EVROPSKÁ UNIE

EVROPSKÝ PARLAMENT **RADA**

Brusel 20. listopadu 2024
(OR. en)

2023/0108(COD) **PE-CONS 93/24**

CYBER 207
JAI 1083
TELECOM 217
DATAPROTECT 246
MI 632
IND 327
CODEC 1587

PRÁVNÍ PŘEDPISY A JINÉ AKTY

Předmět:	NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY, kterým se mění nařízení (EU) 2019/881, pokud jde o řízené bezpečnostní služby

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

(EU) 2024/...

ze dne ...,

kterým se mění nařízení (EU) 2019/881, pokud jde o řízené bezpečnostní služby

(Text s významem pro EHP)

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 114 této smlouvy,

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

s ohledem na stanovisko Evropského hospodářského a sociálního výboru[1],

po konzultaci s Výborem regionů,

v souladu s řádným legislativním postupem[2],

---

1 Úř. věst. C 349, 29.9.2023, s. 167.

2 Postoj Evropského parlamentu ze dne 24. dubna 2024 (dosud nezveřejněný v Úředním věstníku) a rozhodnutí Rady ze dne …

vzhledem k těmto důvodům:

(1) Nařízení Evropského parlamentu a Rady (EU) 2019/881[3] stanoví rámec pro vytváření evropských schémat certifikace kybernetické bezpečnosti, jejichž účelem je zajistit odpovídající úroveň kybernetické bezpečnosti produktů, služeb a procesů informačních a komunikačních technologií (IKT) v Unii a zabránit roztříštění vnitřního trhu, pokud jde o schémata certifikace kybernetické bezpečnosti v Unii.

[3] 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 (akt o kybernetické bezpečnosti) (Úř. věst. L 151, 7.6.2019, s. 15).

(2) S cílem zajistit odolnost Unie vůči kybernetickým útokům a předcházet zranitelnostem na vnitřním trhu má toto nařízení doplnit horizontální regulační rámec, který stanoví komplexní požadavky na kybernetickou bezpečnost pro produkty s digitálními prvky podle nařízení Evropského parlamentu a Rady (EU) .../...[4+], stanovením základních bezpečnostních cílů pro řízené bezpečnostní služby, jakož i na uplatňování a důvěryhodnost těchto služeb.

---

[4] Nařízení Evropského parlamentu a Rady (EU) 2024/... ze dne ... o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 168/2013 a (EU) 2019/1020 a směrnice (EU) 2020/1828 (akt o kybernetické odolnosti) (Úř. věst. L, ..., ELI: ...).

[+] Pro Úř. věst.: vložte prosím do textu číslo nařízení obsaženého v dokumentu PE-CONS 100/23 (2017/0272(COD)) a do poznámky pod čarou číslo, datum, odkaz na vyhlášení uvedeného nařízení v Úředním věstníku a odkaz ELI.

(3) Řízené bezpečnostní služby poskytují poskytovatelé řízených bezpečnostních služeb ve smyslu v čl. 6 bodu 40 směrnice Evropského parlamentu a Rady (EU) 2022/2555[5]. Definice řízených bezpečnostních služeb v tomto nařízení by proto měla být v souladu s definicí poskytovatelů řízených bezpečnostních služeb ve směrnici (EU) 2022/2555. Tyto služby spočívají v provádění činností souvisejících s řízením kybernetických bezpečnostních rizik zákazníků nebo v poskytování pomoci s těmito činnostmi a mají stále větší význam při předcházení a zmírňování incidentů. Poskytovatelé těchto služeb jsou proto považováni za základní nebo důležité subjekty náležející do vysoce kritického odvětví podle směrnice (EU) 2022/2555. Jak je uvedeno v 86. bodu odůvodnění uvedené směrnice, poskytovatelé řízených bezpečnostních služeb mají v oblastech, jako jsou reakce na incidenty, penetrační testování, bezpečnostní audity a konzultační činnost, zvlášť důležitou úlohu v pomoci subjektům v jejich úsilí předcházet incidentům, odhalovat je, reagovat na ně nebo zotavovat se se z nich nebo zmírňovat jejich dopad. Poskytovatelé řízených bezpečnostních služeb se však také sami stávají terčem kybernetických útoků a představují zvláštní riziko vzhledem k úzkému začlenění do činností svých zákazníků. Je proto zásadní, aby základní a důležité subjekty ve smyslu směrnice (EU) 2022/2555 postupovaly při výběru poskytovatelů řízených bezpečnostních služeb s náležitou péčí.

---

[5] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2) (Úř. věst. L 333, 27.12.2022, s. 80).

(4) Definice řízených bezpečnostních služeb podle tohoto nařízení zahrnuje demonstrativní výčet řízených bezpečnostních služeb, které by mohly být způsobilé pro evropská kybernetická bezpečnostní schémata certifikace, jako je řešení incidentů, penetrační testování, bezpečnostní audity a konzultace související s technickou podporou. Řízené bezpečnostní služby by mohly zahrnovat služby kybernetické bezpečnosti, které podporují připravenost na incidenty, jejich předcházení, odhalování, analýzu, zmírňování, reakci na ně nebo zotavení se z nich. Za řízené bezpečnostní služby by mohlo být považováno také poskytování poznatků kybernetických hrozeb (tzv. „cyber threat intelligence“) a posouzení rizik související s technickou podporou. Pro jednotlivé řízené bezpečnostní služby by mohla být zřízena samostatná evropská schémata certifikace kybernetické bezpečnosti. Evropské certifikáty kybernetické bezpečnosti vydané v souladu s těmito schématy by měly odkazovat na konkrétní řízené bezpečnostní služby konkrétního poskytovatele těchto služeb.

(5) Poskytovatelé řízených bezpečnostních služeb mohou rovněž hrát důležitou úlohu, pokud jde o kroky Unie na podporu reakce a počáteční obnovy v případě významných incidentů a rozsáhlých kybernetických bezpečnostních incidentů, přičemž se spoléhají na služby důvěryhodných soukromých poskytovatelů a na testování kritických subjektů z hlediska potenciálních zranitelností na základě koordinovaného posouzení bezpečnostních rizik, a to na úrovni Unie. Certifikace řízených bezpečnostních služeb by mohla hrát roli při výběru důvěryhodných poskytovatelů řízených bezpečnostních služeb podle nařízení Evropského parlamentu a Rady (EU) .../...[6+].

(6) Certifikace řízených bezpečnostních služeb je důležitá nejen pro proces výběru rezervy EU pro kybernetickou bezpečnost stanovenou nařízením (EU) .../...[++], ale je rovněž zásadním ukazatelem kvality pro soukromé a veřejné subjekty, které mají v úmyslu tyto služby zakoupit. S ohledem na kritičnost řízených bezpečnostních služeb a citlivost zpracovávaných údajů by certifikace mohla potenciálním zákazníkům poskytnout důležitá vodítka a záruky ohledně důvěryhodnosti těchto služeb. Cílem evropských schémat certifikace kybernetické bezpečnosti pro řízené bezpečnostní služby je pomoci zabránit roztříštění vnitřního trhu. Cílem tohoto nařízení je proto zlepšit fungování vnitřního trhu.

---

6 Nařízení Evropského parlamentu a Rady (EU) …/… ze dne …, kterým se stanovují opatření k posílení solidarity a kapacit v Unii pro odhalování kybernetických hrozeb a incidentů a pro připravenost a reakci na ně a mění nařízení (EU) 2021/694 (nařízení o kybernetické solidaritě) (Úř. věst. L, …, ELI: …).

\+ Pro Úř. věst.: vložte prosím do textu číslo nařízení obsaženého v dokumentu PE-CONS 94/24 (2023/0109(COD)) a do poznámky pod čarou číslo, datum, odkaz na vyhlášení uvedeného nařízení v Úředním věstníku a odkaz ELI.

\++ Pro Úř. věst.: vložte prosím do textu číslo nařízení obsaženého v dokumentu PE-CONS 94/24 (2023/0109 (COD)).

(7) Evropská schémata certifikace kybernetické bezpečnosti řízených bezpečnostních služeb by měla vést k rozšíření těchto služeb a k posílení konkurence mezi poskytovateli řízených bezpečnostních služeb. Aniž je dotčen cíl zajistit dostatečnou a vhodnou úroveň příslušných technických znalostí a profesní integrity těchto poskytovatelů, měla by proto tato schémata certifikace usnadnit vstup na trh a nabízení řízených bezpečnostních služeb tím, že v co největší míře zjednoduší případnou regulační, administrativní a finanční zátěž, kterým by poskytovatelé, zejména malé a střední podniky, včetně mikropodniků, mohli při nabízení řízených bezpečnostních služeb čelit. Za účelem podpory rozšíření řízených bezpečnostních služeb a stimulace poptávky po nich by evropská schémata certifikace kybernetické bezpečnosti řízených bezpečnostních služeb měla navíc přispívat k jejich dostupnosti, zejména pro menší subjekty, jako jsou malé a střední podniky, včetně mikropodniků, jakož i místní a regionální orgány, které mají omezené kapacity a zdroje, ale které jsou náchylnější k narušením kybernetické bezpečnosti, která mají finanční, právní, reputační a provozní důsledky.

(8) Malým a středním podnikům, včetně mikropodniků, je třeba poskytovat podporu při provádění tohoto nařízení a při náboru pracovníků s odpovídajícími specializovanými dovednostmi a odbornými znalostmi v oblasti kybernetické bezpečnosti nezbytnými k poskytování řízených bezpečnostních služeb v souladu požadavky stanovenými v tomto nařízení. Program Digitální Evropa stanovený nařízením Evropského parlamentu a Rady (EU) 2021/694[7] a další příslušné programy Unie stanoví, že Komise má zavést finanční a technickou podporu, která těmto podnikům umožní přispívat k růstu hospodářství Unie a posilování společné úrovně kybernetické bezpečnosti v Unii, mimo jiné zefektivněním finanční podpory z programu Digitální Evropa a dalších příslušných programů Unie a podporou malých a středních podniků, včetně mikropodniků.

(9) Evropská schémata certifikace kybernetické bezpečnosti pro řízené bezpečnostní služby by měla přispívat k dostupnosti zabezpečených a vysoce kvalitních služeb, které zaručují bezpečnou digitální transformaci, a k dosažení cílů stanovených v politickém programu Digitální dekáda 2030 stanoveném rozhodnutím Evropského parlamentu a Rady (EU) 2022/2481[8], zejména pokud jde o cíl, aby 75 % podniků v Unii začalo používat služby cloud computingu, data velkého objemu nebo umělou inteligenci, aby více než 90 % a malých a středních podniků, včetně mikropodniků, dosáhlo alespoň základní úrovně digitální vyspělosti a aby klíčové veřejné služby byly přístupné on-line.

---

7 Nařízení Evropského parlamentu a Rady (EU) 2021/694 ze dne 29. dubna 2021, kterým se zavádí program Digitální Evropa a zrušuje rozhodnutí (EU) 2015/2240 (Úř. věst. L 166, 11.5.2021, s. 1).

8 Rozhodnutí Evropského parlamentu a Rady (EU) 2022/2481 ze dne 14. prosince 2022, kterým se zavádí politický program Digitální dekáda 2030 (Úř. věst. L 323, 19.12.2022, s. 4).

(10) Kromě zavádění produktů, služeb nebo procesů IKT poskytují řízené bezpečnostní služby často další prvky služeb, které se opírají o kompetence, odborné znalosti a zkušenosti zaměstnanců poskytovatelů těchto služeb. Velmi vysoká úroveň těchto kompetencí, odborných znalostí a zkušeností, jakož i vhodné vnitřní postupy by měly být součástí bezpečnostních cílů, aby byla zajištěna velmi vysoká kvalita poskytovaných řízených bezpečnostních služeb. S cílem zajistit, aby se na všechny prvky řízených bezpečnostních služeb mohly vztahovat zvláštní evropská schémata certifikace kybernetické bezpečnosti, je proto nutné změnit nařízení (EU) 2019/881. Měly by být zohledněny výsledky a doporučení hodnocení a přezkumu podle nařízení (EU) 2019/881.

(11) S cílem usnadnit růst spolehlivého vnitřního trhu a zároveň navázat partnerství s podobně smýšlejícími třetími zeměmi by měl být proces certifikace zavedený v oblasti evropského rámce pro certifikaci kybernetické bezpečnosti stanoveného tímto nařízením nastaven tak, aby se usnadnilo mezinárodní uznávání a soulad s mezinárodními normami.

(12) Unie se potýká s nedostatkem talentů v podobě nedostatku kvalifikovaných odborníků a čelí rychle se vyvíjejícím hrozbám, jak je uvedeno ve sdělení Komise ze dne 18. dubna 2023 nazvaném „Řešení nedostatku talentů v oblasti kybernetické bezpečnosti za účelem posílení konkurenceschopnosti, růstu a odolnosti EU („Akademie kybernetických dovedností“). Vzdělávací zdroje a formy formálního školení se liší a znalosti lze získávat různými způsoby: formálními, například prostřednictvím univerzit nebo kurzů, nebo neformálními, například prostřednictvím profesní přípravy na pracovišti nebo pracovní praxe v příslušném oboru. Za účelem usnadnění vzniku kvalitních řízených bezpečnostních služeb a získání lepšího přehledu o struktuře pracovníků Unie v oblasti kybernetické bezpečnosti je třeba posílit spolupráci mezi členskými státy, Komisí, Agenturou Evropské unie pro kybernetickou bezpečnost (dále jen „agentura ENISA“) a zúčastněnými stranami, včetně soukromého sektoru a akademické obce, a to prostřednictvím rozvoje partnerství veřejného a soukromého sektoru, podpory výzkumných a inovačních iniciativ, rozvoje a vzájemného uznávání společných norem a certifikace dovedností v oblasti kybernetické bezpečnosti, mimo jiné pomocí evropského rámce dovedností v oblasti kybernetické bezpečnosti. Tato spolupráce by rovněž usnadnila mobilitu odborníků na kybernetickou bezpečnost v rámci Unie a začlenění znalostí a odborné přípravy v oblasti kybernetické bezpečnosti do vzdělávacích programů a zároveň by mladým lidem, včetně osob žijících ve znevýhodněných regionech, jako jsou ostrovy, řídce osídlené, venkovské a odlehlé oblasti, zajistila přístup k učňovské přípravě a stážím. Je důležité, aby cílem této spolupráce bylo přilákat do tohoto oboru více žen a dívek a přispět k řešení genderových rozdílů v přírodních vědách, technologiích, inženýrství a matematice a aby soukromý sektor usiloval o zajištění profesní přípravy na pracovišti zaměřené na nejžádanější dovednosti zahrnující veřejnou správu a začínající podniky, jakož i malé a střední podniky, včetně mikropodniků. Je rovněž třeba, aby poskytovatelé a členské státy spolupracovali a přispívali ke shromažďování údajů o situaci a vývoji na trhu práce v oblasti kybernetické bezpečnosti.

(13) Při vypracovávání návrhů evropských schémat certifikace kybernetické bezpečnosti hraje důležitou úlohu agentura ENISA. Při vypracovávání návrhu souhrnného rozpočtu Unie by Komise měla v souladu s postupem stanoveným v článku 29 nařízení (EU) 2019/881 posoudit nezbytné rozpočtové zdroje pro plán pracovních míst agentury ENISA.

(14) Toto nařízení stanoví cílené změny nařízení (EU) 2019/881 s cílem umožnit vytváření evropských schémat certifikace kybernetické bezpečnosti pro řízené bezpečnostní služby. Tím rovněž upřesňuje a vyjasňuje některá ustanovení uvedeného nařízení týkající se vypracovávání a fungování všech evropských schémat certifikace kybernetické bezpečnosti s cílem zajistit jejich transparentnost a otevřenost. Posledně uvedenými změnami, které se omezují na upřesnění nebo vyjasnění nařízení (EU) 2019/881, zejména změnami ohledně informací, jež má agentura ENISA poskytovat při předávání návrhů schémat, **ad hoc** pracovních skupin zřízených pro každý návrh schématu, a informací a konzultací týkajících se evropských schémat certifikace kybernetické bezpečnosti, by nemělo být žádným způsobem dotčeno širší hodnocení a přezkum uvedeného nařízení vyžadované podle jeho článku 67, zejména hodnocení dopadu, účinnosti a účelnosti hlavy uvedeného nařízení týkající se rámce pro certifikaci kybernetické bezpečnosti. Hodnocení a přezkum týkající se uvedené hlavy by měly vycházet z co nejširších konzultací se zúčastněnými stranami a z úplné a důkladné analýzy příslušných postupů.

(15) Jelikož cíle tohoto nařízení, totiž umožnit zřizování evropských schémat certifikace kybernetické bezpečnosti pro řízené bezpečnostní služby, nemůže být dosaženo uspokojivě členskými státy, ale spíše jej z důvodu jeho rozsahu a účinků může být lépe dosaženo na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy o Evropské unii. V souladu se zásadou proporcionality stanovenou v uvedeném článku nepřekračuje toto nařízení rámec toho, co je nezbytné pro dosažení uvedeného cíle.

(16) Evropský inspektor ochrany údajů byl konzultován v souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725[9] a dne 10. ledna 2024 vydal své stanovisko,

PŘIJALY TOTO NAŘÍZENÍ:

[9] Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39).

Článek 1

Změny nařízení (EU) 2019/881

Nařízení (EU) 2019/881 se mění takto:

1) V čl. 1 odst. 1 prvním pododstavci se písmeno b) nahrazuje tímto:

„b) rámec pro zavedení evropských schémat certifikace kybernetické bezpečnosti, jehož účelem je zajistit odpovídající úroveň kybernetické bezpečnosti produktů, služeb a procesů IKT a řízených bezpečnostních služeb v Unii a zabránit roztříštění vnitřního trhu, pokud jde o schémata certifikace kybernetické bezpečnosti v Unii.“

2) Článek 2 se mění takto:

a) body 9, 10 a 11 se nahrazují tímto:

„9) „evropským schématem certifikace kybernetické bezpečnosti“ komplexní soubor pravidel, technických požadavků, norem a postupů, které jsou stanoveny na úrovni Unie a které se uplatňují na certifikaci nebo posuzování shody určitých produktů, služeb a procesů IKT nebo řízených bezpečnostních služeb;

10) „vnitrostátním schématem certifikace kybernetické bezpečnosti“ komplexní soubor pravidel, technických požadavků, norem a postupů, které vyvinuly a přijaly vnitrostátní veřejné orgány, a které se uplatňují na certifikaci nebo na posuzování shody produktů, služeb a procesů IKT nebo řízených bezpečnostních služeb spadajících do oblasti působnosti konkrétního schématu;

11) „evropským certifikátem kybernetické bezpečnosti“ dokument vydaný příslušným orgánem a osvědčující, že byl hodnocen soulad daného produktu, služby nebo procesu IKT nebo řízené bezpečnostní služby s konkrétními bezpečnostními požadavky stanovenými v evropském schématu certifikace kybernetické bezpečnosti;“

b) vkládá se nový bod, který zní:

„14a) „řízenou bezpečnostní službou“ služba poskytovaná třetí straně spočívající v provádění činností souvisejících s řízením kybernetických bezpečnostních rizik nebo v poskytování pomoci při takových činnostech, jako je řešení incidentů, penetrační testování, bezpečnostní audity a konzultační činnost, včetně odborného poradenství, které souvisí s technickou podporou;“

c) body 20, 21 a 22 se nahrazují tímto:

„20) „technickou specifikací“ dokument, který předepisuje technické požadavky, které má produkt, služba nebo proces IKT nebo řízená bezpečnostní služba splňovat, nebo postup posuzování shody produktu, služby nebo procesu IKT nebo řízené bezpečnostní služby;

21) „úrovní záruky“ podklad pro důvěru, že produkt, služba nebo proces IKT nebo řízená bezpečnostní služba splňuje bezpečnostní požadavky konkrétního evropského schématu certifikace kybernetické bezpečnosti, přičemž uvádí, na jakou úroveň bylo hodnocení produktu, služby nebo procesu IKT nebo řízená bezpečnostní služba provedeno, avšak jako taková neměří bezpečnost dotčeného produktu, služby nebo procesu IKT nebo řízené bezpečnostní služby;

22) „vlastním posuzováním shody“ úkon prováděný výrobcem nebo poskytovatelem produktů, služeb, procesů IKT nebo řízených bezpečnostních služeb, jímž se vyhodnocuje, zda tyto produkty, služby nebo procesy IKT nebo řízené bezpečnostní služby splňují požadavky konkrétního evropského schématu certifikace kybernetické bezpečnosti;“.

3) V článku 4 se odstavec 6 nahrazuje tímto:

„6. Agentura ENISA prosazuje využívání evropské certifikace kybernetické bezpečnosti, aby se zabránilo roztříštění vnitřního trhu. S cílem zvýšit transparentnost kybernetické bezpečnosti produktů, služeb a procesů IKT a řízených bezpečnostních služeb, a posílit tak důvěru v digitální vnitřní trh a jeho konkurenceschopnost, přispívá agentura ENISA k zavedení a správě evropského rámce pro certifikaci kybernetické bezpečnosti v souladu s hlavou III tohoto nařízení.“

4) Článek 8 se mění takto:

a) odstavec 1 se mění takto:

i) návětí se nahrazuje tímto:

„1. Agentura ENISA podporuje a prosazuje tvorbu a provádění politiky Unie v oblasti certifikace kybernetické bezpečnosti produktů, služeb a procesů IKT a řízených bezpečnostních služeb, jak je stanoveno v hlavě III tohoto nařízení, tím, že:

ii) písmeno b) se nahrazuje tímto:

b) vypracovává návrhy evropských schémat certifikace kybernetické bezpečnosti (dále jen „návrhy schémat“) pro produkty, služby a procesy IKT a řízené bezpečnostní služby v souladu s článkem 49;

b) odstavec 3 se nahrazuje tímto:

„3. Agentura ENISA ve spolupráci s vnitrostátními orgány certifikace kybernetické bezpečnosti a průmyslovým odvětvím oficiálním, strukturovaným a transparentním způsobem sestavuje a zveřejňuje pokyny a vypracovává osvědčené postupy týkající se požadavků na kybernetickou bezpečnost produktů, služeb a procesů IKT a řízených bezpečnostních služeb.“;

c) odstavec 5 se nahrazuje tímto:

„5. Agentura ENISA usnadňuje stanovení a zavádění evropských a mezinárodních norem pro řízení rizik a pro bezpečnost produktů, služeb a procesů IKT a řízených bezpečnostních služeb.“

5) Článek 46 se nahrazuje tímto:

„*Článek 46*

Evropský rámec pro certifikaci kybernetické bezpečnosti

1. Zřizuje se evropský rámec pro certifikaci kybernetické bezpečnosti s cílem zlepšit podmínky fungování vnitřního trhu tím, že dojde ke zvýšení úrovně kybernetické bezpečnosti v Unii a umožní harmonizovaný přístup k evropským schématům certifikace kybernetické bezpečnosti na úrovni Unie, a to s výhledem na vytvoření jednotného digitálního trhu s produkty, službami, procesy IKT a řízenými bezpečnostními službami.

2. Evropský rámec pro certifikaci kybernetické bezpečnosti poskytne mechanismus pro vytváření evropských schémat certifikace kybernetické bezpečnosti a pro osvědčování toho, že produkty, služby a procesy IKT hodnocené v souladu s takovými schématy splňují stanovené bezpečnostní požadavky, pokud jde o ochranu dostupnosti, autenticity, integrity nebo důvěrnosti uchovávaných, předávaných či zpracovávaných údajů nebo funkcí či služeb nabízených nebo přístupných prostřednictvím těchto produktů, služeb a procesů během celého jejich životního cyklu. Kromě toho osvědčí, že řízené bezpečnostní služby, které byly hodnoceny v souladu s těmito schématy, splňují stanovené bezpečnostní požadavky, pokud jde o ochranu dostupnosti, autenticity, integrity a důvěrnosti údajů, které jsou v souvislosti s poskytováním těchto služeb předmětem přístupu, zpracování, ukládání či předávání, a že tyto služby jsou trvale poskytovány s nezbytnými kompetencemi, odborností a zkušenostmi, a to zaměstnanci s dostatečnou a odpovídající úrovní příslušných technických znalostí a profesní integrity.“

6) Článek 47 se mění takto:

a) odstavec 2 se nahrazuje tímto:

„2. Průběžný pracovní program Unie obsahuje zejména seznam produktů, služeb a procesů IKT či jejich kategorií a řízených bezpečnostních služeb, pro něž by mohlo být zařazení do oblasti působnosti evropského schématu kybernetické bezpečnosti prospěšné.“;

b) odstavec 3 se mění takto:

i) návětí se nahrazuje tímto:

„3. Zařazení každého konkrétního produktu, služby či procesu IKT či jejich kategorií nebo řízených bezpečnostních služeb do průběžného pracovního programu Unie musí být podloženo jedním či více z následujících důvodů:“;

ii) písmeno a) se nahrazuje tímto:

„a) dostupnost a rozvoj vnitrostátních schémat certifikace kybernetické bezpečnosti vztahujících se na konkrétní kategorii produktů, služeb nebo procesů IKT nebo řízených bezpečnostních služeb, zejména pokud jde o riziko roztříštěnosti;“

iii) vkládá se nové písmeno, které zní:

„(ca) technologický vývoj a dostupnost a rozvoj mezinárodních schémat certifikace kybernetické bezpečnosti a mezinárodních norem a standardů používaných v tomto odvětví;“.

7) Článek 49 se mění takto:

a) odstavce 1 až 4 se nahrazují tímto:

„1. Agentura ENISA na základě žádosti Komise podle článku 48 vypracuje návrh schématu, který splňuje příslušné požadavky stanovené v článcích 51, 51a, 52 a 54.

2. Agentura ENISA může na základě žádosti Evropské skupiny pro certifikaci kybernetické bezpečnosti podle čl. 48 odst. 2 vypracovat návrh schématu, který splňuje příslušné požadavky stanovené v článcích 51, 51a, 52 a 54. Pokud agentura ENISA takovou žádost odmítne, poskytne k tomu odůvodnění. Každé rozhodnutí o odmítnutí žádosti přijímá správní rada.

3. Při vypracovávání návrhu schématu agentura ENISA konzultuje včas všechny příslušné zúčastněné strany prostřednictvím formálních, otevřených, transparentních a inkluzivních konzultačních postupů. Při předávání návrhu schématu Komisi podle odstavce 6 poskytne agentura ENISA informace o způsobu, jakým zajistila soulad s tímto odstavcem.

4. Pro každý návrh schématu agentura ENISA zřídí ad hoc pracovní skupinu v souladu s čl. 20 odst. 4, která agentuře ENISA poskytuje konkrétní poradenství a odborné poznatky. Podle potřeby, a aniž jsou dotčeny postupy a prostor pro uvážení stanovené v čl. 20 odst. 4 jsou součástí *ad hoc* pracovních skupin odborníci z orgánů veřejné správy členských států, orgánů, institucí a jiných subjektů Unie a soukromého sektoru.“;

b) odstavec 7 se nahrazuje tímto:

„7. Na základě návrhu schématu vypracovaného agenturou ENISA může Komise přijmout prováděcí akty, kterými stanoví, že evropské schéma certifikace kybernetické bezpečnosti pro produkty, služby a procesy IKT a řízené bezpečnostní služby, splňuje relevantní požadavky stanovené v článcích 51, 51a, 52 a 54. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 66 odst. 2.“

8) Vkládá se nový článek, který zní:

„*Článek 49a*

Informace a konzultace týkající se evropských schémat certifikace kybernetické bezpečnosti

1. Komise zveřejní informace o své žádosti agentuře ENISA, aby vypracovala návrh schématu nebo přezkoumala stávající evropské schéma certifikace kybernetické bezpečnosti uvedený v článku 48.

2. V průběhu vypracovávání návrhu schématu agenturou ENISA podle článku 49 mohou Evropský parlament, Rada nebo oba požádat Komisi coby předsedu Evropské skupiny pro certifikaci kybernetické bezpečnosti (ECCG) a agenturu ENISA, aby čtvrtletně předkládaly příslušné informace o návrhu schématu. Na žádost Evropského parlamentu nebo Rady může agentura ENISA po dohodě s Komisí, a aniž je dotčen článek 27, zpřístupnit Evropskému parlamentu a Radě příslušné části návrhu schématu způsobem, který odpovídá požadované úrovni důvěrnosti, a případně omezeným způsobem.

3. S cílem posílit dialog mezi orgány Unie a přispět k formálnímu, otevřenému, transparentnímu a inkluzivnímu konzultačnímu procesu mohou Evropský parlament, Rada, nebo oba vyzvat Komisi a agenturu ENISA, aby projednaly záležitosti týkající se fungování evropských schémat certifikace kybernetické bezpečnosti pro produkty, služby a procesy IKT nebo řízené bezpečnostní služby.

4. Komise při hodnocení tohoto nařízení podle článku 67 případně zohlední skutečnosti vyplývající z názorů vyjádřených Evropským parlamentem a Radou k záležitostem uvedeným v odstavci 3 tohoto článku.“

9) Článek 51 se mění takto:

a) název se nahrazuje tímto:

„*Bezpečnostní cíle evropských schémat certifikace kybernetické bezpečnosti pro produkty, služby a procesy IKT*“;

b) úvodní věta se nahrazuje tímto:

„Evropské schéma certifikace kybernetické bezpečnosti pro produkty, služby nebo procesy IKT musí být navrženo tak, aby v příslušných případech bylo dosaženo alespoň těchto bezpečnostních cílů:“.

10) Vkládá se nový článek, který zní:

„*Článek 51a*
Bezpečnostní cíle evropských schémat certifikace kybernetické bezpečnosti pro řízené bezpečnostní služby

Evropské schéma certifikace kybernetické bezpečnosti pro řízené bezpečnostní služby musí být navrženo tak, aby v příslušných případech bylo dosaženo alespoň těchto bezpečnostních cílů:

a) zajistit, aby řízené bezpečnostní služby byly poskytovány s nezbytnými kompetencemi, odborností a zkušenostmi, což zahrnuje, že zaměstnanci odpovědní za poskytování těchto služeb mají dostatečnou a odpovídající úroveň technických znalostí a kompetencí v dané oblasti, dostatečné a odpovídající zkušenosti a nejvyšší úroveň profesní integrity;

b) zajistit, aby měl poskytovatel zavedeny vhodné vnitřní procesy k zajištění toho, aby řízené bezpečnostní služby byly vždy poskytovány na dostatečné a odpovídající úrovni kvality;

c) zajistit, aby se data, jež jsou v souvislosti s poskytováním řízených bezpečnostních služeb předmětem přístupu, ukládání či předávání nebo jiného zpracování, chránila proti neúmyslnému nebo neoprávněnému přístupu, ukládání, sdělení, zničení, jinému zpracování, ztrátě, změně či nedostupnosti;

d) zajistit, aby byla včas obnovena dostupnost dat, služeb a funkcí a přístup k nim v případě fyzických nebo technických incidentů;

e) zajistit, aby oprávněné osoby, programy nebo stroje měly přístup pouze k údajům, službám nebo funkcím, jichž se týkají jejich přístupová práva;

f) zajistit, aby byly pořizovány a uchovávány záznamy o datech, službách nebo funkcích, jež byly zpřístupněny, použity nebo jinak zpracovány, kdy k tomu došlo a kdo tak učinil, a umožněno posouzení těchto záznamů;

g) zajistit, aby produkty, služby a procesy IKT zaváděné v rámci poskytování řízených bezpečnostních služeb byly bezpečné na úrovni výchozího návrhu a výchozího nastavení („secure by design“ a „secure by default“) a aby v příslušných případech zahrnovaly nejnovější bezpečnostní aktualizace a neobsahovaly veřejně známé zranitelnosti;“.

11) Článek 52 se mění takto:

a) odstavec 1 se nahrazuje tímto:

„1. Evropské schéma certifikace kybernetické bezpečnosti může u produktů, služeb a procesů IKT a řízených bezpečnostních služeb určit jednu nebo více těchto úrovní záruky: „základní“, „významná“ nebo „vysoká“. Úroveň záruky je přiměřená úrovni rizika z hlediska pravděpodobnosti a dopadu incidentu, jež je spojeno se zamýšleným použitím produktu, služby nebo procesu IKT nebo řízené bezpečnostní služby.“;

b) odstavec 3 se nahrazuje tímto:

„3. Evropské schéma certifikace kybernetické bezpečnosti stanoví bezpečnostní požadavky, které odpovídají každé úrovni záruky, včetně odpovídajících bezpečnostních funkcí a odpovídající míry náročnosti a podrobnosti hodnocení, kterým má produkt, služba nebo proces IKT nebo řízená bezpečnostní služba projít.“;

c) odstavce 5, 6 a 7 se nahrazují tímto:

„5. Evropský certifikát kybernetické bezpečnosti nebo EU prohlášení o shodě, které odkazují na úroveň záruky „základní“, poskytují záruku, že produkty, služby a procesy IKT nebo řízené bezpečnostní služby, pro něž jsou tento certifikát nebo toto EU prohlášení o shodě vydány, splňují odpovídající bezpečnostní požadavky včetně bezpečnostních funkcí a že byly vyhodnoceny na úrovni, jejímž cílem je minimalizovat známá základní rizika incidentů a kybernetických útoků. Prováděné hodnotící činnosti zahrnují alespoň přezkum technické dokumentace. Pokud takový přezkum není vhodný, provedou se náhradní hodnotící činnosti s rovnocenným účinkem.

6. Evropský certifikát kybernetické bezpečnosti, který odkazuje na úroveň záruky „významná“, poskytuje záruku, že produkty, služby a procesy IKT nebo řízené bezpečnostní služby, pro něž je tento certifikát vydán, splňují odpovídající bezpečnostní požadavky včetně bezpečnostních funkcionalit a že byly vyhodnoceny na úrovni, jejímž cílem je minimalizovat známá kybernetická rizika a rizika incidentů a kybernetických útoků prováděných subjekty s omezenými dovednostmi a zdroji. Prováděné hodnotící činnosti zahrnují alespoň: přezkum s cílem prokázat neexistenci veřejně známých zranitelností a zkouška k prokázání toho, že produkty, služby a procesy IKT nebo řízené bezpečnostní služby náležitě uplatňují nezbytné bezpečnostní funkcionality. Pokud některá z těchto hodnotících činností není vhodná, provedou se náhradní hodnotící činnosti s rovnocenným účinkem.

7. Evropský certifikát kybernetické bezpečnosti, který odkazuje na úroveň záruky „vysoká“, poskytuje záruku, že produkty, služby nebo procesy IKT a řízené bezpečnostní služby, pro něž je tento certifikát vydán, splňují odpovídající bezpečnostní požadavky včetně bezpečnostních funkcionalit a že byly vyhodnoceny na úrovni, jejímž cílem je minimalizovat rizika sofistikovaných kybernetických útoků prováděných subjekty s významnými dovednostmi a zdroji. Prováděné hodnotící činnosti zahrnují alespoň: přezkum s cílem prokázat neexistenci veřejně známých zranitelností; zkouška k prokázání toho, že produkty, služby, procesy IKT nebo řízené bezpečnostní služby IKT náležitě uplatňují nezbytné nejnovější bezpečnostní funkcionality; a posouzení jejich odolnosti vůči zručným útočníkům prostřednictvím penetrační testování. Pokud některá z těchto hodnotících činností není vhodná, provedou se náhradní hodnotící činnosti s rovnocenným účinkem.“

12) V článku 53 se odstavce 1, 2 a 3 nahrazují tímto:

„1. Evropské schéma certifikace kybernetické bezpečnosti může umožnit vlastní posuzování shody pod výhradní odpovědností výrobce nebo poskytovatele produktů, služeb či procesů IKT nebo řízených bezpečnostních služeb. Vlastní posuzování shody je přípustné pouze u produktů, služeb a procesů IKT nebo řízených bezpečnostních služeb, které vykazují nízké riziko odpovídající úrovni záruky „základní“.

2. Výrobce nebo poskytovatel produktů, služeb či procesů IKT nebo řízených bezpečnostních služeb může vydat EU prohlášení o shodě uvádějící, že bylo prokázáno plnění požadavků stanovených v příslušném schématu. Vydáním tohoto prohlášení výrobce produktů IKT nebo poskytovatel služeb či procesů IKT nebo řízených bezpečnostních služeb přebírá odpovědnost za soulad produktu, služby nebo procesu IKT nebo řízené bezpečnostní služby s požadavky stanovenými v daném schématu.

3. Výrobce nebo poskytovatel produktů, služeb či procesů IKT nebo řízených bezpečnostních služeb zpřístupní EU prohlášení o shodě, technickou dokumentaci a veškeré ostatní příslušné informace související se shodou produktů, služeb a procesů IKT nebo řízených bezpečnostních služeb se schématem k dispozici vnitrostátního orgánu certifikace kybernetické bezpečnosti určenému podle v článku 58 po dobu stanovenou v odpovídajícím evropském schématu certifikace kybernetické bezpečnosti. Jedno vyhotovení EU prohlášení o shodě se předkládá vnitrostátnímu orgánu certifikace kybernetické bezpečnosti a jedno vyhotovení agentuře ENISA.“

13) V článku 54 se odstavec 1 mění takto:

a) písmeno a) se nahrazuje tímto:

„a) předmět a oblast působnosti schématu certifikace včetně druhu nebo kategorií zahrnutých produktů, služeb a procesů IKT a řízených bezpečnostních služeb, na něž se vztahuje;“

b) písmeno g) se nahrazuje tímto:

„g) konkrétní kritéria a metody hodnocení používané k prokázání toho, že bylo dosaženo příslušných bezpečnostních cílů uvedených v článcích 51 a 51a, včetně typů těchto hodnocení;“

c) písmeno j) se nahrazuje tímto:

„j) pravidla pro monitorování souladu produktů, služeb a procesů IKT nebo řízených bezpečnostních služeb s požadavky evropských certifikátů kybernetické bezpečnosti nebo EU prohlášení o shodě, včetně mechanismů prokázání pokračujícího plnění specifikovaných požadavků kybernetické bezpečnosti;“

d) písmeno l) se nahrazuje tímto:

„l) pravidla upravující důsledky pro produkty, služby a procesy IKT nebo řízené bezpečnostní služby, jež jsou certifikovány nebo pro něž bylo vydáno EU prohlášení o shodě, avšak nesplňují požadavky schématu;“;

e) písmeno o) se nahrazuje tímto:

„o) identifikaci vnitrostátních nebo mezinárodních schémat certifikace kybernetické bezpečnosti zahrnující stejné druhy nebo kategorie produktů, služeb a procesů IKT nebo řízených bezpečnostních služeb, bezpečnostní požadavky a hodnotící kritéria a metody a úrovně záruky;“

f) písmeno q) se nahrazuje tímto:

„q) dobu dostupnosti EU prohlášení o shodě, technické dokumentace a veškerých dalších relevantních informací, které má výrobce nebo poskytovatel produktů, služeb či procesů IKT nebo řízených bezpečnostních služeb mít k dispozici;“.

14) Článek 56 se mění takto:

a) odstavec 1 se nahrazuje tímto:

„1. U produktů, služeb a procesů IKT a řízených bezpečnostních služeb, které byly certifikovány v rámci evropského schématu certifikace kybernetické bezpečnosti přijatého podle článku 49, se předpokládá, že splňují požadavky daného schématu.“;

b) odstavec 3 se mění takto:

i) první pododstavec se nahrazuje tímto:

„Komise pravidelně hodnotí účinnost a využití přijatých evropských schémat certifikace kybernetické bezpečnosti, přičemž rovněž posuzuje, zda by se určité evropské schémat certifikace kybernetické bezpečnosti mělo na základě příslušných právních předpisů Unie stát povinným za účelem zajištění patřičné úrovně kybernetické bezpečnosti produktů, služeb a procesů IKT a od ... [den vstupu tohoto nařízení v platnost] řízených bezpečnostních služeb v Unii a za účelem zlepšení fungování vnitřního trhu. První takové hodnocení proběhne do 31. prosince 2023 a následná hodnocení se poté uskuteční alespoň každé dva roky. Na základě výsledku těchto hodnocení Komise z produktů, služeb a procesů IKT a řízených bezpečnostních služeb, na něž se již vztahuje stávající schéma certifikace, určí ty, na něž by se mělo vztahovat povinné schéma certifikace.“;

ii) třetí pododstavec se mění takto:

– písmeno a) se nahrazuje tímto:

„a) zohlední dopad opatření na výrobce nebo poskytovatele daných produktů, služeb či procesů IKT nebo řízených bezpečnostních služeb a na uživatele z hlediska nákladů na tato opatření a společenských nebo hospodářských přínosů plynoucích z očekávaného zvýšení úrovně bezpečnosti pro dotčené produkty, služby a procesy IKT nebo řízené bezpečnostní služby;“

– písmeno d) se nahrazuje tímto:

„d) zohlední prováděcí lhůty, přechodná opatření nebo přechodná období, zejména se zřetelem na možný dopad daného opatření na výrobce nebo poskytovatele produktů, služeb či procesů IKT nebo řízených bezpečnostních služeb, včetně specifických zájmů a potřeb malých a středních podniků, včetně mikropodniků;“;

c) odstavce 7 a 8 se nahrazují tímto:

„7. Fyzická nebo právnická osoba, která předkládá produkty, služby nebo procesy IKT nebo řízené bezpečnostní služby k certifikaci, zpřístupní vnitrostátnímu orgánu certifikace kybernetické bezpečnosti určenému podle článku 58, pokud je tento orgán subjektem vydávajícím evropský certifikát kybernetické bezpečnosti, nebo subjektu posuzování shody uvedenému v článku 60 veškeré informace nezbytné pro provedení certifikace.

8. Držitel evropského certifikátu kybernetické bezpečnosti informuje orgán či subjekt uvedený v odstavci 7 o veškerých později zjištěných zranitelnostech nebo nesrovnalostech týkajících se bezpečnosti certifikovaného produktu, služby nebo procesu IKT nebo řízené bezpečnostní služby, které by mohly mít dopad na jejich soulad s požadavky na certifikaci. Tento orgán či subjekt neprodleně tyto informace postoupí příslušnému vnitrostátnímu orgánu certifikace kybernetické bezpečnosti.“

15) V článku 57 se odstavce 1 a 2 nahrazují tímto:

„1. Aniž je dotčen odstavec 3 tohoto článku, vnitrostátní schémata certifikace kybernetické bezpečnosti a související postupy pro produkty, služby a procesy IKT a řízené bezpečnostní služby zahrnuté do evropského schématu certifikace kybernetické bezpečnosti pozbývají účinnosti ode dne stanoveného v prováděcím aktu přijatém podle čl. 49 odst. 7. Vnitrostátní schémata certifikace kybernetické bezpečnosti a související postupy pro produkty, služby a procesy IKT a řízené bezpečnostní služby, na něž se evropské schéma certifikace kybernetické bezpečnosti nevztahuje, zůstávají v platnosti.

2. Členské státy nezavedou nová vnitrostátní schémata certifikace kybernetické bezpečnosti pro produkty, služby a procesy IKT a řízené bezpečnostní služby, které jsou již zahrnuty do platného evropského schématu certifikace kybernetické bezpečnosti.“

16) Článek 58 se mění takto:

a) odstavec 7 se mění takto:

i) písmena a) a b) se nahrazují tímto:

„a) dohlížejí na pravidla zahrnutá v evropských schématech certifikace kybernetické bezpečnosti podle čl. 54 odst. 1 písm. j) pro monitorování souladu produktů, procesů, služeb a procesů IKT a řízených bezpečnostních služeb s požadavky evropských certifikátů kybernetické bezpečnosti, jež byly vydány na území jejich států, a dodržování těchto pravidel vymáhají, přičemž spolupracují s dalšími příslušnými orgány dohledu nad trhem;

b) sledují dodržování povinností výrobců a poskytovatelů produktů, služeb a procesů IKT nebo řízených bezpečnostních služeb, kteří jsou usazeni na území jejich států a kteří provádějí vlastní posuzování shody, zejména pak povinností těchto výrobců a poskytovatelů stanovených v čl. 53 odst. 2 a 3 a v odpovídajícím evropském schématu certifikace kybernetické bezpečnosti, a dodržování těchto povinností vymáhají;“

ii) písmeno h) se nahrazuje tímto:

„h) spolupracují s dalšími vnitrostátními orgány certifikace kybernetické bezpečnosti nebo jinými veřejnými orgány, mimo jiné prostřednictvím sdílení informací o možných případech nesouladu produktů, služeb a procesů IKT nebo řízených bezpečnostních služeb s požadavky tohoto nařízení nebo s požadavky konkrétních evropských schémat certifikace kybernetické bezpečnosti; a“;

b) odstavec 9 se nahrazuje tímto:

„9. Vnitrostátní orgány certifikace kybernetické bezpečnosti spolupracují mezi sebou a s Komisí, a zejména si vyměňují informace, zkušenosti a osvědčené postupy týkající se certifikace kybernetické bezpečnosti a technických otázek v oblasti kybernetické bezpečnosti, produktů, služeb a procesů IKT a řízených bezpečnostních služeb.“

17) V čl. 59 odst. 3 se písmena b) a c) nahrazují tímto:

„b) postupy dohledu nad pravidly pro monitorování souladu produktů, služeb a procesů IKT a řízených bezpečnostních služeb s evropskými certifikáty kybernetické bezpečnosti a vymáhání těchto pravidel, v souladu čl. 58 odst. 7 písm. a);

c) postupy pro sledování povinností výrobců nebo poskytovatelů produktů, služeb a procesů IKT nebo řízených bezpečnostních služeb a vymáhání těchto povinností, v souladu s čl. 58 odst. 7 písm. b);“.

18) V článku 67 se odstavce 2 a 3 nahrazují tímto:

2. Hodnocení rovněž posoudí dopad, efektivnost a účinnost ustanovení hlavy III tohoto nařízení, včetně postupů vedoucích k přijetí evropských schémat certifikace kybernetické bezpečnosti a jejich podkladových materiálů,, s ohledem na cíle zajištění odpovídající úrovně kybernetické bezpečnosti produktů, služeb a procesů IKT a řízených bezpečnostních služeb v Unii a zlepšení fungování vnitřního trhu.

3. Hodnocení posoudí, zda jsou základní požadavky na kybernetickou bezpečnost pro přístup na vnitřní trh nezbytné k tomu, aby se zabránilo produktům, službám a procesům IKT a řízeným bezpečnostním službám, které nesplňují základní požadavky na kybernetickou bezpečnost, vstupovat na trh Unie.“

19) Příloha se mění v souladu s přílohou tohoto nařízení.

Článek 2

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V ... dne ...

Za Evropský parlament	*Za Radu*
předsedkyně	*předseda/předsedkyně*

PŘÍLOHA

Příloha nařízení (EU) 2019/881 se mění takto:

1) Body 2 až 5 se nahrazují tímto:

„2. Subjekt posuzování shody musí být třetí stranou nezávislou na organizaci nebo produktech, službách či procesech IKT nebo na řízených bezpečnostních službách, které posuzuje.

3. Za subjekt posuzování shody lze považovat subjekt patřící k hospodářskému sdružení nebo profesnímu svazu zastupujícímu podniky, jež se podílejí na navrhování, výrobě, dodávání, montáži, používání nebo údržbě produktů, služeb nebo procesů IKT nebo řízených bezpečnostních služeb, které tento subjekt posuzuje, pokud je prokázána jeho nezávislost a neexistence jakéhokoli střetu zájmů.

4. Subjekty posuzování shody, jejich nejvyšší vedení a osoby odpovědné za plnění úkolů posuzování shody nesmí být osobami, které navrhují, vyrábějí, dodávají, instalují, nakupují, vlastní, používají nebo udržují posuzovaný produkt, službu či proces IKT nebo řízenou bezpečnostní službu, ani zplnomocněnými zástupci jakékoli z těchto stran. Tento zákaz nevylučuje používání posuzovaných produktů IKT, které jsou nezbytné pro činnost subjektu posuzování shody, ani používání takových produktů IKT k osobním účelům.

5. Subjekty posuzování shody, jejich nejvyšší vedení a osoby odpovědné za plnění úkolů posuzování shody se nesmí přímo podílet na navrhování, výrobě nebo konstrukci, dodávání, uvádění na trh, instalaci, používání ani údržbě posuzovaných produktů, služeb či procesů IKT nebo řízených bezpečnostních služeb, ani nesmí zastupovat strany, které se těmito činnostmi zabývají. Subjekty posuzování shody, jejich nejvyšší vedení a osoby odpovědné za plnění úkolů posuzování shody nesmí vykonávat žádnou činnost, která by mohla ohrozit jejich nezávislý úsudek nebo důvěryhodnost ve vztahu k jejich činnostem posuzování shody. Tento zákaz platí zejména pro poradenské služby.“

2) Bod 10 se mění takto:

a) návětí se nahrazuje tímto:

„10. Subjekt posuzování shody musí mít k dispozici vždy, pro každý postup posuzování shody a pro každý druh, kategorii nebo podkategorii produktů, služeb a procesů IKT nebo řízených bezpečnostních služeb, nezbytné:“;

b) písmeno c) se nahrazuje tímto:

„c) postupy pro výkon činností, jež řádně zohledňují velikost a strukturu podniku, odvětví, v němž působí, míru složitosti technologie daného produktu, služby či procesu IKT nebo řízené bezpečnostní služby a hromadnou či sériovou povahu výrobního procesu.“

3) Body 19 a 20 se nahrazují tímto:

„19. Subjekty posuzování shody plní požadavky příslušné harmonizované normy ve smyslu čl. 2 bodu 9 nařízení (ES) č. 765/2008 pro akreditaci subjektů posuzování shody provádějících certifikaci produktů, služeb a procesů IKT nebo řízených bezpečnostních služeb.

20. Subjekty posuzování shody zajistí, aby zkušební laboratoře používané pro účely posuzování shody plnily požadavky příslušné harmonizované normy ve smyslu čl. 2 bodu 9 nařízení (ES) č. 765/2008 pro akreditaci laboratoří provádějících zkoušení.“

K tomuto aktu bylo učiněno prohlášení, které lze nalézt v .. [Pro Úř. věst.: Úř. věst. C XXX, XX.XX.2024, s. XX] a na této internetové adrese: … [Pro Úř. věst.: vložte prosím odkaz na prohlášení].