PŘEDSEDA
ČESKÉHO ÚŘADU ZEMĚMĚŘICKÉHO
A KATASTRÁLNÍHO
Ing. Karel Štencel

V Praze dne 27. ledna 2026
Sp. zn. ČÚZK-005755/2026-1
Čj: ČÚZK-009688/2026

R O Z H O D N U T Í

Předseda Českého úřadu zeměměřického a katastrálního (dále jen „předseda“) jako příslušný správní orgán podle § 152 odst. 2 zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů (dále jen „správní řád“), ve spojení s § 1 odst. 2 zákona č. 359/1992 Sb., o zeměměřických a katastrálních orgánech, ve znění pozdějších předpisů, na návrh rozkladové komise ustavené podle § 152 odst. 3 správního řádu, o rozkladu podaného panem Janem Harsou, [redacted] (dále jen „žadatel“), dne 12. 1. 2026, proti rozhodnutí Českého úřadu zeměměřického a katastrálního (dále jen „úřad“) ze dne 12. 1. 2026, sp. zn. ČÚZK-072516/2025-11, čj. ČÚZK-004849/2026, o odmítnutí žádosti o poskytnutí informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále jen „informační zákon“), **r o z h o d l** podle § 16 ve spojení s § 20 odst. 4 informačního zákona a § 152 odst. 1, 5 a 6 písm. b) správního řádu

t a k t o :

Rozklad žadatele proti rozhodnutí úřadu ze dne 12. 1. 2026, sp. zn. ČÚZK-072516/2025-11, čj. ČÚZK-004849/2026,

s e z a m í t á .

Odůvodnění:

Úřadu byl dne 12. 1. 2026 doručen rozklad žadatele datovaný týmž dnem proti rozhodnutí úřadu ze dne 12. 1. 2026, sp. zn. ČÚZK-072516/2025-11, čj. ČÚZK-004849/2026, kterým byla odmítnuta jeho žádost o informace v rozsahu bodů 1, 3 a části bodu 7 jeho žádosti ze dne 30. 12. 2025. Žadatel uvádí, že plošné omezení anonymního přístupu k údajům o vlastnících nemovitostí úřadem představuje zásah s významným dopadem na širokou veřejnost, což odůvodňuje podle jeho názoru vyšší nároky na transparentnost rozhodovacího procesu, který k takovému opatření vedl. Napadené rozhodnutí považuje za nedostatečně odůvodněné, v podstatné části za nepřezkoumatelné a založené na příliš extenzivním a obecném výkladu důvodů pro neposkytnutí informace. Poukazuje na to, že rozhodnutí je opřené o obecné tvrzení o možnosti ohrožení kybernetické bezpečnosti provozovaných informačních systémů zpřístupněním požadovaných informací. Má přitom za to, že informace mohly být poskytnuty „*i bez ohrožení bezpečnostního systému, a to pouhým zobecněním či agregací*“. Zároveň ale také namítá, že informace ve zbývajících bodech jeho žádosti mu byly poskytnuty jen formou obecných odpovědí. Žadatel navrhuje, aby předseda rozhodnutí v napadeném rozsahu zrušil a uložil povinnému subjektu žádost znovu posoudit, případně aby sám rozhodl o poskytnutí požadovaných informací „*v rozsahu, který nezasahuje do legitimních bezpečnostních zájmů, avšak respektuje podstatu práva na informace*“.

Ze spisového materiálu bylo zjištěno následující: Úřadu byla dne 30. 12. 2025 doručena žádost žadatele o poskytnutí informací podle informačního zákona vztahujícím se k dočasnému omezení informací o vlastnících nemovitostí v aplikaci Nahlížení do katastru nemovitostí. Žadatel koncipoval požadované informace do sedmi bodů (1. Technická opatření proti nežádoucím přístupům, 2. Ochrana pomocí CAPTCHA, 3. Škálování a architektura služby, 4. Proporcionalita zvoleného opatření, 5. Dopad na osoby bez elektronické identity, 6. Dočasnost opatření a časový plán, 7. Vyhodnocení zahraničních přístupů), které dále strukturoval do bodů označených malými písmeny. Úřad přípisem ze dne 12. 1. 2026, sp. zn. ČÚZK-072516/2025-11, čj. ČÚZK-004848/2026. poskytl žadateli informace ohledně bodů 2, 4, 5, 6 a části bodu 7 - písm. b žádosti. Napadeným rozhodnutím ze dne 12. 1. 2026, sp. zn. ČÚZK-072516/2025-11, čj. ČÚZK-004849/2026, úřad odmítl zbývající část žádosti formulovanou žadatelem jako:

„*1. Technická opatření proti nežádoucím přístupům*
Byla před zavedením povinného přihlášení provedena, vyhodnocena nebo zavedena některá technická opatření k eliminaci nežádoucích přístupů porušujících provozní podmínky aplikace, zejména: a) omezení počtu dotazů (rate-limiting), například na úrovni IP adres, geografických oblastí nebo autonomních systémů (ASN), b) behaviorální ochrana, zejména detekce automatizovaných přístupů (botů), c) throttling dotazů, tj. záměrné zpožďování odpovědí při nadměrném počtu požadavků, d) jiná technická nebo aplikační opatření běžně používaná u veřejných webových služeb, e) Pokud některá z uvedených opatření nebyla zavedena nebo alespoň vyhodnocena, žádám o sdělení důvodů, proč k jejich využití nepřistoupil správce aplikace.
3. Škálovatelnost a architektura služby
Jakým způsobem je u aplikace nahlizenidokn.cuzk.gov.cz a jejích přidružených služeb zajištěna: a) horizontální škálovatelnost (např. možnost přidávání aplikačních instancí při zvýšené zátěži), b) vertikální škálovatelnost (navyšování výpočetního výkonu nebo kapacit), c) oddělení zátěžově náročných částí aplikace (např. čtení veřejných údajů) od citlivějších nebo omezených služeb. d) Pokud škálovatelnost aplikace nebyla řešena nebo byla vyhodnocena jako nedostatečná, žádám o vysvětlení důvodů tohoto stavu.
7. Vyhodnocení zahraničních přístupů
Na základě jakých podkladů a technických dat úřad dospěl k závěru, že k porušování provozních podmínek aplikace docházelo zejména ze zahraničí, a: a) zda byla tato skutečnost vyhodnocena na základě IP adres, geografického určení nebo příslušnosti k autonomním systémům“.

Úřad jako povinný subjekt odmítnutí odůvodnil tím, že podmínky pro omezení práva na informace deklarovaného v čl. 17 odst. 5 Listiny základních práv vymezuje § 12 informačního zákona, který umožňuje neposkytnutí těch informací, o nichž to stanoví zákon, přičemž jedním z takových zákonů je kybernetický zákon. Podle něj se kromě jiného neposkytují podle předpisů upravujících svobodný přístup k informacím informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti. Úřad vyhodnotil, že výše specifikované informace požadované žadatelem takový charakter mají. Na základě testu proporcionality pak dospěl k závěru, že veřejný zájem na kybernetické bezpečnosti informačních systémů státu v tomto případě svou důležitostí přesahuje právo žadatele na poskytnutí informací.

V rozkladovém řízení předseda vycházel z totožného spisového materiálu jako v řízení na prvním stupni. V daném případě tedy nebylo třeba přistoupit k výzvě k seznámení žadatele s podklady pro rozhodnutí a k vyjádření se s nimi (§ 36 odst. 3 správního řádu) neboť byly splněny podmínky pro výjimku z tohoto pravidla dle § 90 odst. 1 písm. c) správního řádu.

Předseda nejprve posoudil předložený rozklad z hlediska jeho přípustnosti a dodržení lhůty pro jeho podání se závěrem, že je přípustný a byl podán včas, tedy v rámci lhůty stanovené v § 83 odst. 1 správního řádu.

Předseda po posouzení podkladů pro vydání rozhodnutí a návrhu rozkladové komise věc přezkoumal a dospěl k závěru, že rozklad není důvodný.

Předseda na základě spisového materiálu shledal, že rozhodnutí vycházelo z odborného stanoviska vyjádřeného ředitelem příslušné sekce úřadu, do jehož gesce spadá problematika, které se požadované informace týkají. V řízení o rozkladu bylo prověřeno, že bylo zaujato na základě výsledků projednání s týmem odborníků úřadu erudovaných v oblasti kybernetické bezpečnosti. Lze tedy konstatovat, že přes stručné odůvodnění rozhodnutí byla věci věnována náležitá pozornost. V této souvislosti stojí za zmínku, že stanovisko reflektovalo účel dočasného opatření proti robotickému získávání dat z aplikace Nahlížení do katastru nemovitostí (KN), přijatého úřadem, ke kterému se žadatelem požadované informace vztahují. Toto opatření vyvolala potřeba urgentní stabilizace provozu aplikace, který se dostal v průběhu prosince 2025 do vážných provozních problémů v důsledku automatického/robotického vytěžování údajů katastru nemovitostí, přičemž dosavadní ochrana testem CAPTCHA se ukázala jako neúčinná. Dočasné opatření spočívající v umožnění zobrazení informací o osobních údajích vlastníků a jiných oprávněných pouze po přihlášení má za cíl citelné omezení možnosti využívat anonymní automatizované/robotické vytěžování, vedoucí k přetěžování technické infrastruktury.

Při posuzování předmětné věci je třeba vycházet z § 12 informačního zákona ve spojení s § 36 zákona č. 264/2025 Sb., o kybernetické bezpečnosti, který stanoví výjimku z práva na informace. V napadeném rozhodnutí je sice nesprávně odkazováno na předchozí právní úpravu obsaženou v § 10a zákona č. 181/2014 Sb., o kybernetické bezpečnosti, avšak text, dopadající na daný případ tj. „*informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti, se podle předpisů upravujících svobodný přístup k informacím neposkytují*“ je v obou zákonech zcela totožný. Uvedená vada tak nemohla mít na meritorní rozhodování žádný vliv. Předseda proto v této věci postupoval v souladu se zásadou rychlosti a hospodárnosti řízení.

Při aplikaci citované normy je pak třeba reflektovat fakt, že v oblasti kybernetické bezpečnosti, která hraje v oblasti bezpečnosti státu stále důležitější roli, převažuje požadavek na zajištění bezpečnosti státu a veřejné bezpečnosti. Na druhou stranu i v této sféře musí povinný subjekt pečlivě zvažovat potřebu omezení práva na informace. V rámci moderního právního státu představuje právo na svobodný přístup k informacím, garantované článkem 17 Listiny základních práv a svobod, jeden ze základních nástrojů demokratické kontroly výkonu veřejné moci. Nicméně v éře pokročilé digitalizace veřejné správy naráží toto právo na limity, které jsou nezbytné pro zajištění bezpečnosti kritických informačních systémů a ochranu soukromí občanů. Specifickým a vysoce citlivým případem jsou žádosti směřující k technické architektuře, bezpečnostním prvkům a stavu přípravy nových technologických řešení.

Informace požadované žadatelem mají charakter citlivých technických informací, proto povinný subjekt musí zvlášť obezřetně vyvažovat mezi veřejným zájmem na transparentnost a veřejným zájmem na bezpečnost, jak bylo již rozebráno výše. Judikatura Ústavního soudu zdůrazňuje princip proporcionality, který vyžaduje, aby omezení práva na informace bylo co nejmenší, avšak dostatečné k naplnění účelu ochrany jiného chráněného zájmu. V oblasti IT architektury je však často nemožné informaci poskytnout jen částečně, neboť i fragmentární znalost technických detailů může útočníkovi posloužit k identifikaci zranitelností.

Pro daný konkrétní případ jsou pak relevantní následující skutečnosti. Nahlížení do KN slouží k elektronickému přístupu k vybraným údajům katastru nemovitostí. Od roku 2021 prošla aplikace zásadními změnami. Z technického hlediska je Nahlížení do KN prezentační vrstvou nad rozsáhlou databází Informačního systému katastru nemovitostí (ISKN). Systém je úzce propojen s dalšími základními registry. Tato provázanost pak vyžaduje aplikaci přísnějších bezpečnostních standardů a omezení přístupu k informacím o samotné architektuře. Předseda má za to, že automatizované vytěžování dat přitom nelze považovat pouze za technický problém (zátěž aplikace), ale za zásadní zásah do práv subjektů údajů ve smyslu zákona

č. 110/2019 Sb., o zpracování osobních údajů a Obecného nařízení o ochraně osobních údajů (GDPR). Bylo tedy na místě, aby úřad, ve snaze minimalizovat dopad tohoto nežádoucího chování s odkazem na § 5 odst. 4 vyhlášky č. 358/2013 Sb., o poskytování údajů z katastru nemovitostí, využil a zavedl technická a aplikační opatření, o čemž byl žadatel v obecné rovině informován. Nicméně zveřejnění konkrétních opatření, jejich řešení, limitů a případně i konfigurace by bylo výrazně ve prospěch tvůrců těchto robotů a mohlo by dojít k značnému snížení efektivity zavedených opatření. Pro úplnost je možné zmínit, že s tím nepochybně souvisí i otázka eventuálního zvýšení finančních nákladů státu v důsledku nutnosti zapojení více lidských zdrojů, resp. zavádění nějakých dalších nových opatření. Úřad jakožto ústřední orgán státní správy je povinen zcela nepochybně prostředky daňových poplatníků využívat s péčí řádného hospodáře.

Předseda považuje odmítnutí informací v posuzované věci s odkazem na § 36 zákona č. 264/2025 Sb., o kybernetické bezpečnosti, za případné a zákonné. Naplnění zákonných podmínek pak spatřuje v tom, že zveřejnění detailních parametrů systému Nahlížení do KN (zejména síťové topologie, verzí software a metod šifrování) představuje vysoké bezpečnostní riziko, neboť by potenciálnímu útočníkovi poskytlo výhody, které mohou vyústit ve snížení efektivity zavedených opatření/postupů v rámci hrozeb a zvýšit riziko vzniku kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů. Za riziko je třeba považovat zejména:

- Znalost vnitřní mapy systému útočníkem
  Umožňuje útočníkovi naplánovat cestu k citlivým datům. Pokud by úřad zveřejnil, jaká konkrétní opatření (rate-limiting, throttling, behaviorální analýza a jiné) používá, používal nebo nepoužívá, de facto by mu tím poskytl mapu obrany a návod, jak systém efektivněji napadnout, popř. mu napomohl odhadnout limity systému. I dílčí informace by útočníkům umožnily odhadnout obranné hranice systému a upravit útoky tak, aby je obešly.
- Využití konkrétních slabin systému útočníkem
  Informace o technické architektuře umožňuje útočníkovi vyhledat již zdokumentované chyby těchto produktů. Útok pak není veden náhodně, ale je přesně zacílen na konkrétní, dosud neopravené zranitelnosti systému.
- Znehodnocení připravovaných ochranných prvků útočníkem
  Detailní popis metod šifrování a chystaných bezpečnostních změn dává útočníkovi možnost vyvinout metody k jejich prolomení s předstihem. Informace o logickém či fyzickém oddělení částí aplikace (viz bod 3 písm. c žádosti) jsou pak informacemi o bezpečnostním designu systému. Jejich zveřejnění by vedlo ke zvýšení rizika v rámci cílených útoků na citlivé segmenty systému. Pokud by úřad potvrdil, na základě jakých konkrétních dat (IP, geolokalizace, ASN) identifikoval porušování podmínek (viz bod 7 písm. a žádosti), dává tím útočníkům návod, na jaká data/ukazatele je potřeba minimalizovat dopad jejich činnosti a jak příště detekci obejít nebo způsobit prodlevu v nasazení/konfiguraci ochranných prvků. Data o tom, jaký typ provozu byl vyhodnocen jako škodlivý, jsou samy o sobě citlivým údajem, u kterého existuje důvodná obava ze zneužití pro možnou přípravu další vlny útoků.
- Zneužití informací o procesu vyhodnocování a následném (ne)zavedení konkrétních technických prvků útočníkem
  Tyto informace jsou integrální součástí bezpečnostní strategie úřadu. Jejich zveřejnění by odhalilo slabá místa v infrastruktuře, odhalení kapacity a přesnosti monitorovacích nástrojů a v konečném důsledku zvýšilo riziko vzniku kybernetických bezpečnostních událostí/incidentů.

Zveřejnění technické dokumentace a konfiguračních detailů by fakticky znamenalo poskytnutí návodu k narušení integrity a dostupnosti informační infrastruktury státu, odhalilo by konkrétní prvky bezpečnostního designu, provozní limity a metody detekce, které jsou součástí bezpečnostní dokumentace. Ochrana těchto informací je nezbytná pro zajištění kybernetické bezpečnosti a ochranu osobních údajů v souladu s platnými právními předpisy. Údaje

o architektuře a škálovatelnosti jsou součástí bezpečnostní dokumentace podle zákona č. 264/2025 Sb., o kybernetické bezpečnosti a prováděcích předpisů. Tato dokumentace je vedena v režimu, který vylučuje její zveřejnění, protože obsahuje souhrn slabých míst a způsobů jejich ochrany.

Předseda na základě námitek žadatele přezkoumal zákonnost provedeného testu proporcionality, resp. závažnosti veřejného zájmu nad právem na informace, a dospěl ke stejnému závěru jako úřad v prvé instanci. Požadované informace o architektuře aplikace, technických datech, analýzách provozu a limitech systému představují citlivou dokumentaci, ze které vychází zavedená bezpečnostní opatření. Jejich zpřístupnění, a to i částečné, by umožnilo třetím osobám identifikovat meze odolnosti systému a adaptovat útočné techniky tak, aby obešly stávající detekční mechanismy. V zájmu zachování funkčnosti Informačního systému katastru nemovitostí jako celku proto převažuje zájem na ochraně bezpečnosti nad právem na informace.

Na základě výše uvedeného lze uzavřít, že úřad jako povinný subjekt posoudil možnost poskytnutí informací v obecné, agregované nebo zobecněné podobě. Tam, kde to bylo možné bez ohrožení bezpečnosti, byly žadateli poskytnuty obecné informace potvrzující, že technická opatření byla prováděna. U informací, jejichž zveřejnění by reálně zvýšilo riziko úspěšnosti útoku nebo odhalilo slabá místa, bylo odmítnutí nezbytné a přiměřené. Posouzení bylo individuální vzhledem k povaze každého požadovaného údaje a k rizikům spojeným s jeho zveřejněním. Námitky žadatele týkající se nepřezkoumatelnosti rozhodnutí, extenzivního výkladu právních předpisů a nedostatečného testu proporcionality nejsou důvodné.

Předseda tak poté, co přezkoumal ve smyslu § 89 odst. 2 ,ve spojení s § 152 odst. 5 správního řádu, soulad napadeného rozhodnutí a řízení, které mu předcházelo, s právními předpisy, jakož i správnost napadeného rozhodnutí v rozsahu žadatelem podaných námitek, shledal, že se nejedná o rozhodnutí nezákonné ani nesprávné a nejsou tedy dány důvody pro jeho zrušení či změnu. Podaný rozklad z výše popsaných důvodů proto považuje za nedůvodný a jako takový jej zamítá.

Poučení:

Proti tomuto rozhodnutí se podle ustanovení § 91 odst. 1 správního řádu ve spojení s § 152 odst. 5 téhož zákona nelze odvolat ani podat rozklad.

Ing. Karel Štencel
podepsáno elektronicky

Oznamuje se doručením: Jan Harsa, ID DS: [redacted]

Na vědomí: Český úřad zeměměřický a katastrální, kancelář předsedy