

DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

SEKCE REGISTRŮ, ROZHRANÍ A SLUŽEB EGOVERNMENTU



DIAPX007BG3E
PRVOTNÍ IDENTIFIKAČNÍ KÓD

ADRESÁT

(osobní údaje anonymizovány)

NAŠE ČÍSLO JEDNACÍ
DIA- 4660-3/OSEG-2026

K VAŠEMU Č. J.
X

POČET PŘÍLOH
1

MÍSTO ODESLÁNÍ / DNE
Praha / datum uvedeno v doložce
elektronického podpisu

Odpověď na žádost podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím

Digitální a informační agentura, sekce registrů, rozhraní a služeb eGovernmentu (dále také „Agentura“) obdržela dne 5. března 2026 žádost podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím (dále také „InfZ“), podanou (osobní údaje anonymizovány), jakožto žadatelem (dále také „žadatel“).

Žadatel požaduje následující informaci:

Podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, žádám o poskytnutí kompletního textu analýzy příčin technických problémů aplikace eDoklady v průběhu sněmovních voleb v říjnu 2025, kterou Digitální a informační agentura na podzim 2025 předložila vládě ČR. Žádám o doručení textu analýzy v digitální podobě do mé datové schránky.

V reakci na žádost Agentura **poskytuje** žadateli dokument „Incident eDoklady 3.-4.10.2025“ a to s výjimkou částí, které jsou odstraněny (znečitelněny). Dokument je přiložen k této odpovědi.

V reakci na žádost, pokud jde o části dokumentu „Incident eDoklady 3.-4.10.2025“, které jsou odstraněny (znečitelněny), Agentura jakožto povinný subjekt podle § 2 InfZ ve spojení s § 11 odst. 1 písm. d), 15 odst. 1 a § 20 odst. 4 písm. a) InfZ, § 36 zákona č. 264/2025 Sb., o kybernetické bezpečnosti, a zákona č. 500/2004 Sb., správního řádu, vydává

rozhodnutí,

jímž se žádost o informace v rozsahu částí dokumentu „Incident eDoklady 3.-4.10.2025“, které jsou odstraněny (znečitelněny), **odmítá**.

Odůvodnění:

Digitální a informační agentura, sekce registrů, rozhraní a služeb eGovernmentu (dále také „Agentura“) obdržela dne 5. března 2026 žádost podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím (dále také „InfZ“), podanou (osobní údaje anonymizovány), jakožto žadatelem.

DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

Žadatel požaduje následující informaci:

Podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, žádám o poskytnutí kompletního textu analýzy příčin technických problémů aplikace eDoklady v průběhu sněmovních voleb v říjnu 2025, kterou Digitální a informační agentura na podzim 2025 předložila vládě ČR. Žádám o doručení textu analýzy v digitální podobě do mé datové schránky.

Z důvodu konzultace mezi více útvary Agentury, a sice odborem služeb eGovernmentu, odborem právním a legislativním, odborem tisku a PR a vedením Agentury, prodloužila Agentura lhůtu k vyřízení žádosti podle § 14 odst. 6 písm. c) InfZ o 10 dnů, o čemž byl žadatel vyrozuměn vyrozuměním ze dne 17. března 2026, č. j. DIA-4460-2/OSEG-2026.

V reakci na žádost Agentura poskytla žadateli dokument „Incident eDoklady 3.-4.10.2025“ a to s výjimkou částí, které jsou odstraněny (znečitelněny), jak je uvedeno výše.

Pokud jde o částí dokumentu „Incident eDoklady 3.-4.10.2025“, které jsou odstraněny (znečitelněny) a tedy v tomto rozsahu došlo k odmítnutí žádosti, Agentura rozhodla o odmítnutí z důvodu (i) možného ohrožení zajišťování kybernetické bezpečnosti, jakož i souvisejícího důvodu (ii) významného ohrožení účinnosti bezpečnostního opatření stanoveného na základě zvláštního předpisu pro účel ochrany bezpečnosti osob, majetku a veřejného pořádku nebo připravenosti na krizové situace a jejich řešení.

Podle § 36 zákona o kybernetické bezpečnosti platí, že informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti, se podle právních předpisů upravujících svobodný přístup k informacím neposkytují.

V neposkytnutých částech dokumentu jsou obsaženy informace o:

1. vztazích mezi Agenturou a dalšími subjekty ohledně systémů zajišťujících fungování systému eDoklady, jakož i ohledně dalších systémů spravovaných či provozovaných Agenturou nebo dalšími subjekty;
2. vztazích mezi systémy spravovanými či provozovanými Agenturou a mezi systémy spravovanými či provozovanými dalšími subjekty;
3. parametrech testování systému eDoklady a jeho průběhu;
4. organizačním a personálním zajištění, pokud jde o činnosti ve vztahu k systému eDoklady, včetně předpokládaného budoucího vývoje;
5. organizačnímu, personálnímu a technickému zajištění, pokud jde o činnosti ve vztahu k jiným systémům, včetně předpokládaného budoucího vývoje;
6. konkrétní údaje o využívání systému eDoklady;
7. konkrétní údaje o událostech v systému eDoklady a popis jejich proběhlého řešení;
8. architekturu systému eDoklady; a
9. již přijatých a navrhovaných opatřeních přijatých k zajištění dostupnosti systému eDoklady.

Agentura dospěla k závěru, že znalost informací výše uvedeného charakteru, ať již jednotlivě, ve vzájemném souhrnu či ve spojení s dalšími informacemi, by umožnila naplánovat úspěšný kybernetický útok nebo jiný incident či více útoků nebo incidentů, ať již z hlediska volby konkrétních použitých mechanismů ze strany útočníka, oblastí, na které se má být útočeno, časového situování útoku, a reakce útočníka na obranná opatření. Možné ohrožení je dále zvýšeno tím, že informace se netýkají jen systému eDoklady a Agentury, ale též jiných subjektů a systémů, které spravuje či provozuje Agentura nebo jiné subjekty. Možné ohrožení je dále zvýšeno tím, že podle § 5 odst. 3 InfZ je Agentura povinna do 15 dnů od poskytnutí informací na žádost zveřejnit poskytnuté informace způsobem umožňujícím dálkový přístup. Agentura tedy fakticky neposkytuje informace toliko žadateli, nýbrž je

DIGITÁLNÍ A INFORMAČNÍ AGENTURA

zveřejňuje a požadované informace by se tak staly dostupné každému. Postup, kdy by informace byly poskytnuty toliko žadateli, avšak zveřejněny by nebyly, InfZ nepřipouští.

Podle § 11 odst. 1 písm. d) InfZ platí, že povinný subjekt (zde Agentura) může omezit poskytnutí informace, pokud její poskytnutí významně nebo přímo ohrožuje účinnost bezpečnostního opatření stanoveného na základě zvláštního předpisu pro účel ochrany bezpečnosti osob, majetku a veřejného pořádku nebo připravenosti na krizové situace a jejich řešení.

Pokud jde o bezpečnostní opatření stanovená zvláštním právním předpisem, jak o nich zmíněný § 11 odst. 1 písm. d) InfZ hovoří (pojmem „zvláštní právní předpis“ je v tomto ustanovení míněn jiný předpis než InfZ), Agentura přijímá bezpečnostní opatření jakožto tzv. poskytovatel regulované služby v tzv. režimu vyšších povinností, podle § 13 již zmíněného zákona o kybernetické bezpečnosti. Agentura nicméně neplní povinnosti jen z důvodu ochrany kybernetické bezpečnosti jako takové, jak je již podrobně popsáno výše, plní též povinnosti směřující k ochraně kritické infrastruktury, neboť je subjektem kritické infrastruktury, kterou spravuje, jak to Agentuře ukládá zákon č. 266/2025 Sb., o kritické infrastruktuře. Neposkytnuté informace se týkají systémů, které tvoří součást kritické infrastruktury, a které poskytují služby napříč celou veřejnou správou včetně např. ozbrojených sil či bezpečnostních sborů, obsahují osobní údaje fyzických osob nebo podporují komunikaci mezi systémy jiných orgánů veřejné moci navzájem. Poskytnutí takových informací by z důvodů, které byly uvedeny výše, ohrozilo účinnost bezpečnostních opatření stanovených na základě zvláštního předpisu (zde zákona o kybernetické bezpečnosti a zákona o kritické infrastruktuře) pro účel ochrany bezpečnosti osob, majetku a veřejného pořádku nebo připravenosti na krizové situace a jejich řešení.

Mezi opatření, zejména pokud jde o ochranu majetku, ale též o ochranu bezpečnosti osob či veřejného pořádku, patří též opatření k prevenci škod. Mezi zvláštní právní předpisy, které taková opatření Agentuře ukládají, patří nejen již zmíněný zákon o kybernetické bezpečnosti a zákon o kritické infrastruktuře, ale též např. § 45 odst. 1 zákona č. 218/2000 Sb., o rozpočtových pravidlech, podle kterého jsou organizační složky státu povinny plnit své úkoly nejehospodárnějším způsobem, dále také § 14 odst. 1 zákona č. 219/2000 Sb., o majetku České republiky a jejím vystupování v právních vztazích, podle něhož musí být majetek využíván mj. hospodárně k plnění funkcí státu a k výkonu stanovených činností, nebo ustanovení § 2900 a násl. zákona č. 89/2012 Sb. občanského zákoníku, ukládající obecnou povinnost k prevenci škod.

Pokud jde o ochranu bezpečnosti osob, majetku a veřejného pořádku nebo připravenosti na krizové situace a jejich řešení, riziko spojené s poskytnutím požadované informace není čistě kyberneticko-bezpečnostní, popř. finanční, ale s ohledem na výše uvedené představuje hrozba či dokonce provedení kybernetického útoku riziko (záměrné) snížení důvěry veřejnosti ve stát, jeho instituce a schopnost státu zajišťovat bezpečnost. To platí zejména v kontextu aktuální geopolitické situace.

Agentura shrnuje, že poskytnutí požadované informace by mohlo ohrozit zajišťování kybernetické bezpečnosti, resp. by významně ohrozilo účinnost bezpečnostního opatření stanoveného na základě zvláštního předpisu pro účel ochrany bezpečnosti osob, majetku a veřejného pořádku nebo připravenosti na krizové situace a jejich řešení, a proto rozhodla o odmítnutí žádosti, jak je uvedeno ve výroku.

Poučení:

Proti rozhodnutí o odmítnutí žádosti lze podat podle § 16 odst. 1 InfZ ve spojení s § 152 odst. 1 správního řádu, rozklad. Rozklad je možné podat do 15 dnů ode dne doručení rozhodnutí (§ 16 odst. 3 InfZ), a to k Agentuře, nejlépe cestou odboru služeb eGovernmentu, o rozkladu rozhoduje ředitel Agentury (§ 16 odst. 3 InfZ ve spojení s § 152 odst. 2 správního řádu).

S pozdravem

DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

Mgr. Denisa Škantová

ŘEDITELKA SEKCE REGISTRU, ROZHRANÍ A SLUŽEB EGOVERNMENTU