Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

REGULACE VYUŽÍVÁNÍ CLOUD COMPUTINGU ORGÁNY VEŘEJNÉ MOCI V ZÁKONĚ O KYBERNETICKÉ BEZPEČNOSTI

VÝKLAD USTANOVENÍ § 4 ODST. 5
ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI

Shrnutí:

Orgán veřejné moci se musí řídit § 4 odst. 5 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „ZKB“) jen v případě, že je zároveň orgánem veřejné správy a jeho informační nebo komunikační systém spadá do působnosti zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů (dále jen „ZoISVS“).

Podrobnější vysvětlení:

Orgány veřejné moci mají podle § 4 odst. 5 ZKB mimo jiné povinnost před uzavřením smlouvy s poskytovatelem služeb cloud computingu zařadit poptávaný cloud computing do bezpečnostní úrovně s ohledem na povahu dotčeného informačního nebo komunikačního systému a zajistit, že budou dodržována bezpečnostní pravidla pro poskytování služeb cloud computingu. Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) vydává tento podpůrný materiál, aby vyjasnil svůj výklad zmíněného ustanovení.

V současné době je regulace cloud computingu rozdělena do dvou místy se překrývajících rovin. Zatímco orgány veřejné moci se řídí ZKB, orgány veřejné správy mají své povinnosti týkající se využívání cloudových služeb stanoveny v ZoISVS. Pro orgány veřejné správy vyplývají ze ZoISVS zjednodušeně povinnosti **(1)** využívat cloud computing, jehož bezpečnostní úroveň je stejná nebo vyšší než bezpečnostní úroveň informačního systému veřejné správy (dále jen „ISVS“) nebo jeho části, k zajištění jehož provozu je využíván dle § 6n písm. d) ZoISVS (předpokladem je přitom zařazení cloud computingu do správné bezpečnostní úrovně), **(2)** postupovat podle bezpečnostních pravidel dle § 5b odst. 2 ZoISVS, a **(3)** využívat pouze služeb cloud computingu, které jsou zapsané v katalogu cloud computingu společně s jejich poskytovateli dle § 6l odst. 1 písm. a) ZoISVS.

S cílem sjednotit regulaci cloud computingu NÚKIB plánuje vyjmout část úpravy obsaženou v ZKB a vložit ji do ZoISVS. Jedná se zejména o problematiku bezpečnostních úrovní[1] a bezpečnostních pravidel[2], přičemž tzv. vstupní kritéria[3] již pod ZoISVS jsou. Tyto změny jsou součástí návrhu doprovodného zákona k návrhu nového zákona o kybernetické bezpečnosti. S ohledem na budoucí sjednocení regulace, ke kterému by mělo dojít v roce 2024 poté, co se nový zákon o kybernetické bezpečnosti stane účinným, se NÚKIB rozhodl upravit svůj výklad § 4 odst. 5 ZKB. Ačkoliv se ve znění tohoto ustanovení mluví o orgánech veřejné moci, bude NÚKIB tyto povinnosti vztahovat pouze na orgány veřejné správy a jejich ISVS podle ZoISVS. Výsledkem interpretačního zúžení bude, že se regulace pro povinné subjekty zjednoduší a zpřehlední. NÚKIB zdůrazňuje, že se jedná pouze o vymezení povinných subjektů, nikoliv o změnu povinností.

[1] Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci.
[2] Vyhláška č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu.
[3] Vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu.

V případě dotazů se prosím obracejte na sekretariát Národního úřadu pro kybernetickou a informační bezpečnost:

Národní úřad pro kybernetickou a informační bezpečnost

Mučednická 1125/31

616 00 Brno – Žabovřesky

E-mail: regulace@nukib.cz

Upozornění:

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

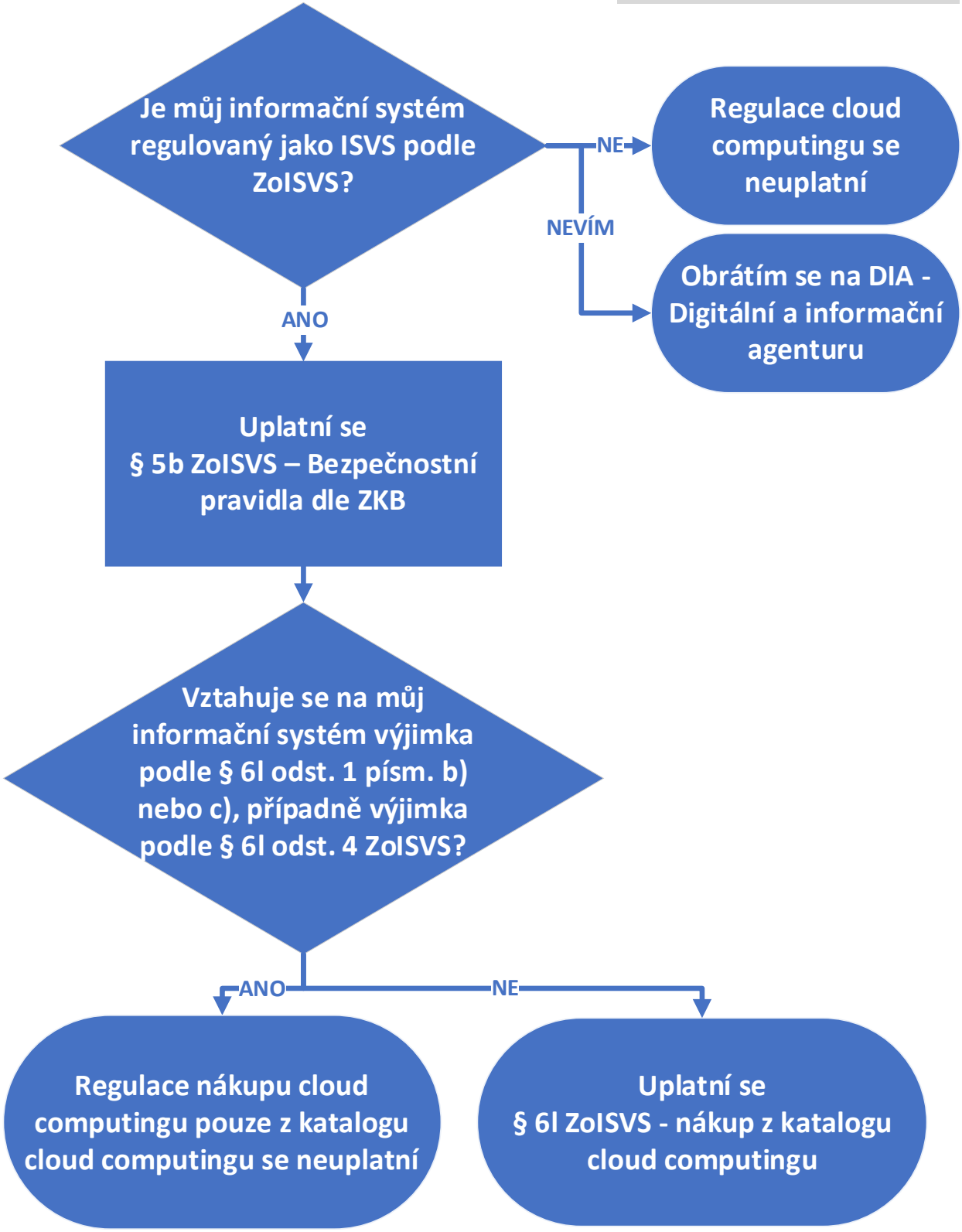
Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti publikované verze dokumentu.

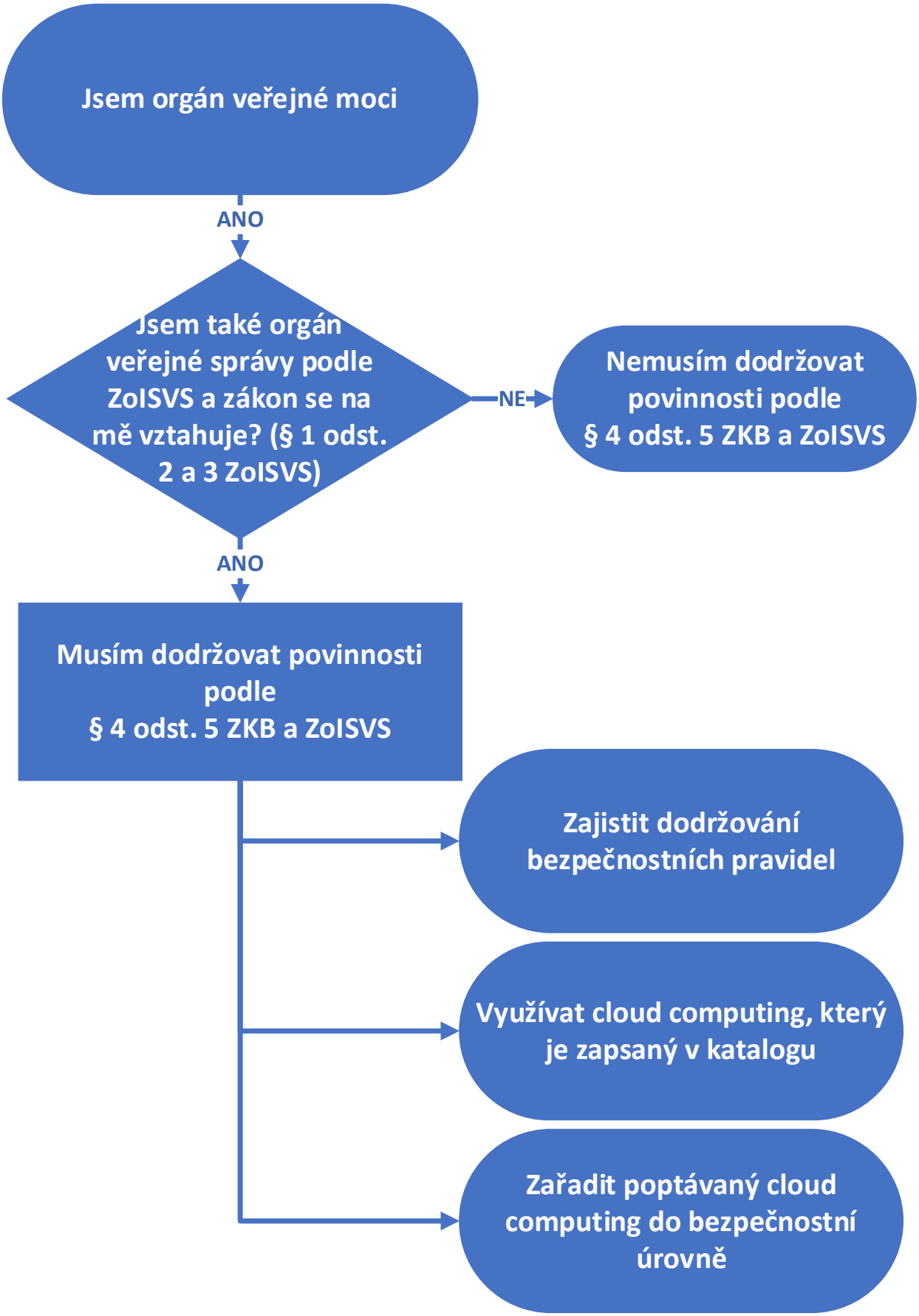
Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Následnující schémata slouží jako vodítko při určování dopadu regulace cloud computingu* na informační systémy.

*Regulací cloud computingu je myšleno uplatnění požadavků podle zákona č. 365/2000 Sb., o informačních systémech veřejné správy (dále jen „ISVS“) a zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „ZKB“)




Jsem orgán veřejné moci
ANO
Jsem také orgán veřejné správy podle ZoISVS a zákon se na mě vztahuje? (§ 1 odst. 2 a 3 ZoISVS)
NE
Nemusím dodržovat povinnosti podle § 4 odst. 5 ZKB a ZoISVS
ANO
Musím dodržovat povinnosti podle § 4 odst. 5 ZKB a ZoISVS
Zajistit dodržování bezpečnostních pravidel
Využívat cloud computing, který je zapsaný v katalogu
Zařadit poptávaný cloud computing do bezpečnostní úrovně

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol. Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
Červená **TLP: RED**	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
Oranžová **TLP: AMBER**	Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám než výše uvedeným, nesmí být informace poskytnuta.
Oranžová **TLP: AMBER+STRICT**	Informace může být sdílena pouze v rámci organizace, které byla informace poskytnuta.
Zelená **TLP: GREEN**	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
Bílá **TLP: CLEAR**	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Verze dokumentu			
datum	**verze**	**změněno**	**popis změny**
3. července 2023	1.0	OREG	Vznik dokumentu
14. července 2023	1.1	OREG	Úprava dokumentu