

FRANCOUZSKÁ REPUBLIKA

Předseda vlády

Návrh vyhlášky o ochraně strategických a citlivých údajů na trhu s cloud computingem

NOR:

Cílová skupina: *Orgány státní správy a provozovatelé, skupiny veřejného zájmu*

Věc: ...

Vstup v platnost: *vyhláška vstupuje v platnost následující den po jejím zveřejnění.*

Poznámka:

Odkazy: *Vyhláškou se provádí článek 31 zákona č. 2024-449 ze dne 21. května 2024 o zabezpečení a regulaci digitálního prostoru. Je k dispozici na internetových stránkách Légifrance (<http://www.legifrance.gouv.fr>).*

Předseda vlády,

Ke zprávě ze dne XX,

s ohledem na nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013;

s ohledem na směrnici Evropského parlamentu a Rady (EU) 2015/1535 ze dne 9. září 2015 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti;

s ohledem na obranný zákoník, zejména na článek D. 3126-2;

s ohledem na nařízení č. 2005-1516 ze dne 8. prosince 2005 o elektronické výměně mezi uživateli a správními orgány a mezi správními orgány, a zejména na článek 9 uvedeného nařízení;

s ohledem na zákon č. 2016-1321 ze dne 7. října 2016 o digitální republice, a zejména na článek 16 tohoto zákona;

s ohledem na zákon č. 2024-449 ze dne 21. května 2024 o zabezpečení a regulaci digitálního prostoru, a zejména na článek 31 tohoto zákona;

s ohledem na výnos č. 2014-445 ze dne 30. dubna 2014 o úkolech a organizaci Generálního ředitelství pro vnitřní bezpečnost;

s ohledem na vyhlášku č. 2015-350 ze dne 27. března 2015, v platném znění, o kvalifikaci bezpečnostních produktů a poskytovatelů služeb vytvářejících důvěru pro účely bezpečnosti informačních systémů;

s ohledem na oznámení č. **XX** zaslané Evropské komisi dne **XXX**;

po konzultaci se Státní radou (správní sekce),

nařizuje:

Článek 1

Do seznamu skupin veřejného zájmu uvedený v čl. 31 část I výše uvedeného zákona ze dne 21. května 2024 náleží:

- skupina veřejného zájmu známá jako „Agentura pro digitální zdraví (ANS)“;
- skupina veřejného zájmu známá jako „Národní agentura pro výzkum AIDS (ANRS)“;
- skupina veřejného zájmu známá jako „Agentura pro podporu vzdělávání a vědecké přípravy a výměny“;
- skupina veřejného zájmu „Centrum zabezpečeného přístupu k datům (CASD)“;
- skupina veřejného zájmu „Centrum pro prevenci radikalizace“;
- skupina veřejného zájmu „Národní veterinární škola“;
- skupina veřejného zájmu „Skupina veřejného zájmu, pokud jde o vysoce aktivní uzavřené radioaktivní zdroje (GIP SOURCES HA)“;
- skupina veřejného zájmu „Národní systém pro evidenci žádostí po sociálním bydlení (GIP SNE)“;
- skupina veřejného zájmu „Modernizace sociálních prohlášení (GIP-MDS)“;
- Skupina veřejného zájmu „Vědecko-technická observatoř“.

Článek 2

I – Pro použití článku 31 výše uvedeného zákona ze dne 21. května 2024 musí soukromý poskytovatel služeb zavést níže uvedená kritéria bezpečnosti a ochrany údajů:

- zdokumentovanou politiku bezpečnosti informací a řízení rizik zahrnující subdodavatelský řetězec;

- bezpečný systém řízení lidských zdrojů pro zaměstnance podílející se na poskytování služby;
- nástroje a postupy pro bezpečnou správu zařízení, která provádějí služby, a informačních systémů;
- fyzická, environmentální a logická bezpečnostní opatření, jako je použití šifrovacích mechanismů, kontrola přístupu a správa identity uživatele;
- postupy pro řízení bezpečnostních incidentů a opatření pro zajištění kontinuity provozu;
- opatření k zajištění souladu s právními předpisy platnými ve Francii a opatření, zejména smluvní, na ochranu zpracovávaných nebo uchovávaných údajů před přístupem orgánů veřejné moci třetích zemí, které nejsou oprávněny podle práva Evropské unie nebo členského státu, včetně zejména podmínek týkajících se držení kapitálu a hlasovacích práv ve společnosti poskytovatele služeb a usazení poskytovatele služeb a případných subdodavatelů.

Požadavky týkajících se těchto kritérií stanoví rámec vypracovaný Francouzskou agenturou pro kybernetickou bezpečnost za podmínek výše uvedené vyhlášky ze dne 27. března 2015. Konzultace nezbytné pro vytvoření a rozvoj tohoto referenčního rámce pro státní informační systém probíhají ve spolupráci s Meziresortním digitálním ředitelstvím.

II – Za účelem splnění požadavků na ochranu a bezpečnost údajů stanovených v čl. 31 části I výše uvedeného zákona ze dne 21. května 2024 využijí dotčené orgány státní správy služby v oblasti cloud computingu poskytované kvalifikovaným soukromým poskytovatelem služeb za podmínek stanovených v kapitole III výše uvedené vyhlášky ze dne 27. března 2015 a splňující kritéria uvedená v části I tohoto článku nebo evropské certifikace alespoň rovnocenné úrovně.

III – Z oblasti působnosti tohoto článku jsou vyloučeny provozní informační a komunikační systémy, vědecké a technické informační systémy a informační systémy, které zahrnují, vyžadují nebo obsahují utajovaná média nebo informace tvořící obranný informační a komunikační systém, jakož i informační a komunikační systémy provozované službami uvedenými v článku D. 3126-2 obranného zákoníku a v článku 1 výše uvedené vyhlášky ze dne 30. dubna 2014.

Článek 3

I – Pokud ke dni, kdy vstoupí v platnost článek 31 výše uvedeného zákona ze dne 21. května 2024, správní orgán již zahájil projekt, který splňuje podmínky definované ve výše uvedeném článku, a využívá službu cloud computingu poskytovanou soukromým poskytovatelem služeb, který neuplatňuje kritéria bezpečnosti a ochrany údajů definovaná v článku 2 této vyhlášky, může v souladu s postupy stanovenými nařízením předsedy vlády požádat o výjimku z povinností stanovených v témže článku.

Tato výjimka nesmí překročit 18 měsíců, pokud jsou ve Francii k dispozici přijatelné služby cloud computingu ve smyslu části II tohoto článku. Pokud v den podání žádosti o výjimku není ve Francii k dispozici žádná přijatelná nabídka založená na cloudu, nesmí výjimka trvat déle než jeden rok před podáním nové žádosti.

Tato výjimka je udělena na základě odůvodněného rozhodnutí ministra odpovědného za projekt a potvrzena předsedou vlády.

Zveřejní se za podmínek stanovených v části III zákoníku vztahů s veřejností.

II – Posouzení přijatelnosti nabídky služeb v oblasti cloud computingu ve smyslu čl. 31 části III výše uvedeného zákona ze dne 21. května 2024 je založeno na následujících kritériích:

- funkční potřeba, na kterou je nabídka schopna reagovat, s přihlédnutím k úkolům příslušné správy;
- finanční podmínky;
- provozní a technické podmínky zabezpečení a ochrany údajů zpracovávaných poskytovatelem nabídky v souladu s požadavky stanovenými v článku 2 této vyhlášky;
- podmínky ukončení smlouvy a záruky vratnosti;
- podmínky kontroly, udržitelnosti a nezávislosti ve smyslu článku 16 výše uvedeného zákona ze dne 7. října 2016.

Dne

Za předsedu vlády: