Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Brno 25. června 2026

Č. j. 18442/2026-NÚKIB-E/210

NUKIX0069GED

Věc: Poskytnutí informací podle § 14 odst. 5 písm. d) zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

Vážený pane inženýre,

Národní úřad pro kybernetickou a informační bezpečnost (dále jen jako „**Úřad**“ nebo „**NÚKIB**“) obdržel dne 13. června 2026 Vaši žádost podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, evidovanou pod č.j. 18177/2026-NÚKIB-E/210. V žádosti požadujete poskytnutí níže uvedených informací týkajících se možné závislosti České republiky na digitálních službách, konkrétně jde o tyto dotazy:

1. *Zda Národní úřad pro kybernetickou a informační bezpečnost disponuje analytickými, koncepčními strategickými materiály, které se zabývají rizikem závislosti České republiky na digitálních službách (zejména cloudové výpočetní služby, služby umělé inteligence, satelitní polohové a komunikační systémy) poskytovaných subjekty pod jurisdikcí států mimo Evropskou unii.*
2. *Zda a jakým způsobem je v těchto materiálech, případně v Národní strategii kybernetické bezpečnosti reflektováno riziko jednostranného omezení nebo úplného znepřístupnění takových služeb ze orgánu cizího státu (nikoli pouze riziko úniku či zneužití dat). Žádám o poskytnutí příslušných dokumentů, případně odkazů na jejich veřejně dostupné verze.*
3. *Zda Úřad v této souvislosti vydal jakákoli varování, doporučení nebo metodické pokyny (například režimu zákona č. 264/2025 Sb., o kybernetické bezpečnosti) týkající se závislosti na poskytovatelích mimo EU nebo bezpečnosti dodavatelského řetězce ve vztahu k zahraničnímu cloudu a umělé inteligenci.*
4. *Zda a jak Úřad v této oblasti spolupracuje s institucemi Evropské unie (zejména s agenturou Evropskou komisí) v rámci agendy technologické a digitální suverenity.*
5. *Zda existují doporučení nebo opatření týkající se plánů kontinuity činnosti veřejných institucí náhlé nedostupnosti služeb zahraničních poskytovatelů.*

Ve struktuře dle Vaší žádosti uvádím následující.

K dotazu č. 1 žádosti

NÚKIB v současné době neprovádí systematický sběr informací tohoto charakteru, nicméně monitoruje ty subjekty, které se v minulosti profilovaly jako nedůvěryhodné, popřípadě ty, u nichž je na základě objektivních skutečností dán předpoklad určité míry rizika. S ohledem na uvedené tedy NÚKIB nedisponuje vlastními ucelenými materiály zabývajícími se problematikou rizik spojených se závislostí na digitálních službách poskytovaných subjekty podléhajícími jurisdikci států mimo Evropskou unii.

Obecně k tomu lze doplnit, že tato problematika je součástí širší oblasti bezpečnosti dodavatelského řetězce informačních a komunikačních technologií (ICT Supply Chain Security) a je průběžně řešena jak na národní, tak na evropské úrovni. Úřad současně uvádí, že problematika bezpečnosti ICT dodavatelského řetězce je předmětem kontinuálních aktivit Evropské unie směřujících k přijetí metodických, koncepčních i legislativních opatření.

K dotazu č. 2 žádosti

Riziko jednostranného omezení nebo znepřístupnění digitálních služeb poskytovaných zahraničními subjekty je reflektováno zejména v regulatorních opatřeních Úřadu a ve strategických dokumentech v oblasti kybernetické bezpečnosti.

Problematika je obecně zohledněna zejména v Národní strategii kybernetické bezpečnosti České republiky (dostupná zde: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/) a dále v Doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v České republice (dostupné zde: https://nukib.gov.cz/cs/infoservis/doporuceni/1801-doporuceni-pro-hodnoceni-duveryhodnosti-dodavatelu-technologii-do-5g-siti-v-ceske-republice/). Současně se promítá do vydaných varování podle působnosti Úřadu. Veškeré uvedené dokumenty jsou veřejně dostupné na internetových stránkách NÚKIB.

K dotazu č. 3 a č. 4 žádosti

Úřad vydává v rámci své působnosti varování, doporučení a metodické materiály dotýkající se mimo jiné rizikovosti digitálních služeb poskytovaných subjekty sídlícími mimo Evropskou unii. Všechna vydaná varování, doporučení či metodické materiály jsou zveřejněny na úřední desce Úřadu (dostupná zde: Národní úřad pro kybernetickou a informační bezpečnost - Úřední deska). Dotazované oblasti se dotýká zejména Varování před předáváním dat a vzdálenou správou z Číny ze dne 3. září 2025 a Metodika k varování ze dne 3. září 2025.

Problematika závislosti na zahraničních dodavatelích je dále řešena zejména prostřednictvím regulatorních požadavků vyplývajících ze směrnice NIS2, které byly transponovány do zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen **„nový ZKB“**), zejména prostřednictvím opatření v oblasti řízení rizik a řízení dodavatelů.

V evropském kontextu se problematika promítá zejména do následujících iniciativ:

- ICT Supply Chain Security Toolbox, který se zaměřuje na bezpečnost dodavatelského řetězce, závislost na dodavatelích a využívání nedůvěryhodných dodavatelů (viz: Národní úřad pro kybernetickou a informační bezpečnost - EU představila nový nástroj pro posílení bezpečnosti dodavatelských řetězců v ICT - ICT Supply Chain Security Toolbox. Základy položilo české předsednictví Radě EU);
- hodnocení rizik podle čl. 22 směrnice NIS2 pro vybraná odvětví (viz tamtéž);
- připravované revize nařízení Cybersecurity Act (CSA), která mimo jiné řeší otázku označování nedůvěryhodných dodavatelů a jejich využívání v ICT infrastruktuře Evropské unie (viz Commission strengthens EU cybersecurity resilience and capabilities);
- směrnice NIS2, která stanoví požadavky na řízení rizik spojených s dodavateli z pohledu regulovaných osob (směrnice byla transponována do nového ZKB ve formě bezpečnostního opatření řízení rizik a řízení dodavatelů).

K dotazu č. 5 žádosti

Úřad nevydal samostatná doporučení ani opatření specificky zaměřená na plány kontinuity činnosti veřejných institucí pro případ náhlé nedostupnosti služeb zahraničních poskytovatelů. Požadavky na zajištění kontinuity činností, včetně zpracování plánů kontinuity, jsou stanoveny obecně právními předpisy upravujícími požadavky na kybernetickou bezpečnost, zejména vyhláškou č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností a vyhláškou č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností.

S pozdravem

Elektronický podpis: 25.6.2026
Certifikát autora podpisu:
Jméno: Mgr. Vít Hrazdíra
Vydal: I.CA EU Qualified CA2/RSA 06/2022
Platnost do: 19.11.2026 19:15 +01:00

Mgr. Vít Hrazdíra
vedoucí oddělení právního
Národní úřad pro kybernetickou
a informační bezpečnost

Obdrží:
[redacted]

Vypraveno dne:
viz časový údaj na e-mailové zprávě