Digitální a informační agentura

DIAPX007YFJ2
PRVOTNÍ IDENTIFIKÁTOR

ODBOR ARCHITEKTURY

ADRESÁT
(osobní údaje anonymizovány)

NAŠE ČÍSLO JEDNACÍ
DIA- 10909-3/OHA-2026

VYŘIZUJE
Ing. Tomáš Šedivec

E-MAIL
tomas.sedivec@dia.gov.cz

K VAŠEMU Č. J.
x

POČET PŘÍLOH
x

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

Částečné poskytnutí informace, částečné odložení žádosti, částečné odmítnutí žádosti

Digitální a informační agentura, sekce Hlavního architekta eGovernmentu (dále také „Agentura“), obdržela dne 27. června 2026 žádost o poskytnutí informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále jen „InfZ“), podanou (osobní údaje anonymizovány), jakožto žadatelem (dále také „žadatel“).

Žadatel požádal o následující informace:

Úvodem si dovoluji uvést stručný kontext. Oblasti informačních technologií se profesně věnuji od roku 1989, od roku 2000 pak zejména kybernetické bezpečnosti. Z této dlouholeté praxe vyplývá moje odpovědnost za bezpečnost a kontinuitu informačních systémů, o které pečuji. Událost z 12. června 2026, kdy byl provozovatel pokročilého modelu umělé inteligence nucen na základě jednostranné direktivy orgánu třetího státu plošně znepřístupnit službu všem zákazníkům včetně evropských, pro mě představuje konkrétní precedens. Považuji proto za odpovědné porozumět tomu, zda a jak je toto riziko řešeno na úrovni státu.
Navazuji přitom na odpověď Národního úřadu pro kybernetickou a informační bezpečnost ze dne 25. června 2026, č. j. 18442/2026-NÚKIB-E/210, z níž vyplynulo, že NÚKIB nedisponuje uceleným materiálem k riziku závislosti na službách poskytovaných subjekty mimo EU a že samostatný plán kontinuity pro případ náhlé nedostupnosti zahraničních služeb na národní úrovni neexistuje. Vzhledem k působnosti DIA ve vztahu k digitální infrastruktuře státu se proto obracím na Vás a žádám o sdělení:

1. *Zda Digitální a informační agentura disponuje analytickými, koncepčními nebo strategickými materiály, které se zabývají rizikem, že kritické digitální služby státu (eGovernment, národní/státní cloud, základní registry) závislé na poskytovatelích pod jurisdikcí států mimo Evropskou unii by mohly být jednostranně omezeny nebo znepřístupněny rozhodnutím orgánu cizího státu, a to včetně státu spojeneckého.*
2. *Zda na úrovni infrastruktury státu (nikoli pouze v rovině povinností přenesených na jednotlivé subjekty podle zákona č. 264/2025 Sb.) existují plány kontinuity či havarijní scénáře pro případ náhlé nedostupnosti služeb zahraničních poskytovatelů. Pokud ano, žádám o jejich poskytnutí, případně o odkaz na veřejně dostupné verze.*
3. *Zda strategie státního/národního cloudu obsahuje požadavek nebo harmonogram pro zajištění suverénních (v jurisdikci ČR/EU) alternativ ke kritickým službám, včetně případných migračních či „exit“ plánů od zahraničních poskytovatelů.*

4. *Zda DIA provedla či eviduje přehled, které kritické služby státu jsou v současnosti provozovány na infrastruktuře zahraničních poskytovatelů (tzv. hyperscalerů) nebo zahraničních službách umělé inteligence.*
5. *Pokud uvedená agenda nespadá do působnosti DIA, který orgán či instituci považuje DIA za příslušnou k řešení strategické a kontinuitní dimenze tohoto rizika.*

V reakci na dotaz 3. Agentura **poskytuje** následující informaci:

Uvedenou problematiku upravuje Hlava VI zákona č. 365/2000 Sb., o informačních systémech veřejné správy, která zavedla tzv. poskytovatele státního cloud computingu (§ 6i odst. 1 písm. a) zmíněného zákona) a zavedla na jiných místech zmíněné Hlavy VI povinnosti související s poskytovatelem státního cloud computingu (např. § 6m odst. 2 zmíněného zákona).

V reakci na dotaz 2. v rozsahu, v jakém se netýká působnosti Agentury, Agentura **žádost odkládá**, podle § 14 odst. 5 InfZ. Podle tohoto ustanovení platí, že pokud se požadované informace nevztahují k působnosti povinného subjektu (zde Agentury), žádost se odloží. Důvodem pro toto odložení je, že Agentura nemá ve vztahu k oblastem, jichž se týká žádost, žádnou koordinační, strategickou nebo jinou podobnou úlohu vůči jiným orgánům a odpovídá tedy jen za sebe.

V reakci na dotazy 1., 4. a 5., a v reakci na dotaz 2. v rozsahu, v jakém spadá do působnosti Agentury, Agentura jakožto povinný subjekt podle § 2 InfZ ve spojení s § 2 odst. 4, § 11 odst. 1 písm. d), 15 odst. 1 a § 20 odst. 4 písm. a) InfZ, zákona č. 500/2004 Sb., správního řádu, a § 36 zákona č. 264/2025 Sb., o kybernetické bezpečnosti, vydává

rozhodnutí,

jímž se žádost o informace v rozsahu dotazů 1., 4. a 5., a dotazu 2. v rozsahu, v jakém spadá do působnosti Agentury, **odmítá**.

Odůvodnění:

Digitální a informační agentura, sekce Hlavního architekta eGovernmentu (dále také „Agentura“), obdržela dne 27. června 2026 žádost o poskytnutí informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále jen „InfZ“), podanou (osobní údaje anonymizovány), jakožto žadatelem (dále také „žadatel“).

Úvodem si dovoluji uvést stručný kontext. Oblasti informačních technologií se profesně věnuji od roku 1989, od roku 2000 pak zejména kybernetické bezpečnosti. Z této dlouholeté praxe vyplývá moje odpovědnost za bezpečnost a kontinuitu informačních systémů, o které pečuji. Událost z 12. června 2026, kdy byl provozovatel pokročilého modelu umělé inteligence nucen na základě jednostranné direktivy orgánu třetího státu plošně znepřístupnit službu všem zákazníkům včetně evropských, pro mě představuje konkrétní precedens. Považuji proto za odpovědné porozumět tomu, zda a jak je toto riziko řešeno na úrovni státu.
Navazuji přitom na odpověď Národního úřadu pro kybernetickou a informační bezpečnost ze dne 25. června 2026, č. j. 18442/2026-NÚKIB-E/210, z níž vyplynulo, že NÚKIB nedisponuje uceleným materiálem k riziku závislosti na službách poskytovaných subjekty mimo EU a že samostatný plán kontinuity pro případ náhlé nedostupnosti zahraničních služeb na národní úrovni neexistuje. Vzhledem k působnosti DIA ve vztahu k digitální infrastruktuře státu se proto obracím na Vás a žádám o sdělení:

1. *Zda Digitální a informační agentura disponuje analytickými, koncepčními nebo strategickými materiály, které se zabývají rizikem, že kritické digitální služby státu (eGovernment, národní/státní cloud, základní registry) závislé na poskytovatelích pod jurisdikcí států mimo*

Evropskou unii by mohly být jednostranně omezeny nebo znepřístupněny rozhodnutím orgánu cizího státu, a to včetně státu spojeneckého.

2. *Zda na úrovni infrastruktury státu (nikoli pouze v rovině povinností přenesených na jednotlivé subjekty podle zákona č. 264/2025 Sb.) existují plány kontinuity či havarijní scénáře pro případ náhlé nedostupnosti služeb zahraničních poskytovatelů. Pokud ano, žádám o jejich poskytnutí, případně o odkaz na veřejně dostupné verze.*
3. *Zda strategie státního/národního cloudu obsahuje požadavek nebo harmonogram pro zajištění suverénních (v jurisdikci ČR/EU) alternativ ke kritickým službám, včetně případných migračních či „exit" plánů od zahraničních poskytovatelů.*
4. *Zda DIA provedla či eviduje přehled, které kritické služby státu jsou v současnosti provozovány na infrastruktuře zahraničních poskytovatelů (tzv. hyperscalerů) nebo zahraničních službách umělé inteligence.*
5. *Pokud uvedená agenda nespadá do působnosti DIA, který orgán či instituci považuje DIA za příslušnou k řešení strategické a kontinuitní dimenze tohoto rizika.*

Důvody odmítnutí žádosti v rozsahu dotazů 1. až 4. a dotazu 2. v rozsahu, v jakém spadá do působnosti Agentury

Agentura odmítá žádost v nadepsaném rozsahu na základě § 36 zákona o kybernetické bezpečnosti, podle něhož platí, že informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti, se podle právních předpisů upravujících svobodný přístup k informacím neposkytují.

Pokud jde o dotazy žadatele, ve vztahu k nimž bylo o odmítnutí žádosti rozhodnuto, tyto se na první pohled jeví (s výjimkou části dotazu 2.) jako neohrožující, zejména proto, že dotazy jsou jazykově formulovány jako zjišťovací (tj. odpověď dotaz by byla jen „ano" nebo „ne", např. „disponuje" nebo „nedisponuje"). Žadatel nicméně ke každému dotazu uvedl podrobný souhrn témat, které by měly jednotlivé dokumenty obsahovat, v důsledku čehož platí, že ač by odpověď (formou poskytnutí) byla např. jen „disponuje", žadatel by tím fakticky získal podrobný popis obsahu jednotlivých materiálů, a v případě dotazu 2. přímo jejich obsah. Podobný výsledek by nastal i v případě, pokud by odpověď reagovala na jednotlivé části jednotlivých dotazů zvlášť (např. že se zabývají jen znepřístupněním, nikoliv omezením, že se zabývají některými zeměmi mimo Evropskou unii a jinými ne, pokrývají jen některé konkrétní digitální služby státu a jiné nikoliv, že plány kontinuity existují, ale havarijní scénáře např. nikoliv apod., že Agentura provedla přehled v dotazu 4. jen u některých kritických služeb apod. /pozn. jde o ilustrační příklady/).

Z informací, byly-li by takto poskytnuty, by tak získal žadatel podrobný popis o tom, která témata, služby a regiony mimo Evropskou unii dokumenty pokrývají či naopak nepokrývají. Z toho může žadatel (a nejen žadatel, jak je uvedeno dále), usuzovat na to, kde Agentura shledává rizika a jde tedy o zranitelnost, popř. kterými oblasti se Agentura nezabývá (a mohly by tedy být, tentokrát bez vědomí Agentury, rovněž zranitelné). Jinými slovy, informace o tom, že dokument s konkrétním obsahem existuje, anebo i že neexistuje, je rovněž poskytnutím informací s riziky uvedenými v tomto odůvodnění.

Ve vztahu k výše zmíněnému § 36 zákona o kybernetické bezpečnosti Agentura pro úplnost dodává, že ze slov „by mohlo ohrozit" je zřejmé, že zákonodárce stanovil pro uplatnění tohoto ustanovení relativně nízký práh rizika (není použito např. „ohrožuje"). S ohledem na to je Agentura nucena postupovat s předběžnou opatrností. Agentura dále dodává, že pokud jsou podmínky podle zmíněného ustanovení naplněna, nemá již prostor pro uvážení – v ustanovení je slovo „neposkytují", nikoliv „nemusejí se poskytnout".

Popsaná rizika jsou podstatně zvýšena 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 vychází z premisy, podle níž fakticky neposkytuje informace toliko žadateli, nýbrž je zveřejňuje a požadované informace by se tak staly dostupné každému. Postup, kdy by informace byly poskytnuty toliko žadateli, avšak zveřejněny by nebyly, InfZ nepřipouští.

Agentura odmítá žádost ve výše uvedeném rozsahu podpůrně rovněž na základě § 11 odst. 1 písm. d) InfZ, podle něhož 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. Z výše uvedeného je zřejmé, že poskytnutí požadovaných informací by minimálně významné ohrožení vyvolalo.

Žádost byla ve výše uvedeném rozsahu odmítnuta také proto, že Agentura je obecně povinna dodržovat požadavky právních předpisů v oblasti kybernetické bezpečnosti, zejména zákona o kybernetické bezpečnosti a právních předpisů, které tento zákon provádějí. To platí zejména s ohledem na to, že je poskytovatelem regulovaných služeb, včetně tzv. režimu vyšších povinností, a je tedy povinna provádět bezpečnostní opatření a zajišťovat bezpečnost informací, tj. jejich důvěrnost, integritu a dostupnost. Protože hrozby či incidenty v oblasti kybernetické bezpečnosti vedou zpravidla ke vzniku finančních škod, je tedy nutné poukázat též na povinnost hospodárného postupu Agentury. Ten vyplývá např. z § 45 odst. 1 zákona č. 218/2000 Sb., o rozpočtových pravidlech, podle kterého jsou organizační složky státu povinny plnit své úkoly nejhospodárnějším způsobem, nebo na § 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. Lze též poukázat na obecnou povinnost k prevenci škod (§ 2900 a násl. zákona č. 89/2012 Sb. občanského zákoníku).

Lze podpůrně dodat, že riziko spojené s poskytnutím požadované informace není čistě kybernetickobezpečnostní, popř. finanční, ale hrozba či dokonce provedení kybernetického útoku představuje riziko (záměrné) snížení důvěry veřejnosti ve stát, jeho instituce a schopnost státu zajišťovat bezpečnost. V kontextu aktuální geopolitické situace je toto riziko zvýšené zejména, ale nikoliv pouze, z důvodu invaze vojsk Ruské federace na Ukrajinu, jakož i souvisejících aktivit Ruské federace vůči členským státům Evropské unie a Severoatlantické aliance.

Agentura uzavírá, že poskytnutí informace požadované žadatelem by bylo v rozporu s požadavky výše uvedených právních předpisů a v rozporu s účelem a smyslem bezpečnostních opatření, které Agentura k jejich realizaci přijímá, pročež z tohoto důvodu žádost žadatele v rozsahu uvedeném ve výroku odmítá, jak je uvedeno výše.

Důvody odmítnutí žádosti v rozsahu dotazu 5.

Podle § 2 odst. 4 InfZ platí, že povinnost poskytovat informace se netýká mj. dotazů na názory a vytváření nových informací. Podle tohoto ustanovení platí, že informace se nevytvářejí až k žádosti (s ohledem na odbornost žadatele lze zjednodušeně říci, že funguje na principu Ctrl+C, Ctrl+V).

Požadovanou úvahu nemá Agentura k dispozici a musela by ji provést teprve k této žádosti. Jednalo by se tedy o nově vytvářenou informaci, na kterou se povinnost poskytovat informace nevztahuje.

Požadovaná informace má rovněž charakter názoru. To vyplývá nejen ze samotné textace dotazu (*„který orgán či instituci považuje DIA za“*), ale také z toho, že Agentura (ani jiný orgán) není povolán, pokud jde o výklad právních předpisů (právní předpisy jsou pro odpověď na tento dotaz nejdůležitější), k tzv. autentickému výkladu, tedy výkladu závaznému pro všechny orgány i osoby. Jednalo by se tedy toliko o názor Agentury, na který se povinnost poskytovat informace nevztahuje.

S ohledem na to, že požadovaná informace má charakter názoru a musela by být vytvořena nově, rozhodla Agentura o odmítnutí žádosti též v rozsahu dotazu 5., jak je uvedeno ve výroku.

Poučení:

Proti odložení žádosti lze podat podle § 16a odst. 3 písm. a) InfZ stížnost. Stížnost je možné podat do 30 dnů ode dne doručení odložení (§ 16a odst. 3 InfZ), a to k Agentuře, nejlépe cestou sekce Hlavního

architekta eGovernmentu, o stížnosti rozhoduje ředitel Agentury (§ 16a odst. 4 InfZ ve spojení s § 178 odst. 2 správního řádu).

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 sekce Hlavního architekta eGovernmentu, o rozkladu rozhoduje ředitel Agentury (§ 16 odst. 3 Infz ve spojení s § 152 odst. 2 a § 178 odst. 2 správního řádu).

Ing. Tomáš Šedivec

ŘEDITEL
ODBORU ARCHITEKTURY