KRAJSKÝ SOUD V ČESKÝCH BUDĚJOVICÍCH

Zátkovo nábřeží 2, 370 84 České Budějovice

tel.: 389 018 111, fax: 389 018 500, e-mail: podatelna@ksoud.cbu.justice.cz, IDDS: 832abay

Rozhodnutí

Krajský soud v Českých Budějovicích jako povinný subjekt podle § 2 odst. 1 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, rozhodl předsedkyní soudu Mgr. Martinou Flanderovou, PhD., o žádosti [redacted], nar. [redacted], bytem [redacted], ze dne 15. 6. 2025 (dále jen „žádost“) na základě § 15 odst. 1 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění účinném ke dni podání žádosti (dále jen „InfZ“) takto:

I. Žádost ze dne 15. 6. 2025, v níž žadatel požadoval v bodech pod jednotlivými odrážkami informace
„-používá váš soud softwarové nástroje pro anonymizaci dokumentů?
-pokud soud SW používá, o jaký software/jaké softwary se jedná?
-pokud soud SW používá, jak dlouho váš soud SW pro anonymizaci používá?
-pokud soud SW používá, jaká se dodavatelem SW uváděná spolehlivost anonymizace?
-pokud soud SW používá, vede si soud vlastní statistiku spolehlivosti SW a pokud ano, jaké úrovně spolehlivosti SW podle soudu dosahuje (vyjádřete % na roční bázi - za rok 2024, případně podle toho, co soud sleduje, pokud to sledujete).“
se podle § 15 odst. 1 InfZ v části „*pokud soud SW používá, o jaký software/jaké softwary se jedná?“* odmítá na na základě § 11 odst. 1 písm. d) InfZ, neboťposkytnutí této informace významně nebo přímo ohrožuje účinnost bezpečnostního opatření stanoveného na základě zvláštního předpisu pro účel ochrany bezpečnosti osob, majetku a veřejného pořádku. Informace k softwaru a jeho technickým parametrům nelze sdělit, neboť jde o citlivé informace z pohledu kybernetické bezpečnosti.

Odůvodnění

1. Dne 15. 6. 2025 byla Krajskému soudu v Českých Budějovicích (dále jen „povinný subjekt“) doručena do datové schránky žádost žadatele [redacted], nar. [redacted], bytem [redacted], [redacted], (dále jen „žadatel), o poskytnutí informací dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění
„-používá váš soud softwarové nástroje pro anonymizaci dokumentů?
-pokud soud SW používá, o jaký software/jaké softwary se jedná?
-pokud soud SW používá, jak dlouho váš soud SW pro anonymizaci používá?
-pokud soud SW používá, jaká se dodavatelem SW uváděná spolehlivost anonymizace?
-pokud soud SW používá, vede si soud vlastní statistiku spolehlivosti SW a pokud ano, jaké úrovně spolehlivosti SW podle soudu dosahuje (vyjádřete % na roční bázi - za rok 2024, případně podle toho, co soud sleduje, pokud to sledujete).“
Vzhledem k tomu, že doručená žádost neobsahovala úplné údaje týkající se osoby žadatele podle § 14 odst. 2) InfZ, a to datum narození, adresu místa trvalého pobytu, byl žadatel vyzván soudem k doplnění. K výzvě soudu byla žádost doplněna 23. 6. 2025.

2. O žádosti bylo Krajským soudem v Českých Budějovicích rozhodnuto 27. června 2025. Části žádosti bylo vyhověno, č.j. Si 141/2025-6. Část žádosti byla podle § 15 odst. 1 InfZ krajským soudem odmítnuta na na základě § 11 odst. 1 písm. d) InfZ, neboťposkytnutí informace významně nebo přímo ohrožuje účinnost bezpečnostního opatření stanoveného na základě zvláštního předpisu pro účel ochrany bezpečnosti osob, majetku a veřejného pořádku.

Požadované informace k softwaru a jeho technickým parametrům nelze sdělit, neboť jde o citlivé informace z pohledu kybernetické bezpečnosti. Rozhodnutí bylo vydáno dne 27. června 2025, č.j. Si 141/2025 – 7.

3. Proti citovanému rozhodnutí podal žadatel v zákonné lhůtě odvolání, které bylo krajskému soudu doručeno do datové schránky 1. 7. 2025. O odvolání rozhodlo Ministerstvo spravedlnosti 21. 7. 2025, č.j. MSP-548/2025-OSV-OSV/2. Rozhodnutí krajského soudu bylo zrušeno a věc vrácena k novému projednání.

4. Krajský soud jako povinný subjekt přistoupil po doručení rozhodnutí k novému projednání žádosti. Poukazuje na aplikovaná zákonná ustanovení. Podle § 15 odst. 1 InfZ pokud povinný subjekt žádosti, byť i jen zčásti, nevyhoví, vydá ve lhůtě pro vyřízení žádosti rozhodnutí o odmítnutí žádosti, popřípadě o odmítnutí části žádosti (dále jen „rozhodnutí o odmítnutí žádosti"), s výjimkou případů, kdy se žádost odloží. Podle § 11 odst. 1 písm. d) InfZ povinné subjekty neposkytnou informace, jejichž poskytnutí významně nebo přímo ohrožuje účinnost bezpečnostního opatření stanoveného na základě zvláštního předpisu pro účel ochrany bezpečnosti osob, majetku a veřejného pořádku.

5. Povinný subjekt se opakovaně zabýval otázkami žadatele vymezenými v bodě 1., 3. – 6. (odrážka) žádosti, které se týkaly poskytnutí informací
„-používá váš soud softwarové nástroje pro anonymizaci dokumentů?
-pokud soud SW používá, jak dlouho váš soud SW pro anonymizaci používá?
-pokud soud SW používá, jaká se dodavatelem SW uváděná spolehlivost anonymizace?
-pokud soud SW používá, vede si soud vlastní statistiku spolehlivosti SW a pokud ano, jaké úrovně
- spolehlivosti SW podle soudu dosahuje (vyjádřete % na roční bázi - za rok 2024, případně podle toho, co soud sleduje, pokud to sledujete).“
Této části žádosti bylo vyhověno 31. 7. 2025 přípisem č.j. Si 141/2025 – 21.

6. Následně se povinný subjekt zabýval otázkou žadatele vymezenou v bodě 2. žádosti týkající se poskytnutí informace
-„pokud soud SW používá, o jaký software/jaké softwary se jedná?
a došel k závěru, že tyto požadované informace k softwaru a jeho technickým parametrům nelze sdělit, neboť jde o citlivé informace z pohledu kybernetické bezpečnosti.

7. Ustanovení § 11 odst. 1 písm. d) zák. o svobodném přístupu k informacím směřuje k ochraně účinnosti bezpečnostních opatření stanovených na základě zvláštního předpisu pro účel ochrany bezpečnosti osob, majetku a veřejného pořádku. Pojem „bezpečnostní opatření“ je neurčitým právním pojmem. Poskytnutím informace může být ohroženo i bezpečnostní opatření soukromé. V praxi se bude jednat o informace, které sice nejsou utajované, ale i přesto jsou citlivé povahy a není žádoucí, aby vešly v obecnou známost. Například půjde o detaily ostrahy objektů, strategické a taktické postupy bezpečnostních sborů, informace, jejichž zveřejnění by mohlo ohrozit kybernetickou bezpečnost atd. Aby toto ustanovení nemohlo být nadužíváno či zneužíváno, musí jít o opatření, které má svůj podklad v zákoně. Například půjde o § 4 zákona č. 181/2014 Sb., o kybernetické bezpečnosti; § 5 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, § 22 až 26 zákona č. 61/1988 Sb., o hornické činnosti, výbušninách a o státní báňské správě; § 3 zákona č. 137/2001 Sb., o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením; § 5 odst. 1 písm. a) zákona č. 133/1985 Sb., o požární ochraně; čl. 32 odst. 1 GDPR. apod.

Shodu s prvopisem potvrzuje Věra Křesinová.

8. § 11 odst. 1 písm. d) InfZ byl zákonodárcem přijat za účelem vytvoření výluk z práva na informace, což podporuje též důvodová zpráva. Pojem bezpečnostní opatření je pojmem, který dopadá na širokou paletu konkrétních případů, a je nutné je v daném kontextu vykládat tak, aby poskytnutím informace nedošlo k nenapravitelnému ohrožení účinnosti bezpečnostního opatření. Informace, nemá-li být poskytnuta, musí významně nebo přímo ohrožovat účinnost bezpečnostního opatření na základě zvláštního předpisu pro účely ochrany bezpečnosti osob, majetku a veřejného pořádku. V daném případě je tímto zvláštním předpisem zákon o kybernetické bezpečnosti a další předpisy v oblasti kybernetické bezpečnosti, například vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „Vyhláška č. 82/2018 Sb.“). Právní předpisy v oblasti kybernetické bezpečnosti jsou přijaty právě za účelem ochrany bezpečnosti osob, majetku a veřejného pořádku.

9. Dle instrukce MS č. 5/2022 ze dne 30. června 2022, č. j. 115/2022-OI-SP/1 o zajištění bezpečnosti informací v prostředí informačních a komunikačních technologií resortu spravedlnosti a bezpečnostních politik, které jsou její součástí, musí být na každé složce justice – tedy i na našem KS provedena identifikace, evidence, klasifikace a hodnocení všech aktiv, mj. i z pohledu důvěrnosti. Jelikož veškeré agendové informační systémy KS jsou klasifikovány jako VIS (významný informační systém dle zatím stále platného ZoKB č. 181/2014 Sb.), je i veškerý podpůrný SW používaný v souvislosti s těmito aktivy klasifikován stupněm DUV-C, tedy citlivá informace. Není tak možné zveřejňovat jakékoli informace o používaných SW, kam patří i SW pro anonymizaci. Obecně má toto hodnocení opodstatnění. Jakákoli informace o používaných SW dává potencionálnímu útočníkovi výhodu – v případě znalosti SW může zneužít případných slabých míst apod. Důvod, proč byly informace o všech používaných SW aktivech na krajském soudu takto klasifikovány, vychází z analýzy rizik, kde bylo identifikováno riziko zneužití zranitelností, a to u jakéhokoli používaného SW. Obecně shrnuto, jakýkoli i méně významný SW obsahuje veřejně známé i neznámé zranitelnosti, které může potencionální útočník zneužít a skrze tyto zranitelnosti útočit i na významná aktiva v síti. Jako jedno z opatření ke snížení tohoto rizika byl přijat právě zvýšený stupeň klasifikace z hlediska důvěrnosti u používaných nástrojů. A byl takto klasifikován veškerý SW, v analýze rizik nerozlišujeme používané SW na více skupin – méně, nebo více důvěrná.

10. Ústavní soud ve svém nálezu ze dne 17. 10. 2017, sp. zn. IV. ÚS 1378/16, konstatoval, že: *"Právo na informace ve veřejném zájmu není absolutní; pokud jeho výkon zasahuje do práva na ochranu soukromého života, chráněného článkem 10 Listiny a článkem 8 Úmluvy, je nutno v každém jednotlivém případě všechna tato práva poměřovat, a zajistit mezi nimi spravedlivou rovnováhu, neboť jde o práva rovnocenná. Takovou povinnost mají i všechny subjekty aplikující relevantní právní úpravu, obsaženou v zákoně o svobodném přístupu k informacím, tj. osoby poskytující informaci, správní orgány a soudy v systému správního soudnictví. Žádným zákonem nelze abstraktně vyloučit ochranu základních práv a svobod zaručenou ústavním pořádkem. V každém jednotlivém případě střetu ústavně zaručených práv musejí soudy a jiné orgány veřejné moci zvážit význam a intenzitu dotčených práv."*

11. Při řešení konfliktu mezi základními lidskými právy a svobodami je využíván tzv. test proporcionality, jehož výsledkem je závěr o nutnosti upřednostnit jedno z konkurujících si subjektivních práv při současném minimálním omezení práva druhého, skládající se ze tří kritérií, která byla definována v nálezu Ústavního soudu ze dne 13. 8. 2002, sp. zn. Pl. ÚS 3/02: *„První z nich je princip způsobilosti naplnění účelu (nebo také vhodnosti), dle něhož musí být příslušné opatření vůbec schopno dosáhnout zamýšleného cíle, jímž je ochrana jiného základního práva nebo veřejného statku. Dále se pak jedná o princip potřebnosti, dle něhož je povoleno použití pouze nejšetrnějšího - ve vztahu k*

dotčeným základním právům a svobodám - z více možných prostředků. Třetím principem je princip přiměřenosti (v užším smyslu), dle kterého újma na základním právu nesmí být nepřiměřená ve vztahu k zamýšlenému cíli, tj. opatření omezující základní lidská práva a svobody nesmějí, jde-li o kolizi základního práva či svobody s veřejným zájmem, svými negativními důsledky přesahovat pozitiva, která představuje veřejný zájem na těchto opatřeních."

12. V souvislosti s aktuální judikaturou musí krajský soud jako povinná osoba provést u všech zákonných důvodů test proporcionality. Judikaturou byla dovozena základní kritéria tohoto posuzování, kdy je třeba zohlednit vhodnost, potřebnost a porovnat závažnost obou v kolizi stojících základních práv. K otázce vhodnosti, tedy zda lze tímto postupem docílit ochrany kybernetické bezpečnosti, žalovaný uzavřel, že jednoznačně ano. Naopak poskytnutí požadovaných informací má potenciál tuto bezpečnost ohrozit. K otázce potřebnosti, tedy zda by cíle nemohlo být dosaženo bez zasažení do základních práv a svobod, žalovaný uvedl, že nikoliv. Jakmile by byly jednou požadované informace veřejné, šlo by SW ochránit pouze velmi obtížně, resp. tento cíl by byl za stávající situace téměř nemožný. K otázce poměřování závažnosti obou v kolizi stojících základních práv žalovaný uzavřel, že informace, které o SW mohly být poskytnuty, poskytnuty byly. Poskytnuta nebyla pouze odpověd na otázku č. 2. odrážka, kde bylo vyhodnoceno, že její poskytnutí není z bezpečnostních důvodů možné.

13. K omezení práva na informace bylo tedy přistoupeno pouze v minimálním rozsahu, a to tam, kde bylo nebezpečí ohrožení systému kritické infrastruktury vyhodnoceno jako vysoké. Není možné nahradit omezení práva na informace jiným opatřením, které umožní uchránit zájem na bezpečnosti SW u krajského soudu. V tomto rozsahu opatření spočívající v omezení práva na informace je rovněž vhodné (způsobilé k naplnění ochrany právem chráněného zájmu) a při zohlednění povahy a významu SW, jakož i zvýšeném zájmu na jeho bezpečnosti, je proto třeba jej upřednostnit před realizací práva na informace. Poskytnutí požadovaných informací by ve vzájemné propojenosti oslabily jednotlivé prvky SW, neboť by žadatel, resp. veřejnost, po zveřejnění poskytnutých informací podle § 5 odst. 3 InfZ věděli o potenciálních rizicích zabezpečení SW. Vedlo by to k celé řadě dalších dotazů (např. na antiviry) a vedlo by to k dalšímu vysvětlování proč informace o některých SW prozradíme a o jiných ne, a jak to máme rozděleno, řízeno atd. Takovéto informace nemůže povinný subjekt poskytnout.

14. Povinný subjekt proto podle § 15 odst. 1 InfZ ve spojení s § 11 odst. 1 písm. d) InfZ odmítá poskytnout informace specifikované v žádosti.

Poučení:

Proti tomuto rozhodnutí lze podat odvolání do 15 dnů ode dne doručení Ministerstvu spravedlnosti ČR prostřednictvím Krajského soudu v Českých Budějovicích.

V Českých Budějovicích 31. července 2025

Mgr. Martina Flanderová, Ph.D. v. r.
předsedkyně Krajského soudu v Českých Budějovicích

Shodu s prvopisem potvrzuje Věra Křesinová.