožuje účinnost



bezpečnostních opatření stanovených na základě zvláštního právního předpisu pro účel ochrany osob, majetku a veřejného pořádku. S ohledem na tuto skutečnost nelze poskytnout Žadateli informace v rozsahu, jak popsáno shora, resp. tak, jak jím byly v části jeho Žádosti požadovány.

S přihlédnutím k výše uvedenému rozhodl povinný subjekt tak, že Žádost o poskytnutí informací v rozsahu, jak popsáno výše, odmítl.

XXXXXXXXXXXXXXXXXXXXXXXXXXXX

vedoucí oddělení právního a corporate governance

Poučení:

Proti tomuto rozhodnutí je možno podat dle ust. § 16, odst. 1 a § 20, odst. 4, písm. b) InFZ a dle ust. § 83, odst. 1 zák. č. 500/2004 Sb. správní řád, ve znění pozdějších předpisů, odvolání, a to ve lhůtě do 15 dnů ode dne doručení písemného vyhotovení tohoto rozhodnutí k Úřadu pro ochranu osobních údajů (ve smyslu ust. § 20, odst. 5 InFZ) prostřednictvím Technické správy komunikací hl. m. Prahy, a.s.

Upozornění:

Technická správa komunikací hl. m. Prahy, a.s. (dále jen „TSK.“) odmítá při své činnosti jakékoli protiprávní a neetické jednání a v maximální míře dodržuje transparentnost a legalitu. Zaměstnanci a osoby jednající za TSK jsou povinni se při svém jednání řídit zásadami Etického kodexu společnosti Technická správa komunikací hl. m. Prahy, a.s. (dále jen „Etický kodex“), který je nedílnou součástí firemní kultury TSK. Každá z osob jednajících za TSK je povinna oznámit jakékoli podezřelý a protiprávní jednání, které je v rozporu s Etickým kodexem. Pokud osoba jednající za TSK jedná v rozporu s Etickým kodexem, není takové jednání považováno za jednání v rámci nebo zájmu TSK.