C/2026/6013

17.11.2026

SDĚLENÍ KOMISE

Pokyny Evropské komise k uplatňování nařízení (EU) 2024/2847 (akt o kybernetické odolnosti)

(C/2026/6013)

Obsah

Strana

1. ÚVOD 3
   - 1.1 Akt o kybernetické odolnosti 3
   - 1.2 Účel těchto pokynů 3
2. OBLAST PŮSOBNOSTI 4
   - 2.1 Uvádění na trh 4
   - 2.2 Software jako produkt s digitálními prvky 5
   - 2.3 Počítačový kód 6
   - 2.4 Kombinace hardwaru a softwaru tvořící produkt s digitálními prvky 7
   - 2.5 Datové připojení 8
   - 2.6 Složité systémy 8
   - 2.7 Produkty s digitálními prvky, které byly navrženy před datem použitelnosti aktu 9
3. SVOBODNÝ SOFTWARE S OTEVŘENÝM ZDROJOVÝM KÓDEM 11
   - 3.1 Určení, zda daná osoba odpovídá za svobodný software s otevřeným zdrojovým kódem 12
   - 3.2 Určení, zda je svobodný software s otevřeným zdrojovým kódem uváděn na trh EU 13
     - 3.2.1 Stanovení ceny 13
     - 3.2.2 Zpeněžení dalších služeb nebo vyžadování zpracování osobních údajů 13
     - 3.2.3 Podpůrné služby 14
     - 3.2.4 Dary 15
     - 3.2.5 Financování svobodného softwaru s otevřeným zdrojovým kódem 15
     - 3.2.6 Neziskové subjekty zřízené za účelem dosažení neziskových cílů 16
     - 3.2.7 Začlenění jinými výrobci 16
   - 3.3 Správci softwaru s otevřeným zdrojovým kódem 16
     - 3.3.1 Dlouhodobá podpora a zajištění životaschopnosti svobodného softwaru s otevřeným zdrojovým kódem 17
   - 3.4 Přispěvatelé a následná využití 18
   - 3.5 Ilustrativní scénáře 19
4. PODSTATNÉ ZMĚNY A NÁHRADNÍ DÍLY 21
   - 4.1 Fyzické opravy 22
   - 4.2 Náhradní díly 23
   - 4.3 Aktualizace softwaru jako podstatné změny 24

4.4 Důsledky podstatné změny ... 27
4.4.1 Podstatné změny provedené jinou osobou než původním výrobcem ... 28
4.4.2 Podstatné změny provedené původním výrobcem ... 29
5. DOBA PODPORY ... 29
5.1 Podstatné změny a doba podpory ... 31
6. DŮLEŽITÉ A KRITICKÉ PRODUKTY S DIGITÁLNÍMI PRVKY ... 32
6.1 Klíčová funkce ... 33
6.2 Posuzování shody u důležitých a kritických produktů s digitálními prvky ... 36
6.3 Důsledky pro předpoklad shody ... 38
7. POSOUZENÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH RIZIK A ZAČLENĚNÍ PRODUKTŮ S DIGITÁLNÍMI PRVKY A KOMPONENT ... 41
7.1 O hodnocení a řešení kybernetických bezpečnostních rizik ... 41
7.2 Navrhování, vývoj a výroba produktů s digitálními prvky tak, aby byla zajištěna odpovídající úroveň kybernetické bezpečnosti zohledňující rizika ... 42
7.3 Posouzení rizik a náležitá péče v souvislosti s externími závislostmi a začleněnými komponentami ... 42
7.4 Opětovné použití posouzení rizik a dokumentace o shodě pro řady produktů s digitálními prvky ... 44
8. ZPRACOVÁNÍ DAT NA DÁLKU ... 44
8.1 Co se považuje za řešení pro zpracování dat na dálku u produktu s digitálními prvky? ... 45
8.1.1 Pojem „na dálku“ ... 46
8.1.2 Bránila by neexistence takového zpracování dat tomu, aby produkt s digitálními prvky plnil některou ze svých funkcí? ... 46
8.1.3 Byl software navržen a vyvinut výrobcem nebo odpovídá výrobce za jeho návrh a vývoj? ... 47
8.2 Praktické a technické důsledky řešení pro zpracování dat na dálku a využívání řešení třetích stran ... 49
8.3 Případy použití pro řešení pro zpracování dat na dálku ... 50
8.3.1 Aplikace pro mobilní bankovnictví ... 51
8.3.2 Chytrý termostat ... 52
8.3.3 Čtečka elektronických knih ... 53
8.3.4 Průmyslový robot ... 53
8.3.5 Mobilní síť ... 53
9. DALŠÍ PRVKY ... 54
9.1 Povinnosti podávat zprávy ... 54
9.2 Řešení zranitelností ... 56
9.2.1 Podávání zpráv výše v řetězci a sdílení bezpečnostních oprav ... 56
9.2.2 Známé zneužitelné zranitelnosti ... 57
9.2.3 Účinné a pravidelné testy a přezkumy ... 58
9.3 Vzájemný vztah s ostatními právními předpisy ... 59
9.3.1 Nařízení (EU) 2019/2144 a nařízení (EU) č. 168/2013 ... 59
9.3.2 Platnost certifikátů EU přezkoušení typu (čl. 69 odst. 1) ... 59

1. ÚVOD

1.1 Akt o kybernetické odolnosti

1. Dne 10. prosince 2024 vstoupilo v platnost nařízení Evropského parlamentu a Rady (EU) 2024/2847 ze dne 23. října 2024 o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) č. 168/2013 a (EU) 2019/1020 a směrnice (EU) 2020/1828 (akt o kybernetické odolnosti) ([1]). Cílem nařízení je posílit přístup EU ke kybernetické bezpečnosti, řešit kybernetickou odolnost na úrovni EU a zlepšit fungování vnitřního trhu tím, že stanoví jednotný právní rámec pro základní požadavky na kybernetickou bezpečnost při uvádění produktů s digitálními prvky na trh EU, jakož i během životního cyklu takového produktu.

2. Akt o kybernetické odolnosti (akt) vychází z Nového legislativního rámce EU stanoveného v nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93, a rozhodnutí Evropského parlamentu a Rady č. 768/2008/ES ze dne 9. července 2008 o společném rámci pro uvádění výrobků na trh a o zrušení rozhodnutí Rady 93/465/EHS ([2]).

3. Dozor nad trhem a prosazování právních předpisů zajišťují vnitrostátní orgány pro dozor nad trhem. Na produkty s digitálními prvky, které spadají do oblasti působnosti aktu, se vztahují ustanovení nařízení Evropského parlamentu a Rady (EU) 2019/1020 ze dne 20. června 2019 o dozoru nad trhem a souladu výrobků s předpisy a o změně směrnice 2004/42/ES a nařízení (ES) č. 765/2008 a (EU) č. 305/2011. Komise a Agentura Evropské unie pro kybernetickou bezpečnost (ENISA) podporují hospodářské subjekty a členské státy při uplatňování aktu.

1.2 Účel těchto pokynů

4. Podle požadavku čl. 26 odst. 1 aktu zveřejní Komise doporučující pokyny, které hospodářským subjektům pomohou s jeho uplatňováním, a to zejména s důrazem na usnadnění jeho dodržování ze strany mikropodniků a malých a středních podniků (MSP). Ustanovení čl. 26 odst. 2 stanoví minimální aspekty, jimiž by se pokyny měly zabývat. Patří mezi ně: i) oblast působnosti aktu (zejména řešení pro zpracování dat na dálku a svobodný software s otevřeným zdrojovým kódem); ii) pojem „doba podpory“; iii) vzájemná provázanost aktu s jinými právními předpisy EU a iv) koncept „podstatné změny“.

5. Dne 3. prosince 2025 zveřejnila Komise soubor nejčastěji kladených otázek, jejichž cílem je pomoci hospodářským subjektům připravit se na zavedení aktu ([3]).

6. Účelem těchto pokynů je pomoci hospodářským subjektům být v souladu s aktem a podpořit činnost orgánů dozoru nad trhem, oznamujících orgánů a oznámených subjektů s cílem zajistit harmonizované prosazování aktu v celé Unii. Tyto pokyny nemají pokrýt akt v plném rozsahu, ale spíše vyjasnit důvody některých klíčových ustanovení a způsoby jejich provádění v praxi. Tyto pokyny se týkají aktu a nejsou použitelné pro jiné právní předpisy EU.

([1]) Úř. věst. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

([2]) Pracovní program Komise na rok 2026 počítá s předložením „evropského aktu o výrobcích“, který aktualizuje Nový legislativní rámec a pravidla pro dozor nad trhem a normalizaci: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52025DC0870.

([3]) Často kladené otázky si lze stáhnout na speciální stránce, na niž se dostanete z webové stránky Komise věnované provádění aktu.

7. Při přípravě těchto pokynů proběhly rozsáhlé konzultace se zúčastněnými stranami, a to mimo jiné s Expertní skupinou pro kybernetickou bezpečnost produktů s digitálními prvky ([4]) a v rámci veřejné konzultace, která se konala ve dnech 3. března až 13. dubna 2026 ([5]).

8. Tyto pokyny nejsou pro hospodářské subjekty ani pro jiné subjekty, na které se akt vztahuje, závazné. Závazný výklad aktu může v konečném důsledku podat pouze Soudní dvůr Evropské unie. Tyto pokyny nicméně představují výklad aktu ze strany Komise a jejich cílem je podpořit dodržování předpisů a přispět k účinnému provádění nařízení. Kromě obsahují řadu příkladů, které ilustrují uplatňování konkrétních ustanovení. Tyto příklady však nemají nahradit posouzení každého jednotlivého případu zvlášť, které bude vždy nezbytné, aby se zohlednila specifika konkrétního případu.

9. V souladu s článkem 26 aktu může Komise zvážit vydání dalších pokynů, včetně pokynů určených výrobcům, na které se vztahuje akt i jiné harmonizační právní předpisy Unie nebo další související právní akty Unie. Těmito pokyny se mohou například řešit otázky týkající se vzájemné provázanosti aktu s nařízením (EU) 2024/1689, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (akt o umělé inteligenci), a nařízením (EU) 2022/2554 o digitální provozní odolnosti finančního sektoru (DORA).

2. **OBLAST PŮSOBNOSTI**

2.1 **Uvádění na trh**

10. Akt se vztahuje na produkty s digitálními prvky, které jsou dodávány na trh EU. Pojem „dodání na trh“ je definován v čl. 3 bodě 22 aktu jako „dodání produktu s digitálními prvky k distribuci nebo použití na trhu Unie v rámci obchodní činnosti, ať už za úplatu, nebo bezplatně“. V souladu s čl. 3 bodem 21 se produkt s digitálními prvky uvádí na trh EU v okamžiku prvního dodání.

11. Nejnovější vydání „Modré příručky k provádění pravidel EU pro výrobky“, vydané v roce 2022 (dále jen „Modrá příručka“) ([6]), poskytuje informace usnadňující pochopení předpisů EU týkajících se výrobků a jejich jednotného uplatňování v rámci různých odvětvových právních rámců, které jsou v souladu s Novým legislativním rámcem, jako je například akt. Modrá příručka uvádí, že pojmy „uvádění na trh“ a „dodávání na trh“ je třeba chápat tak, že se vztahují „na každý jednotlivý výrobek, nikoli typ výrobku, bez ohledu na to, zda je vyroben jako samostatná jednotka, nebo sériově“ (oddíl 2.3).

12. U „tradičnějších“ produktů s digitálními prvky, na které se vztahuje Nový legislativní rámec, jako je například hardware v podobě strojních zařízení nebo rádiová zařízení s digitálními prvky, je pojem „uvedení na trh“ dobře zaveden a Modrá příručka poskytuje další pokyny k objasnění toho, kdy se má za to, že jsou takové produkty uvedeny na trh. „Souhrnné příklady“ uvedené v oddíle 2.12 Modré příručky obsahují další příklady pojmu „uvádění na trh“.

13. Vzhledem k povaze nehmotných produktů s digitálními prvky, jako je například samostatný software, jsou však zapotřebí další pokyny upřesňující, kdy jsou takové produkty s digitálními prvky pokládány za uvedené na trh. Jakmile je fáze výroby softwaru dokončena a produkt s digitálními prvky je nabízen potenciálním uživatelům na trhu EU, lze mít za to, že jeho výrobce vyrobil více kopií téhož softwarového produktu s digitálními prvky a dodal je za účelem distribuce nebo použití. Na rozdíl od hmotných produktů s digitálními prvky totiž samostatný

([4]) Expertní skupina pro kybernetickou bezpečnost produktů s digitálními prvky v rejstříku expertních skupin Komise a dalších podobných subjektů.
([5]) Veřejná konzultace k návrhu pokynů Komise k aktu o kybernetické odolnosti.
([6]) Sdělení Komise „Modrá příručka“ k provádění pravidel EU pro výrobky 2022, 2022/C 247/01 (Úř. věst. C 247, 29.6.2022, s. 1).

software nepodléhá omezením fyzické výroby ani skladových zásob: Každé dodání softwaru ke stažení nebo distribuci vede k vytvoření nové totožné kopie pro uživatele. Pokud tato verze softwaru nebude upravena způsobem, který bude mít vliv na soulad s aktem, má se za to, že k uvedení na trh EU došlo v okamžiku první nabídky k distribuci nebo použití. Možnost následného stažení či distribuce této verze softwarového produktu s digitálními prvky je proto třeba považovat za případ, kdy je tento softwarový produkt s digitálními prvky dodán ([7]).

14. Samostatný softwarový produkt s digitálními prvky by proto měl být považován za uvedený na trh v okamžiku, kdy je dokončena jeho výrobní fáze a kdy je tento software poprvé dodán za účelem distribuce nebo použití na trhu EU v rámci obchodní činnosti. Je třeba vycházet z toho, že výrobce uvedl na trh současně více kopií téhož softwarového produktu s digitálními prvky. Proto i když více kopií téhož softwaru zůstává jednotlivými produkty s digitálními prvky, má se za to, že jsou uvedeny na trh současně, a to bez ohledu na to, kdy dochází k převodu držby nebo užívání každé jednotlivé kopie na jinou fyzickou nebo právnickou osobu. Zároveň platí, že pokud výrobce dodává software v různých variantách, které se liší obsaženými komponentami, konfiguracemi nebo povolenými funkcemi (například verze pro různé operační systémy nebo balíčky s odlišnými sadami funkcí), nelze tyto varianty považovat za více kopií téhož softwarového produktu s digitálními prvky. Z tohoto důvodu by se s nimi pro účely uvádění na trh mělo zacházet jako s odlišnými produkty s digitálními prvky.

Příklad 1: Dne 1. ledna 2028 společnost A poprvé dodá k distribuci prostřednictvím svých internetových stránek verzi 1.0.0 svého softwaru X. Téhož dne si zákazník 1 zakoupí kopii verze 1.0.0 softwaru X. Dne 15. ledna 2028 si zákazník 2 zakoupí kopii verze 1.0.0 softwaru X. Obě kopie verze 1.0.0 softwaru X jsou uvedeny na trh dne 1. ledna 2028.

15. Vzhledem k tomu, že vývoj softwaru je založen na opakovaných změnách, je třeba dále vyjasnit, že následné verze softwarového produktu s digitálními prvky jsou považovány za nově uvedené na trh, pokud tyto verze splňují kritéria „podstatné změny" softwarového produktu s digitálními prvky, který již byl uveden na trh, jak je uvedeno ve 41. bodě odůvodnění aktu. U verzí, které nelze považovat za podstatné změny, není výrobce povinen provést nový postup posuzování shody, a proto se tím nemění datum uvedení daného softwaru na trh. Další informace o pojmu „podstatné změny" naleznete v oddíle 4 *Podstatné změny*.

Příklad 2: Dne 1. ledna 2028 společnost A poprvé dodá k distribuci prostřednictvím svých internetových stránek verzi 1.0.0 softwaru X. Téhož dne si zákazník 1 zakoupí kopii verze 1.0.0 softwaru X. Dne 15. ledna 2028 společnost A vydá aktualizovanou verzi 1.0.1 softwaru X, která nepředstavuje podstatnou změnu. Dne 30. ledna 2028 si zákazník 2 zakoupí kopii softwaru X ve verzi 1.0.1. Obě kopie softwaru X, a to jak verze 1.0.0, tak verze 1.0.1, se považují za uvedené na trh dne 1. ledna 2028.

16. Pokyny uvedené v bodech 13, 14 a 15 se použijí výlučně v případě, že se u produktu s digitálními prvky jedná o samostatný software. To však neplatí například v situaci, kdy je software spojen s hardwarem, jak je popsáno v oddíle *2.4 Kombinace hardwaru a softwaru tvořící produkt*.

2.2 **Software jako produkt s digitálními prvky**

17. V čl. 3 bodě 1 aktu je produkt s digitálními prvky definován jako „softwarový nebo hardwarový produkt a jeho řešení pro zpracování dat na dálku, včetně softwarových nebo hardwarových komponent, které jsou uváděny na trh samostatně". Takové produkty s digitálními prvky spadají do oblasti působnosti aktu, pokud jejich zamýšlený účel nebo rozumně předvídatelné použití zahrnují přímé či nepřímé logické nebo fyzické datové připojení k zařízení nebo síti.

([7]) V souladu s čl. 13 odst. 11 mohou výrobci vést veřejné softwarové archivy, které rozšiřují přístup uživatelů k předchozím verzím. V takových případech jsou uživatelé jasně a snadno přístupným způsobem informováni o rizicích spojených s používáním nepodporovaného softwaru.

18. Akt se proto může vztahovat na celou řadu produktů s digitálními prvky, včetně těchto: i) samostatný software, jako jsou aplikace a počítačové programy, ať už distribuované v digitální nebo fyzické podobě; ii) hardware s vestavěným softwarem (např. zařízení internetu věcí, notebooky, tablety); iii) samostatný hardware (např. integrované obvody, základní desky) a iv) jakákoli kombinace hardwaru a softwaru dodávaných samostatně, avšak určených ke společnému provozu.

19. Samostatný software tedy spadá do oblasti působnosti aktu, pokud je uváděn na trh jako produkt s digitálními prvky. Je užitečné rozlišovat mezi softwarovými produkty s digitálními prvky, na které se akt vztahuje, a poskytováním služeb na dálku, které do oblasti působnosti aktu nespadají.

20. Aby software spadal do oblasti působnosti aktu, musí být uživateli poskytnut softwarový produkt s digitálními prvky, který tento uživatel získal a který je provozován v rámci elektronického informačního systému na straně uživatele nebo jako součást tohoto systému. Software, který je stažen, nainstalován nebo jinak dodán uživateli a který se spouští v elektronickém informačním systému uživatele, splňuje tato kritéria, a to i v případě, že má například podobu rozšíření prohlížeče nebo aplikace, která byla vyvinuta s využitím webových technologií, je však poskytována pro lokální provádění.

21. Naopak software, který se spouští na dálku a k němuž má uživatel pouze přístup, nelze jen na základě této skutečnosti považovat za produkt s digitálními prvky. Toto rozlišení je totiž v 11. a 12. bodě odůvodnění aktu uvedeno vysvětlením, že zpracování nebo uchovávání dat na dálku spadá do oblasti působnosti aktu pouze v rozsahu, v jakém je nezbytné k tomu, aby produkt s digitálními prvky vykonával své funkce (tj. prostřednictvím pojmu „zpracování dat na dálku“ ve smyslu čl. 3 bodu 2), a nikoli samo o sobě jako produkt s digitálními prvky. To platí zejména pro webové aplikace, včetně progresivních webových aplikací, ke kterým je přístup výhradně prostřednictvím internetového prohlížeče. Totéž platí i pro internetové stránky: ačkoli se internetové stránky mohou v omezené míře technicky spouštět a běžet na zařízení uživatele, z 12. bodu odůvodnění aktu vyplývá, že internetové stránky samy o sobě nemají být považovány za produkty s digitálními prvky a že spadají do oblasti působnosti aktu pouze tehdy, pokud podporují funkce produktu s digitálními prvky, tj. v rozsahu, v jakém je lze považovat za zpracování dat na dálku (jak je dále vysvětleno v oddíle *8* a zejména *8.1.2 Bránila by neexistence takového zpracování dat tomu, aby produkt s digitálními prvky plnil některou ze svých funkcí?*).

Příklad 3: Uživateli je dodána mobilní aplikace, kterou si stáhne z obchodu s aplikacemi a nainstaluje do svého chytrého telefonu. Aplikace se spouští v jeho zařízení, a jedná se tedy o produkt s digitálními prvky. Je-li tento produkt uveden na trh v rámci obchodní činnosti, může spadat do oblasti působnosti aktu.

Příklad 4: Uživateli je dodána desktopová aplikace vytvořená s využitím internetových technologií, avšak připravená k lokální instalaci. Aplikace se spouští v jeho zařízení, a jedná se tedy o produkt s digitálními prvky. Je-li tento produkt uveden na trh v rámci obchodní činnosti, může spadat do oblasti působnosti aktu.

Příklad 5: Internetová aplikace, ke které má uživatel přístup výhradně prostřednictvím internetového prohlížeče, není produkt s digitálními prvky. Pokud nepodporuje funkce produktu s digitálními prvky, nespadá do oblasti působnosti aktu. Naproti tomu aplikace dodaná uživateli jako lokálně nainstalovaný klient, který se spouští v zařízení uživatele, je produktem s digitálními prvky. Je-li tento produkt uveden na trh v rámci obchodní činnosti, může spadat do oblasti působnosti aktu.

Pokud se tento klient za účelem plnění jedné nebo více svých funkcí spoléhá na zpracování dat na dálku, které odpovídá definici zpracování dat na dálku, je i toto zpracování dat na dálku součástí produktu s digitálními prvky.

Příklad 6: Internetové stránky, které svým návštěvníkům pouze poskytují informace a nepodporují funkce produktu s digitálními prvky, nejsou samy o sobě produktem s digitálními prvky. Nespadají tedy do oblasti působnosti aktu.

2.3 **Počítačový kód**

22. Je rovněž užitečné objasnit, zda může zdrojový kód představovat softwarový produkt s digitálními prvky. Akt definuje software jako „část elektronického informačního systému, která sestává z počítačového kódu“ (čl. 3 bod 4). Počítačový kód může mít podobu i) strojového kódu, což je soubor instrukcí přímo prováděných procesorem počítače a zapsaných v binárním formátu, nebo ii) zdrojového kódu, tj. souboru instrukcí a příkazů napsaných v programovacím jazyce, který musí být zkompilován nebo interpretován, aby jej počítač mohl provádět. Definice softwaru stanovená v aktu zahrnuje obojí.

23. Samostatnou otázkou je, zda dané dodání počítačového kódu představuje uvedení produktu s digitálními prvky na trh EU, což vyžaduje dodání v rámci obchodní činnosti. U zdrojového kódu tomu tak často nemusí být. Například fyzická nebo právnická osoba, která sdílí svobodný počítačový kód s otevřeným zdrojovým kódem ve veřejně přístupných úložištích, se pro účely aktu obecně nepovažuje za subjekt uvádějící tento kód na trh EU (jak je podrobněji popsáno v oddíle *3 Svobodný software s otevřeným* zdrojovým kódem). Pro účely aktu se za uvedení na trh nepovažuje ani nedokončený kód sdílený během fáze návrhu a vývoje produktu s digitálními prvky (např. za účelem testování nebo kontroly), jelikož jeho výrobní fáze ještě není dokončena. Podobně se pro účely aktu nepovažuje za uvedený na trh ani vzorový nebo ukázkový kód poskytovaný jako součást výukových či školicích materiálů ([8]).

24. Na druhou stranu, pokud výrobce poskytuje svým zákazníkům počítačový kód jako produkt s digitálními prvky, má se za to, že tento kód byl uveden na trh, a to bez ohledu na to, zda se jedná o strojový kód nebo zdrojový kód ([9]).

Příklad 7: Společnost A poskytuje společnosti B licenci na zdrojový kód pro přizpůsobitelnou interní platformu a tento zdrojový kód dodává v textovém souboru. I když tento zdrojový kód před svým použitím vyžaduje další úpravy a sestavení ze strany společnosti B, společnost A tento zdrojový kód uvádí na trh, a proto se na ni vztahuje akt. Společnost A nenese odpovědnost za soulad následných úprav a sestavení tohoto kódu společností B s aktem.

2.4 **Kombinace hardwaru a softwaru tvořící produkt s digitálními prvky**

25. To, zda je software součástí produktu s digitálními prvky, by se nemělo určovat podle toho, jak nebo kdy je tento software uživateli dodán, ale podle toho, zda je tento software s ohledem na zamýšlený účel produktu a jeho rozumně předvídatelné použití nezbytný k tomu, aby produkt s digitálními prvky plnil zamýšlené funkce. Je-li hardwarový produkt s digitálními prvky navržen tak, aby k plnění svých funkcí fungoval s konkrétním softwarem, který dodává stejný výrobce, tvoří tento hardware a uvedený software společně produkt s digitálními prvky. Software, který je nezbytný k provozu, konfiguraci, ovládání nebo používání produktu s digitálními prvky v souladu s jeho zamýšleným účelem, je tudíž součástí produktu s digitálními prvky, i když je získán prostřednictvím samostatného kanálu (např. z obchodu s aplikacemi, na odkazu ke stažení nebo prostřednictvím jiného digitálního kanálu poté, co byl hardwarový produkt s digitálními prvky uveden na trh). Jeho uvedení na trh se tedy uskutečňuje ve stejném okamžiku, kdy jsou na trh uvedeny jednotky hardwarových produktů s digitálními prvky.

Příklad 8: Síťová tiskárna je uvedena na trh jako hardwarový produkt s digitálními prvky, zatímco softwarové ovladače potřebné k odesílání tiskových úloh, konfiguraci zařízení a správě jeho provozu jsou dodávány ke stažení na internetových stránkách výrobce. Ačkoli jsou tiskárna a ovladače dodávány různými kanály, tvoří společně jeden produkt s digitálními prvky, protože tiskárna nemůže bez ovladačů plnit svůj zamýšlený účel.

Příklad 9: Na trh je uvedeno nositelné fitness zařízení, které měří srdeční frekvenci a aktivitu uživatele, přičemž k zobrazení naměřených hodnot a historie a ke konfiguraci zařízení je nutná aplikace pro chytré telefony poskytovaná výrobcem. Ačkoli se aplikace stahuje samostatně z obchodu s aplikacemi, nositelné zařízení a aplikace tvoří společně jeden produkt s digitálními prvky, protože jsou navrženy a určeny k tomu, aby fungovaly společně a zajišťovaly danou funkci produktu s digitálními prvky.

([8]) Je třeba rovněž připomenout, že čl. 4 odst. 3 umožňuje výrobcům dodávat na trh nedokončený software, který není v souladu s nařízením, jako jsou alfa verze, beta verze nebo kandidáti na vydání, pokud je tento nedokončený software dodáván pouze po dobu nezbytnou k jeho otestování a získání zpětné vazby.

([9]) Na druhou stranu je třeba poznamenat, že pro účely práva týkajícího se odpovědnosti za výrobky nepředstavuje samotný počítačový kód výrobek, a proto výrobci, kteří takový kód uvádějí na trh, nemohou být podle směrnice (EU) 2024/2853 (směrnice o odpovědnosti za vadné výrobky) považováni za odpovědné. Podle 13. bodu odůvodnění této směrnice „[z]a výrobek však nelze považovat informace, a pravidla odpovědnosti za vadné výrobky by se proto neměla vztahovat na obsah digitálních souborů, jako jsou mediální soubory nebo elektronické knihy nebo pouhý zdrojový kód softwaru“. To však nevylučuje, že výrobci mohou nést odpovědnost podle vnitrostátního práva v oblasti občanskoprávní odpovědnosti.

2.5 **Datové připojení**

26. Ustanovení čl. 2 odst. 1 uvádí, že se akt „vztahuje na produkty s digitálními prvky dodané na trh, jejichž zamýšlený účel nebo rozumně předvídatelné použití zahrnuje přímé nebo nepřímé logické nebo fyzické datové připojení k zařízení nebo síti“. Oblast působnosti aktu tedy nespočívá pouze v přítomnosti elektronických součástek, ale ve schopnosti produktu s digitálními prvky vyměňovat si digitální informace.

27. Ačkoli jsou v článku 3 definovány pojmy „logické připojení“ a „fyzické připojení“, akt nedefinuje pojmy „datové připojení“ ani „digitální data“. Je proto užitečné vyložit, co se rozumí pod pojmem „datové připojení“, aby byly vyjasněny hranice oblasti působnosti aktu. Tyto hranice jsou obzvláště důležité pro rozlišení produktů s digitálními prvky, které pouze využívají elektrické signály, od těch, které se podílejí na digitální komunikaci, a jsou proto vystaveny kybernetickým bezpečnostním rizikům.

28. V nejzákladnější rovině spočívá datové připojení v přenosu informací v binární podobě, tj. jako posloupnost nul a jedniček. Samotné zapínání a vypínání výstupu (tj. 0/1) ještě neznamená datové připojení, pokud tyto stavy nemají představovat data nebo nejsou snímány digitálním vstupem. Aby mohlo dojít k datovému připojení, musí být binární stavy záměrně zakódovány zdrojem jako informace a musí být možné je na přijímací straně dekódovat jako informace. Jinými slovy, musí existovat odesílatel, který záměrně generuje digitální symboly podle definovaného schématu, a příjemce schopný tyto symboly interpretovat jako data. Pokud se elektrické nebo elektronické signály používají výhradně ke spuštění nebo napájení určité funkce, aniž by přenášely digitálně kódované informace, neexistuje pro účely aktu žádné datové připojení, a proto produkt s digitálními prvky nespadá do oblasti působnosti čl. 2 odst. 1.

2.6 **Složité systémy**

29. Produkty s digitálními prvky spadající do oblasti působnosti aktu mohou sestávat nejen z jednotlivých zařízení nebo softwarových komponent, ale také ze složitých systémů, včetně systémů složených z více hardwarových a softwarových prvků, které společně plní určitou funkci. Je-li takový systém uváděn na trh jako samostatný produkt s digitálními prvky, představuje produkt s digitálními prvky ve smyslu aktu.

30. Takové složité systémy se často vyznačují dlouhými cykly návrhu a vývoje, dlouhou provozní životností a vysokou mírou technické a organizační složitosti, přičemž související smlouvy mohly být uzavřeny ještě před datem použitelnosti aktu. Tyto systémy, které mají být uvedeny na trh po datu použitelnosti aktu, mohou využívat komponenty uvedené na trh před tímto datem, zavedené architektury nebo široce používané standardy interoperability, včetně standardů, na které odkazují jiné právní předpisy EU nebo odvětvové rámce. V důsledku toho může být obtížné nebo nepřiměřené upravit některé technické charakteristiky těchto systémů, aniž by to mělo dopad na jejich zamýšlený účel, bezpečnost, spolehlivost nebo interoperabilitu se stávající infrastrukturou.

31. Tyto charakteristiky samy o sobě nevylučují složité systémy z oblasti působnosti aktu. Spíše ilustrují uplatnění přístupu aktu založeného na riziku, což umožňuje prokázat soulad různými způsoby v závislosti na charakteristikách a omezeních produktu s digitálními prvky, a to v souladu s čl. 13 odst. 3 aktu. Tyto charakteristiky jsou součástí zamýšleného účelu a provozního kontextu, a jsou proto relevantní při posuzování souladu se základními požadavky na kybernetickou bezpečnost (dále jen „základní požadavky“). Zejména v 55. bodě odůvodnění se výslovně uznává, že některé základní požadavky nemusí být plně slučitelné s povahou produktu s digitálními prvky. To může být například případ, kdy by soulad ohrozil závazné požadavky na interoperabilitu nebo řádné fungování systému.

32. V souladu s tím jsou výrobci povinni řešit kybernetická bezpečnostní rizika na základě jejich posouzení podle čl. 13 odst. 2. Jak je rovněž vysvětleno v 55. bodě odůvodnění, v některých případech se konkrétní základní požadavky neuplatňují nebo je nelze splnit zavedením nejmodernějších bezpečnostních opatření, a to například z důvodu

zamýšleného účelu systému, který vyžaduje, aby produkt s digitálními prvky interagoval se stávajícími závislostmi nebo splňoval určité požadavky na interoperabilitu. V takových případech by výrobci měli tato konkrétní omezení identifikovat a zdokumentovat, posoudit rizika s nimi spojená a zavést vhodná alternativní nebo kompenzační opatření ke snížení rizik, aby nedošlo k ohrožení bezpečnosti produktu s digitálními prvky. Pro tyto účely hrají klíčovou roli jak technická dokumentace uvedená v článku 31, tak informace a pokyny pro uživatele uvedené v příloze II, které transparentně popisují zjištěná omezení, související kybernetická bezpečnostní rizika a zavedená opatření ke zmírnění rizik. V souladu s povinností udržovat posouzení rizik v aktuálním stavu po celou dobu poskytování podpory by výrobci měli rovněž pravidelně opětovně posuzovat, zda tato omezení existují i nadále. Pokud lze tato omezení v průběhu času odstranit nebo zmírnit, měli by výrobci produkt s digitálními prvky odpovídajícím způsobem aktualizovat, aby bylo možné dosáhnout odpovídající úrovně kybernetické bezpečnosti ([10]).

Příklad 10: Výrobce uvede na trh produkt s digitálními prvky, který komunikuje s externími systémy pomocí síťového protokolu. V rámci uplatňování základních požadavků výrobce na základě posouzení kybernetických bezpečnostních rizik stanoví, že k zajištění důvěrnosti a integrity dat, která si produkt s digitálními prvky vyměňuje, je nezbytné použít bezpečný komunikační protokol.

Mezi zamýšlené účely produktu s digitálními prvky však patří i interoperabilita se stávajícími systémy, které podporují pouze starší nebo méně bezpečný protokol. V takových případech může výrobce tento protokol zavést, je-li to nezbytné pro zajištění interoperability, pokud související kybernetická bezpečnostní rizika budou identifikována a zmírněna jinými prostředky.

Pokud je z technického hlediska možné, aby produkt s digitálními prvky podporoval jak bezpečný protokol, tak méně bezpečný protokol, očekává se, že výrobce zavede bezpečný protokol a nastaví jeho použití jako výchozí. Méně bezpečný protokol by byl povolen pouze v případech, kdy je to nezbytné pro interoperabilitu.

Příklad 11: Výrobce systému průmyslové automatizace nakoupí určité mikrořadiče ještě před datem použitelnosti aktu. Výrobce provede posouzení kybernetických bezpečnostních rizik u svého systému průmyslové automatizace, který má být uveden na trh po datu použitelnosti aktu. Na základě tohoto posouzení kybernetických bezpečnostních rizik výrobce nezjistil žádná konkrétní kybernetická bezpečnostní rizika spojená s používáním jednoho z těchto mikrořadičů. Výrobce jej integruje do svého systému průmyslové automatizace a zajistí, aby produkt s digitálními prvky jako celek (systém průmyslové automatizace) splňoval základní požadavky.

2.7 **Produkty s digitálními prvky, které byly navrženy před datem použitelnosti aktu**

33. V některých případech uvede výrobce na trh po datu použitelnosti aktu dne 11. prosince 2027 jednotky produktu s digitálními prvky, které byly vyrobeny v souladu s typem nebo modelem navrženým a vyvinutým před datem použitelnosti aktu. V takových případech soulad s tímto nařízením nutně nevyžaduje, aby byly tyto jednotky produktu s digitálními prvky, přepracovány. Výrobce je povinen provést posouzení kybernetických bezpečnostních rizik v souladu s čl. 13 odst. 2 aktu, aby na základě zamýšleného účelu a rozumně předvídatelného použití produktu s digitálními prvky určil, které ze základních požadavků stanovených v části I přílohy I se na tento produkt s digitálními prvky vztahují a jak jsou tyto požadavky naplňovány.

34. Pokud výsledek tohoto posouzení rizik prokáže, že produkt s digitálními prvky již vhodná a účinná bezpečnostní opatření řešící příslušná rizika obsahuje, může se výrobce opřít o tato stávající opatření s cílem prokázat soulad s aktem. Akt sám o sobě neukládá povinnost zavádět nové bezpečnostní prvky ani přepracovat produkt s digitálními prvky, pokud to není nezbytné k řešení zjištěných rizik.

([10]) Je třeba poznamenat, že úvahy uvedené v tomto odstavci se mohou případně vztahovat na všechny produkty s digitálními prvky spadající do oblasti působnosti aktu, a nikoli pouze na „složité systémy“.

35. Na výrobce se však i nadále vztahují povinnosti stanovené v aktu. Mezi ně patří zajištění toho, aby před uvedením produktu s digitálními prvky na trh byl proveden příslušný postup posouzení shody, aby bylo vyhotoveno EU prohlášení o shodě a aby bylo připojeno označení CE. Splnění těchto požadavků nezávisí na tom, zda bylo v důsledku posouzení rizik nutné změnit návrh produktu s digitálními prvky. U produktů s digitálními prvky, které byly sice navrženy před datem použitelnosti aktu, ale na trh byly uvedeny až po tomto datu, pokud výrobce není schopen prokázat, jak bylo posouzení rizik zohledněno během fáze návrhu a vývoje produktu s digitálními prvky, je třeba povinnost podle čl. 13 odst. 2 chápat tak, že výrobci jsou povinni provést posouzení kybernetických bezpečnostních rizik a na základě toho prokázat, že produkt s digitálními prvky obsahuje přiměřená bezpečnostní opatření s cílem minimalizovat kybernetická bezpečnostní rizika, předcházet incidentům a minimalizovat jejich dopad, a to i ve vztahu ke zdraví a bezpečnosti uživatelů.

36. V souladu s tím mohou být produkty s digitálními prvky, které byly navrženy před datem použitelnosti aktu, uvedeny na trh podle aktu bez nutnosti přepracování návrhu za předpokladu, že výrobce může prostřednictvím posouzení kybernetických bezpečnostních rizik a technické dokumentace prokázat, že produkt s digitálními prvky dosahuje přiměřené úrovně kybernetické bezpečnosti s ohledem na svůj zamýšlený účel a rozumně předvídatelné použití a splňuje základní požadavky na kybernetickou bezpečnost.

37. Dále je užitečné vyjasnit uplatňování povinností v oblasti posuzování shody u výrobců produktů s digitálními prvky, které jsou uváděny na trh po datu použitelnosti aktu, které jsou však vyráběny v souladu s typem nebo modelem navrženým a vyvinutým před tímto datem. V souladu s čl. 13 odst. 12 je výrobce povinen prostřednictvím příslušného postupu posuzování shody prokázat, že jeho produkt s digitálními prvky je v souladu s příslušnými základními požadavky, a příslušné důkazy o tom zahrnout do technické dokumentace k produktu (bod 6 přílohy VII).

38. Uplatňování těchto požadavků je však třeba vykládat s ohledem na posouzení kybernetických bezpečnostních rizik a na profil kybernetických bezpečnostních rizik u daného produktu s digitálními prvky. Zejména v případě produktů s digitálními prvky, které byly navrženy před datem použitelnosti aktu (ale uvedeny na trh až po tomto datu) a na které se vztahují postupy posuzování shody podle čl. 32 odst. 1, pokud posouzení rizik prokáže, že produkt s digitálními prvky již obsahuje vhodná a účinná bezpečnostní opatření řešící rizika daného produktu, neměla by být povinnost předložit důkazy v rámci postupu posuzování shody chápána tak, že výrobce je povinen předložit výsledky zkoušek zaměřených na původní fáze návrhu a vývoje takových produktů s digitálními prvky. To by nebylo nutné, protože by to samo o sobě nepřispívalo ke zvýšení bezpečnosti produktu s digitálními prvky. V případech, kdy mohou být testy přesto nezbytné, se od výrobců neočekává, že předloží důkazy o zkouškách provedených na všech variantách produktů, ale mohou tyto zkoušky seskupit v rámci skupin produktů s digitálními prvky, jak je podrobněji popsáno v oddíle *7.4 Opětovné použití posouzení rizik a dokumentace o shodě pro řady produktů s digitálními prvky*.

39. Výrobce by nicméně měl předložit důkazy o tom, jak dodržuje postupy pro řešení zranitelností stanovené v části II přílohy I, měl by své posouzení rizik průběžně aktualizovat v souladu s čl. 13 odst. 3 a plnit všechny ostatní povinnosti stanovené v aktu, včetně poskytování informací a pokynů uživatelům v souladu s čl. 13 odst. 18.

Příklad 12: Výrobce uvádí na trh mikrořadič, který byl navržen a vyvinut před datem použitelnosti aktu. Mikrořadič má být zabudován do řady elektronických produktů s digitálními prvky, včetně produktů s digitálními prvky vybavených funkcemi pro připojení.

Před uvedením nových jednotek mikrořadičů na trh po datu použitelnosti aktu provede výrobce posouzení kybernetických bezpečnostních rizik v souladu s čl. 13 odst. 2. Na základě zamýšleného účelu mikrořadiče a jeho rozumně předvídatelného použití identifikuje výrobce příslušná kybernetická bezpečnostní rizika, jako je neoprávněný přístup, manipulace se softwarem nebo daty a zneužití dostupných rozhraní.

Výsledky posouzení rizik ukazují, že mikrořadič podle původního návrhu již obsahuje vhodná a účinná bezpečnostní opatření, která řeší zjištěná rizika. Výrobce proto dojde k závěru, že produkt s digitálními prvky splňuje příslušné základní požadavky stanovené v části I přílohy I a že není nutné provádět žádné úpravy návrhu ani zavádět další bezpečnostní funkce.

Pokud nelze prokázat, jakým způsobem bylo posouzení kybernetických bezpečnostních rizik zohledněno během původní fáze návrhu a vývoje, zdokumentuje výrobce aktuální posouzení kybernetických bezpečnostních rizik a vysvětlí, jak stávající návrh a opatření zjištěná rizika zmírňují. Výrobce není povinen znovu vyhotovit dokumentaci předchozího návrhu nebo zkoušek, jelikož by to nepřispělo ke zvýšení kybernetické bezpečnosti produktu s digitálními prvky. Pokud je několik variant mikrořadiče založeno na stejném návrhu a vykazuje stejný profil kybernetických bezpečnostních rizik, může se výrobce rovněž opřít o reprezentativní důkazy týkající se příslušné skupiny produktů.

Výrobce rovněž zajišťuje dodržování požadavků na řešení zranitelností stanovených v části II přílohy I, a to mimo jiné udržováním postupů pro řešení a nápravu zranitelností a průběžným přezkumem posouzení kybernetických bezpečnostních rizik v souladu s čl. 13 odst. 3.

Za těchto okolností lze mikrořadič navržený před datem použitelnosti aktu uvést na trh bez nutnosti přepracování návrhu, pokud výrobce může prostřednictvím posouzení kybernetických bezpečnostních rizik a technické dokumentace prokázat, že tento mikrořadič dosahuje přiměřené úrovně kybernetické bezpečnosti s ohledem na svůj zamýšlený účel a rozumně předvídatelné použití a splňuje příslušné základní požadavky.

3. **SVOBODNÝ SOFTWARE S OTEVŘENÝM ZDROJOVÝM KÓDEM**

40. Jak je uvedeno v oddíle *2.1 Uvádění na trh*, akt se vztahuje na produkty s digitálními prvky, které jsou v rámci obchodní činnosti poprvé dodány na trh EU (tj. „uvedeny na trh"), jakož i na jakýkoli následný případ, který představuje dodání téhož produktu s digitálními prvky na trh. Modrá příručka (oddíl 2.2) objasňuje, že pod „obchodní činností" se rozumí poskytování zboží v rámci podnikání, ať už za úplatu či bezplatně, a lze ji posuzovat pouze v každém jednotlivém případě s přihlédnutím k pravidelnosti dodávek, vlastnostem výrobku, záměrům dodavatele atd.

41. Dodávka v rámci obchodní činnosti se vyznačuje řadou okolností, které jsou podrobně popsány v Modré příručce a na které odkazuje 15. bod odůvodnění aktu. Dodávání v rámci obchodní činnosti může být charakterizováno přímým stanovením ceny i „stanovením ceny za technické podpůrné služby, která neslouží pouze k úhradě skutečných nákladů, se záměrem zpeněžení, například poskytnutím softwarové platformy, jejímž prostřednictvím výrobce zpeněžuje jiné služby, stanovením, že podmínkou použití je zpracovávání osobních údajů z jiných důvodů, než je výlučně zlepšení bezpečnosti, kompatibility nebo interoperability softwaru, nebo přijímáním darů v hodnotě přesahující náklady spojené s navrhováním, vývojem a dodáváním produktu s digitálními prvky" (15. bod odůvodnění) ([11]).

42. Akt však bere v úvahu specifika různých způsobů vývoje a zveřejňování „svobodného softwaru s otevřeným zdrojovým kódem" a nabízí určité pokyny, které pomáhají určit, zda se v případě svobodného softwaru s otevřeným zdrojovým kódem jedná o produkt s digitálními prvky uváděný na trh (tj. v rámci obchodní činnosti) ve smyslu aktu. Jak je vysvětleno v 18. bodě odůvodnění, „při určování komerční nebo nekomerční povahy této činnosti by […] neměly být brány v úvahu pouze okolnosti, za nichž byl produkt s digitálními prvky vyvinut, nebo způsob financování jeho vývoje". Konkrétněji „by pro účely tohoto nařízení a ve vztahu k hospodářským subjektům, které spadají do jeho oblasti působnosti, nemělo být za obchodní činnost považováno poskytování produktů s digitálními prvky představujících svobodný software s otevřeným zdrojovým kódem, které není jejich výrobci zpeněženo; takto bude zajištěno jasné rozlišení mezi fází vývoje a fází dodávání".

([11]) Je třeba rovněž připomenout, že ačkoli jsou produkty s digitálními prvky často zpeněžovány (také) prostřednictvím zpracování osobních údajů, ochrana osobních údajů je základním právem, a osobní údaje tudíž nemohou být považovány za komoditu, jak je uvedeno ve 24. bodě odůvodnění směrnice Evropského parlamentu a Rady (EU) 2019/770 ze dne 20. května 2019 o některých aspektech smluv o poskytování digitálního obsahu a digitálních služeb (Úř. věst. L 136, 22.5.2019, s. 1, ELI: http://data.europa.eu/eli/dir/2019/770/oj).

43. Je proto užitečné i) objasnit, co je svobodný software s otevřeným zdrojovým kódem; ii) kdy se má za to, že spadá do oblasti odpovědnosti fyzické nebo právnické osoby; a iii) uvést příklady, které zúčastněným stranám pomohou pochopit, kdy distribuce svobodného softwaru s otevřeným zdrojovým kódem představuje uvedení na trh. Pokud není svobodný software s otevřeným zdrojovým kódem uváděn na trh, nespadá do oblasti působnosti aktu, ledaže by subjekt, který jej zveřejňuje, byl právnickou osobou splňující definici „správce softwaru s otevřeným zdrojovým kódem“ (dále jen „správce“) podle čl. 3 bodu 14. V takovém případě se na něj vztahují pouze povinnosti stanovené v článku 24.

44. V čl. 3 bodě 48 je svobodný software s otevřeným zdrojovým kódem definován jako „software, jehož zdrojový kód je volně sdílen a který je zpřístupněn na základě licence k svobodnému softwaru s otevřeným zdrojovým kódem, jež poskytuje veškerá práva na to, aby byl volně přístupný, použitelný, upravitelný a dále distribuovatelný“. Ačkoli tyto pokyny neuvádějí konkrétní licence k svobodnému softwaru s otevřeným zdrojovým kódem, které jsou v souladu s definicí stanovenou v čl. 3 bodu 48, ze znění tohoto ustanovení vyplývá, že pro účely aktu lze za svobodný software s otevřeným zdrojovým kódem považovat pouze software, který souběžně splňuje dvě podmínky: i) software musí být dodáván na základě licence k svobodnému softwaru s otevřeným zdrojovým kódem, která uděluje veškerá práva uvedená v čl. 3 bodu 48; a ii) jeho zdrojový kód musí být volně sdílen.

45. Požadavek, aby licence zajišťovala, že software bude „volně přístupný, použitelný, upravitelný a dále distribuovatelný“, odráží tradiční pojetí svobodného softwaru s otevřeným zdrojovým kódem, a sice že uživatelé musí mít možnost získat přístup ke zdrojovému kódu, používat jej bez nepřiměřeného omezení, upravovat jej a šířit původní či upravené verze. Přístup ke zdrojovému kódu je proto nezbytnou podmínkou pro uplatnění ostatních práv: Bez přístupu ke zdrojovému kódu není prakticky možné software upravovat ani smysluplně znovu použít.

46. V případě čl. 3 bodu 48 však nejde pouze o pouhé odkázání na licenční podmínky, neboť článek výslovně požaduje, aby byl zdrojový kód „volně sdílen“. Pojem „volně sdílen“ znamená, že zdrojový kód musí být veřejně zpřístupněn (ať už v původním projektu („upstream“), nebo v navazujícím projektu či distribuci („downstream“)), a nesmí být poskytován pouze na základě omezení či podmínek. V souladu s tím nelze software distribuovaný na základě licence k svobodnému softwaru s otevřeným zdrojovým kódem, jehož zdrojový kód je však sdílen (nebo jehož sdílení je povoleno) pouze s platícími zákazníky nebo omezenou skupinou uživatelů, považovat za svobodný software s otevřeným zdrojovým kódem ve smyslu čl. 3 bodu 48. Pro účely aktu by proto měl být za svobodný software s otevřeným zdrojovým kódem považován pouze software, jehož zdrojový kód je volně dostupný a který je poskytován na základě licence k svobodnému softwaru s otevřeným zdrojovým kódem, která uděluje plný rozsah práv uvedených v čl. 3 bodu 48.

3.1 **Určení, zda daná osoba odpovídá za svobodný software s otevřeným zdrojovým kódem**

47. Akt ukládá klíčové povinnosti hospodářským subjektům, které dodávají produkty s digitálními prvky na trh EU. Výrobce definuje jako fyzickou nebo právnickou osobu, která dodává produkt s digitálními prvky pod svým jménem nebo ochrannou známkou a činí tak v rámci obchodní činnosti (čímž jej uvádí na trh). Podobně se dovozcem rozumí fyzická nebo právnická osoba usazená v Unii, která dodává produkt s digitálními prvky od osoby usazené mimo EU a činí tak v rámci obchodní činnosti (čímž jej uvádí na trh). Povinnosti správců se vztahují na právnickou osobu, která dodává svobodný software s otevřeným zdrojovým kódem určený pro obchodní činnost ([12]), avšak neuvádí jej na trh ve smyslu aktu.

48. Aby bylo tedy možné určit, zda fyzická nebo právnická osoba uvádí svobodný software s otevřeným zdrojovým kódem na trh EU, je třeba nejprve objasnit, zda tato fyzická nebo právnická osoba takový software skutečně dodává. Pro správné určení povinností vyplývajících z aktu je nezbytné stanovit, zda fyzická nebo právnická osoba skutečně vykonává činnost spočívající v dodávání svobodného softwaru s otevřeným zdrojovým kódem. Jak je ostatně uvedeno v 18. bodě odůvodnění, akt se nevztahuje na fyzické ani právnické osoby, které přispívají zdrojovým kódem k produktům s digitálními prvky považovaným za svobodný software s otevřeným zdrojovým kódem, za něž však nenesou odpovědnost.

([12]) Jedná se o nezbytnou, nikoli však postačující podmínku pro to, aby se právnická osoba mohla kvalifikovat jako správce softwaru s otevřeným zdrojovým kódem, neboť definice uvedená v čl. 3 bodě 14 stanoví další podmínky, které musí právnická osoba splnit, aby se mohla kvalifikovat jako správce.

49. Vzhledem ke specifikům vývoje svobodného softwaru s otevřeným zdrojovým kódem, který často zahrnuje řadu přispěvatelů, decentralizované modely spolupráce a oddělení samotného přispívání od rozhodování, je užitečné upřesnit, že svobodný software s otevřeným zdrojovým kódem je považován za produkt, za který „odpovídají" fyzické nebo právnické osoby, které jej zveřejňují a vykonávají primární kontrolu nad jeho vývojem, vydáváním a rozhodováním o distribuci (často označované jako „udržovatelé"). Osoby, které přispívají zdrojovým kódem, ale nemají kontrolu nad vydáváním, plány vývoje ani rozhodnutími týkajícími se řízení projektu, se považují za „přispěvatele"; v takových případech za tento svobodný software s otevřeným zdrojovým kódem nenesou odpovědnost, i když do něj přispěly kódem. Samotná existence technických oprávnění, jako je například zápisový přístup (*commit access*), nestačí k tomu, aby bylo možné konstatovat, že daná osoba nese za daný svobodný software s otevřeným zdrojovým kódem odpovědnost; ta leží na těch, kdo tento svobodný software s otevřeným zdrojovým kódem vydávají a mají nad ním kontrolu.

Příklad 13: Jednotlivý vývojář nebo zaměstnanec společnosti předloží žádost o začlenění změn obsahující bezpečnostní opravu nebo novou funkci projektu svobodného softwaru s otevřeným zdrojovým kódem. Osoby, které v rámci projektu software udržují, kód zkontrolují, schválí a začlení do hlavního úložiště, aby jej následně zahrnuly do nového vydání. V tomto scénáři je osoba, která podala žádost o začlenění změn, „přispěvatelem" a akt se na ni nevztahuje. Ačkoli tato osoba přispěla zdrojovým kódem, nemá primární kontrolu nad vývojem, vydáváním ani rozhodnutími o distribuci.

3.2 **Určení, zda je svobodný software s otevřeným zdrojovým kódem uváděn na trh EU**

50. Jakmile se prokáže, že za svobodný software s otevřeným zdrojovým kódem nese odpovědnost fyzická nebo právnická osoba, je třeba zjistit, zda jej tato osoba dodává v rámci obchodní činnosti, což by představovalo uvedení na trh.

3.2.1 *Stanovení ceny*

51. Pokud fyzická nebo právnická osoba, která poskytuje svobodný software s otevřeným zdrojovým kódem, účtuje cenu za samotný software (např. tím, že účtuje cenu za předkompilované binární soubory), uvádí tato osoba na trh produkt s digitálními prvky. Osoba, která uvádí svobodný software s otevřeným zdrojovým kódem na trh, je tedy podle aktu výrobcem.

52. Výrobci svobodného softwaru s otevřeným zdrojovým kódem často poskytují bezplatné verze tohoto softwaru (často označované jako „komunitní" verze), jejichž zdrojový kód je (téměř) totožný se zdrojovým kódem placené verze. Tyto produkty s digitálními prvky jsou však jiné produkty: placená verze je nějakým způsobem zpeněžena (např. buď stanovením ceny, nebo jinými způsoby, jak je rozebráno v tomto oddíle), a má se tudíž za to, že byla uvedena na trh, čímž vznikají povinnosti výrobce. Verze poskytovaná zdarma (neboli komunitní verze) zpeněžována není, a proto se pro účely aktu za uvedenou na trh nepovažuje. To platí i v případě, kdy je placená verze „vylepšenou" komerční verzí, která rozšiřuje kódovou základnu bezplatně poskytované verze nebo tuto verzi začleňuje do širšího produktu s digitálními prvky (např. jako v případě modelu „open-core").

53. Je-li poskytovatelem komunitní verze právnická osoba, vztahují se na ni rovněž povinnosti správců, a to v souvislosti s verzí, kterou poskytuje bezplatně (komunitní verzí). Je-li subjektem fyzická osoba, bezplatná verze (komunitní verze) do oblasti působnosti aktu nespadá.

3.2.2 *Zpeněžení dalších služeb nebo vyžadování zpracování osobních údajů*

54. Fyzická nebo právnická osoba, která zveřejňuje svobodný software s otevřeným zdrojovým kódem, může tento software rovněž uvádět na trh (tj. dodávat jej v rámci obchodní činnosti), pokud poskytuje software, jehož prostřednictvím zpeněžuje jiné produkty s digitálními prvky nebo služby, nebo pokud jako podmínku pro jeho používání vyžaduje zpracování osobních údajů z jiných důvodů než výlučně za účelem zlepšení bezpečnosti, kompatibility nebo interoperability softwaru.

Příklad 14: Fyzická nebo právnická osoba zveřejní svobodnou aplikaci s otevřeným zdrojovým kódem určenou pro tržiště. Aplikace je k dispozici zdarma a jejím prostřednictvím mohou uživatelé nakupovat zboží nebo služby. Aplikace umožňuje osobě, která ji zveřejnila, zpeněžit další produkty s digitálními prvky a služby nabízené prostřednictvím této aplikace (např. prostřednictvím reklam, provizí nebo poplatků za předplatné). Aplikace se proto považuje za uvedenou na trh v rámci obchodní činnosti.

Příklad 15: Fyzická nebo právnická osoba zveřejní svobodnou VPN s otevřeným zdrojovým kódem. Aplikace je k dispozici zdarma, ale uživatelé si mohou zaplatit přístup k dalším serverům nebo vyhrazeným IP adresám. Tato aplikace umožňuje dané osobě zpeněžit další služby, které jsou jejím prostřednictvím nabízeny, a proto se má za to, že je uvedena na trh v rámci obchodní činnosti.

Příklad 16: Fyzická nebo právnická osoba zveřejní svobodnou aplikaci s otevřeným zdrojovým kódem určenou pro sledování fyzické kondice. Aplikace je k dispozici zdarma, její používání je však podmíněno zpracováním osobních údajů uživatelů pro takové účely, jako je cílená reklama nebo analytika, které nesouvisí s bezpečností, kompatibilitou ani interoperabilitou softwaru. Tím, že aplikace vyžaduje takové zpracování údajů jako podmínku pro její používání, má se za to, že je uvedena na trh v rámci obchodní činnosti.

3.2.3 *Podpůrné služby*

55. Pouhá skutečnost, že fyzická nebo právnická osoba, která zveřejňuje svobodný software s otevřeným zdrojovým kódem, nabízí také placené služby podpory související s tímto softwarem, ještě sama o sobě neznamená, že produkt s digitálními prvky je dodáván v rámci obchodní činnosti. Podpůrné služby mohou zahrnovat činnosti, jako je poradenství, odborná příprava nebo odborné služby související s používáním, dokumentací, konfigurací a nasazením softwaru ze strany zákazníka.

56. Rozhodujícím faktorem je, zda je přístup k samotnému svobodnému softwaru s otevřeným zdrojovým kódem (tj. poskytnutí produktu s digitálními prvky), včetně jeho údržby, podmíněn úhradou, nikoli pouhá nabídka odborných služeb souvisejících s volně dostupným produktem s digitálními prvky, jak je uvedeno v 18. bodě odůvodnění aktu („za obchodní činnost [by nemělo být] považováno poskytování produktů s digitálními prvky představujících svobodný software s otevřeným zdrojovým kódem, které není jejich výrobci zpeněženo“). Pokud lze svobodný software s otevřeným zdrojovým kódem bezplatně stáhnout a nainstalovat a uživatelé mají možnost si případně samostatně zakoupit odborné služby, nepovažuje se tento svobodný software s otevřeným zdrojovým kódem za uvedený na trh.

57. Naopak v některých případech je přístup ke konkrétní verzi produktu s digitálními prvky, včetně určitých výhod, jako je technická podpora nebo optimalizace výkonu, podmíněn úhradou. V takových případech se jedná o zpeněžené poskytnutí produktu s digitálními prvky v rámci obchodní činnosti, a proto se toto poskytnutí považuje za uvedení na trh. Patří sem i případy, kdy je placená edice nebo podniková verze poskytována na základě komerční smlouvy, a to bez ohledu na to, zda je funkčně ekvivalentní software k dispozici také bezplatně na základě licence k svobodnému softwaru s otevřeným zdrojovým kódem.

Příklad 17: Fyzická nebo právnická osoba zveřejní svobodný operační systém s otevřeným zdrojovým kódem a nabízí jeho placenou verzi, která zahrnuje podpůrné služby, jako je technická podpora nebo optimalizace výkonu. Placená verze operačního systému je považována za uvedenou na trh v rámci obchodní činnosti.

Příklad 18: Fyzická nebo právnická osoba zveřejňuje svobodný nástroj s otevřeným zdrojovým kódem určený pro příkazový řádek. Tento nástroj je volně dostupný a kdokoli si jej může stáhnout a nainstalovat. Tato fyzická nebo právnická osoba samostatně nabízí odborné služby, jako jsou například volitelné poradenské služby zaměřené na školení uživatelů a podporu při instalaci a používání tohoto nástroje. Tento svobodný software s otevřeným zdrojovým kódem se nepovažuje za uvedený na trh ve smyslu aktu.

58. Zejména v případě fyzických osob, které vydávají svobodný software s otevřeným zdrojovým kódem, by nabízení technické podpory přímo spojené s přístupem k produktu s digitálními prvky stále nebylo považováno za obchodní činnost, pokud, jak uvádí 15. bod odůvodnění aktu, účtovaná cena slouží pouze k úhradě skutečných nákladů. Mezi tyto skutečné náklady patří řada výdajů spojených s návrhem, vývojem a údržbou daného softwaru, včetně přiměřených životních nákladů dané osoby. Fyzická osoba, která zveřejňuje svobodný software s otevřeným zdrojovým kódem a nabízí technickou podporu za účelem pokrytí svých nákladů a získání spravedlivé odměny, proto nesmí být pouze na základě této skutečnosti považována za subjekt uvádějící tento software na trh EU.

59. Fyzická nebo právnická osoba, která nabízí technickou pomoc související se svobodným softwarem s otevřeným zdrojovým kódem, za který nenese odpovědnost, se nepovažuje za subjekt uvádějící tento software na trh, ledaže by v rámci poskytování této pomoci podstatně změnila daný svobodný software s otevřeným zdrojovým kódem v souladu s článkem 22.

Příklad 19: Poskytovatel služeb nezveřejňuje svobodný software s otevřeným zdrojovým kódem, ale pomáhá zákazníkovi s jeho instalací na jeho místním serveru. Děje se tak bez provedení podstatné změny tohoto svobodného softwaru s otevřeným zdrojovým kódem. Poskytovatel služby se proto nepovažuje za subjekt, který uvádí svobodný software s otevřeným zdrojovým kódem na trh.

3.2.4 *Dary*

60. Fyzické nebo právnické osoby, které zveřejňují projekty svobodného softwaru s otevřeným zdrojovým kódem, obvykle poskytují uživatelům tohoto softwaru možnost dobrovolně přispět peněžní částkou, a to jednak jako poděkování vydavateli či vydavatelům projektu, jednak s cílem zajistit, aby byl projekt i nadále aktivně udržován.

61. Jak je uvedeno v 15. bodě odůvodnění aktu, „[p]řijímání darů bez záměru vytvářet zisk by nemělo být považováno za obchodní činnost“. Samotná skutečnost, že je v obsahu uveden odkaz na dárcovskou platformu nebo podobné nástroje sloužící k výběru darů, by neměla být považována za záměr dosáhnout zisku, a to ani v případě, že částka získaná prostřednictvím darů převyšuje pouhé náklady spojené s návrhem, vývojem a poskytováním produktu s digitálními prvky. To zahrnuje přiměřenou odměnu pro přispěvatele najaté právnickou osobou a/nebo přiměřené životní náklady fyzické osoby. Dary nepředstavují ze své podstaty stabilní příjem, a proto je třeba při posuzování, zda lze svobodný software s otevřeným zdrojovým kódem, jehož financování je založeno výhradně na darech, považovat za uvedený na trh, postupovat s určitou mírou flexibility. Je tudíž nepravděpodobné, že by byl svobodný software s otevřeným zdrojovým kódem podporovaný výhradně z darů považován za uvedený na trh ve smyslu aktu.

Příklad 20: Fyzická nebo právnická osoba zveřejní svobodný softwarový nástroj s otevřeným zdrojovým kódem ve veřejném online úložišti, čímž umožní komukoli jej stáhnout, používat, upravovat a dále distribuovat na základě licence k svobodnému softwaru s otevřeným zdrojovým kódem. Vydavatel vyzývá uživatele, aby prostřednictvím dárcovské platformy poskytovali dobrovolné dary na podporu dalšího vývoje a údržby projektu. Přístup k softwaru, jeho zdrojovému kódu a aktualizacím není podmíněn poskytnutím daru. Tento svobodný software s otevřeným zdrojovým kódem se nepovažuje za dodávaný v rámci obchodní činnosti ani za uvedený na trh ve smyslu aktu.

62. Přesto však existují případy, kdy lze svobodný software s otevřeným zdrojovým kódem financovaný z darů považovat za uvedený na trh. Jedná se o případ, kdy na základě celkového posouzení okolností jsou dary vlastně rovnocenné stanovení ceny za přístup k produktu s digitálními prvky nebo k některým z jeho funkcí. To může platit zejména v případech, kdy je přístup k svobodnému softwaru s otevřeným zdrojovým kódem, k základním funkcím nebo k aktualizacím v praxi podmíněn poskytnutím daru nebo kdy jsou dary spojeny se smluvními výhodami či exkluzivními zvýhodněními, která přesahují rámec výhod poskytovaných komunitou.

Příklad 21: Fyzická nebo právnická osoba vydává softwarový produkt s digitálními prvky pod licencí k svobodnému softwaru s otevřeným zdrojovým kódem, avšak verze ke stažení a bezpečnostní aktualizace poskytuje pouze uživatelům, kteří poskytnou dar. Uživatelé, kteří neposkytnou dar, nemají přístup k aktuální verzi softwaru.

V tomto případě jsou dary de facto podmínkou přístupu k produktu s digitálními prvky, a představují tedy stanovení ceny. Tento svobodný software s otevřeným zdrojovým kódem se proto považuje za uvedený na trh ve smyslu aktu.

Příklad 22: Fyzická nebo právnická osoba zpřístupní zdrojový kód svobodného softwaru s otevřeným zdrojovým kódem veřejnosti, avšak předkompilované binární soubory, pravidelné aktualizace a zaručené bezpečnostní opravy poskytuje pouze dárcům. V tomto případě jsou dary spojeny s přístupem k základním aspektům produktu s digitálními prvky a představují odměnu za dodání tohoto produktu. Tento svobodný software s otevřeným zdrojovým kódem se proto považuje za uvedený na trh v rámci obchodní činnosti.

3.2.5 *Financování svobodného softwaru s otevřeným zdrojovým kódem*

63. Pouhá skutečnost, že třetí strana zaplatila, sponzorovala nebo jinak financovala vývoj svobodného softwaru s otevřeným zdrojovým kódem, sama o sobě neurčuje, zda je tento software uveden na trh. V ekosystému svobodného softwaru s otevřeným zdrojovým kódem je běžnou praxí, že jednotliví vývojáři, nadace či komunity získávají finanční prostředky od společností, veřejných orgánů nebo jiných sponzorů za účelem práce na konkrétních funkcích, oprav chyb nebo údržby klíčových komponent. Toto financování může mít mnoho podob, včetně grantů, odměn za nalezení chyb, sponzorských příspěvků, smluv o poskytování služeb nebo placené vývojářské práce.

64. Jak již bylo připomenuto, 18. bod odůvodnění aktu vyjasňuje, že při určování komerční povahy této činnosti by neměly být brány v úvahu pouze okolnosti, za nichž byl produkt s digitálními prvky vyvinut, nebo způsob financování jeho vývoje.

65. Proto v případech, kdy je svobodný software s otevřeným zdrojovým kódem otevřeně sdílen a všichni k němu mají volný přístup a mohou jej používat, upravovat a redistribuovat, by skutečnost, že za daný projekt případně zaplatil komerční subjekt, neměla přispívat k určení, zda je tento software uváděn na trh. Ve skutečnosti platí, že pokud tento svobodný software s otevřeným zdrojovým kódem není jinak zpeněžen, za uvedený na trh se nepovažuje. Pokud společnost, která financovala vývoj svobodného softwaru s otevřeným zdrojovým kódem (stejně jako jakákoli jiná společnost), začlení tento software do svého produktu s digitálními prvky, je v souladu s čl. 13 odst. 5 aktu povinna postupovat s náležitou péčí.

Příklad 23: Individuální vývojář zveřejní projekt svobodného softwaru s otevřeným zdrojovým kódem a aktivně jej udržuje. Výrobce A požádá tohoto individuálního vývojáře, aby do daného svobodného softwaru s otevřeným zdrojovým kódem přidal určitou funkci, a tento vývoj financuje. Vývojář přidá tuto funkci do kódové základny svobodného softwaru s otevřeným zdrojovým kódem, otevřeně ji sdílí a volně ji dodává, takže všichni k ní mají přístup a mohou ji používat, upravovat a redistribuovat. Individuální vývojář se proto nepovažuje za subjekt, který uvádí svobodný software s otevřeným zdrojovým kódem na trh. Pokud výrobce začlení svobodný software s otevřeným zdrojovým kódem do svého produktu s digitálními prvky, je v souladu s čl. 13 odst. 5 povinen postupovat s náležitou péčí.

3.2.6 *Neziskové subjekty zřízené za účelem dosažení neziskových cílů*

66. Je-li právnická osoba zveřejňující svobodný software s otevřeným zdrojovým kódem neziskovou organizací, která „byla zřízena takovým způsobem, aby bylo zajištěno, že veškeré příjmy po odečtení nákladů budou použity k dosažení neziskových cílů“ (18. bod odůvodnění aktu), nepovažuje se svobodný software s otevřeným zdrojovým kódem, který tato organizace zveřejňuje, za uvedený na trh. Pokud tato právnická osoba splňuje definici pojmu „správce“, vztahují se na ni odpovídající povinnosti (článek 24 aktu).

Příklad 24: Právnická osoba vydá svobodný prohlížeč s otevřeným zdrojovým kódem, který je přímo zpeněžen prostřednictvím partnerství s vyhledávači, avšak veškeré její výnosy po odečtení nákladů jsou využívány k neziskovým cílům. Prohlížeč se nepovažuje za uvedený na trh ve smyslu aktu. Na právnickou osobu, která jej zveřejňuje, se vztahují povinnosti platné pro správce.

3.2.7 *Začlenění jinými výrobci*

67. V některých případech je svobodný software s otevřeným zdrojovým kódem zveřejněn jasně identifikovatelnou fyzickou nebo právnickou osobou, avšak tento software je „[určen] k začlenění jinými výrobci do jejich vlastních produktů s digitálními prvky“. V takových případech se má za to, že daný svobodný software s otevřeným zdrojovým kódem není uveden na trh EU, pokud jej osoba, která jej zveřejňuje (tj. původní výrobce), zároveň nezpeněžuje, a to v souladu s předchozími oddíly těchto pokynů.

68. Pokud není daný svobodný software s otevřeným zdrojovým kódem uváděn na trh, vztahovaly by se na právnickou osobu, která jej zveřejňuje, povinnosti správců, pokud v souladu s definicí pojmu „správce“ poskytuje dlouhodobou podporu.

Příklad 25: Právnická osoba zveřejňuje svobodnou softwarovou knihovnu s otevřeným zdrojovým kódem určenou k tvorbě uživatelských rozhraní. Dodávání této knihovny sice nezpeněžuje, ale začleňuje ji do jednoho ze svých produktů s digitálními prvky (který je následně uváděn na trh). Knihovna se nepovažuje za uvedenou na trh ve smyslu aktu, je však určena k začlenění do produktů s digitálními prvky. Právnická osoba, která ji zveřejňuje, je jejím správcem.

Příklad 26: Právnická osoba uvádí na trh operační systém a zároveň zveřejňuje svobodné softwarové knihovny s otevřeným zdrojovým kódem, které slouží jako referenční implementace pro uživatele tohoto operačního systému. Právnická osoba nezpeněžuje svobodné softwarové knihovny s otevřeným zdrojovým kódem, které jsou určeny k začlenění do jiných produktů s digitálními prvky. Právnická osoba, která je zveřejňuje, je správcem těchto knihoven.

3.3 **Správci softwaru s otevřeným zdrojovým kódem**

69. S ohledem na to, že „mnoho produktů s digitálními prvky, které jsou považovány za svobodný software s otevřeným zdrojovým kódem a které jsou zveřejňovány, ale nejsou dodávány na trh ve smyslu [aktu], má význam pro kybernetickou bezpečnost“ (19. bod odůvodnění aktu), zavádí akt novou právní kategorii „správce softwaru s otevřeným zdrojovým kódem“.

70. V některých případech je svobodný software s otevřeným zdrojovým kódem zveřejněn, avšak není dodán na trh ve smyslu aktu právnickou osobou, „jejímž účelem nebo cílem je systematicky a dlouhodobě podporovat vývoj [svobodného softwaru s otevřeným zdrojovým kódem] […] [určeného] pro obchodní činnost, a která zajišťuje životaschopnost těchto produktů“ (čl. 3 bod 14 aktu). V takových případech se na tuto právnickou osobu vztahují povinnosti správců.

71. Správce je definován jako „právnická osoba jiná než výrobce“, protože výrobce je ze své podstaty fyzická nebo právnická osoba, která uvádí produkty s digitálními prvky na trh („nabízí je“) pod svým jménem nebo ochrannou známkou. Právnická osoba může být správcem pouze u produktů s digitálními prvky považovaných za svobodný software s otevřeným zdrojovým kódem, které jsou zveřejněny, avšak nejsou dodávány na trh ve smyslu aktu. Pojem správce se tedy vztahuje na konkrétní případy svobodného softwaru s otevřeným zdrojovým kódem, které „jsou v konečném důsledku určeny pro obchodní činnost, například pro začlenění do komerčních služeb nebo do zpeněžovaných produktů s digitálními prvky“ (19. bod odůvodnění aktu ([13])), které však nejsou dodávány na trh ve smyslu aktu a pro které právnická osoba, jež tento svobodný software s otevřeným zdrojovým kódem zveřejňuje, zajišťuje systematickou podporu.

72. Skutečnost, že určitá právnická osoba je správcem jednoho konkrétního svobodného softwaru s otevřeným zdrojovým kódem, neznamená, že je nutně správcem dalších svobodných softwarů s otevřeným zdrojovým kódem, které zveřejňuje. Podobně i skutečnost, že určitá právnická osoba je výrobcem jednoho konkrétního svobodného softwaru s otevřeným zdrojovým kódem, neznamená, že nemůže být správcem dalších takových svobodných softwarů. To zahrnuje poskytování „komunitních“ verzí téhož svobodného softwaru s otevřeným zdrojovým kódem, jak je popsáno v oddíle *3.2.1 Stanovení ceny*.

73. Právnická osoba tedy může být současně správcem jednoho konkrétního svobodného softwaru s otevřeným zdrojovým kódem (kdy správce systematicky poskytuje dlouhodobou podporu a zajišťuje životaschopnost softwaru) a výrobcem jiného konkrétního svobodného softwaru s otevřeným zdrojovým kódem (kdy jej uvádí na trh). Jinými slovy, od téže právnické osoby může být vyžadováno, aby v rámci různých projektů svobodného softwaru s otevřeným zdrojovým kódem plnila různé role.

74. U každého konkrétního svobodného softwaru s otevřeným zdrojovým kódem, který zveřejňuje, bude právnická osoba muset ověřit, zda je tento svobodný software s otevřeným zdrojovým kódem považován za uvedený na trh ve smyslu aktu. Pokud ano, znamená to, že tato právnická osoba je výrobcem daného softwaru. Pokud se svobodný software s otevřeným zdrojovým kódem nepovažuje za uvedený na trh, může být jeho správcem tato právnická osoba, a to za předpokladu, že je tento software určen pro obchodní činnost a že jej daná právnická osoba spravuje v souladu s definicí správce ([14]).

3.3.1 *Dlouhodobá podpora a zajištění životaschopnosti svobodného softwaru s otevřeným zdrojovým kódem*

75. V 19. bodě odůvodnění je uvedeno, že poskytování dlouhodobé podpory vývoji produktu s digitálními prvky může zahrnovat (mimo jiné): i) hosting a správu platforem pro spolupráci v oblasti vývoje softwaru; ii) hosting zdrojového kódu nebo softwaru; iii) správu nebo řízení produktů s digitálními prvky, které jsou považovány za svobodný software s otevřeným zdrojovým kódem, a iv) směrování vývoje takových produktů s digitálními prvky.

76. To může platit například pro právnickou osobu, která vyvíjí svobodný software s otevřeným zdrojovým kódem za účelem jeho začlenění do svých vlastních produktů s digitálními prvky a následně jej zveřejňuje, aniž by jej uvedla na trh. Této problematice se věnuje také oddíl *3.2.7 Začlenění jinými výrobci*. V tomto případě není právnická osoba výrobcem softwaru, ale může být jeho správcem. Kromě toho, jak již bylo vysvětleno v předchozích oddílech, právnická osoba, která zveřejňuje bezplatnou (nebo komunitní) verzi a zpeněžovanou verzi téhož svobodného softwaru s otevřeným zdrojovým kódem, je považována za správce bezplatné (nebo komunitní) verze a za výrobce zpeněžované verze.

77. Podobně právnická osoba, která svobodný software s otevřeným zdrojovým kódem zpeněžuje, avšak je neziskovým subjektem, jehož výnosy po odečtení nákladů jsou využívány k dosažení neziskových cílů (a jejíž svobodný software s otevřeným zdrojovým kódem tedy není uveden na trh ve smyslu aktu, jak je rozebráno v oddíle *3.2.6 Neziskové subjekty*), je správcem svobodného softwaru s otevřeným zdrojovým kódem, který zveřejňuje.

78. Navíc některé nadace nabízejí platformy pro spolupráci s různými formami řízení, které výrobcům umožňují pravidelně přispívat k vývoji svobodného softwaru s otevřeným zdrojovým kódem a/nebo které jsou pravidelně financovány výrobci. Tyto nadace je třeba považovat za správce v souvislosti s konkrétními svobodnými softwary s otevřeným zdrojovým kódem, které jsou určeny pro obchodní činnost a pro které nadace nabízí dlouhodobou podporu. Jak je však vysvětleno v oddíle *3.3 Správci softwaru s* otevřeným zdrojovým kódem, na takovou nadaci se nemusí vztahovat žádné povinnosti vyplývající z aktu v souvislosti s jiným konkrétním svobodným softwarem s otevřeným zdrojovým kódem, který hostuje, a to v případech, kdy neposkytuje systematickou podporu pro konkrétní svobodný software s otevřeným zdrojovým kódem, nezajišťuje jeho životaschopnost a/nebo pokud tento konkrétní software není určen pro obchodní činnost.

([13]) Tento pojem je rovněž obsažen ve formulaci „určených pro obchodní činnost“, která je součástí definice pojmu „správce softwaru s otevřeným zdrojovým kódem“ uvedené v čl. 3 bodě 14 aktu.

([14]) Na právnickou osobu se rovněž nemusí vztahovat žádné povinnosti vyplývající z aktu v případech, kdy: i) konkrétní svobodný software s otevřeným zdrojovým kódem není uveden na trh ve smyslu aktu a ii) daná právnická osoba nesplňuje v souvislosti s tímto konkrétním svobodným softwarem s otevřeným zdrojovým kódem definici správce.

79. Typ „dlouhodobé podpory“, kterou nadace a podobné organizace poskytují konkrétním projektům svobodného softwaru s otevřeným zdrojovým kódem, se může značně lišit. Například některé právnické osoby poskytují pouze netechnickou podporu, jako je správa značky projektů, stanovení pravidel řízení, organizování komunitních akcí nebo výběr darů. Další subjekty poskytují též podkladovou IT infrastrukturu, která je nezbytná pro chod projektu, například hosting úložišť zdrojových kódů, poskytování systémů pro správu verzí nebo generování podpisových klíčů. Jiné subjekty jdou ve své podpoře ještě dál a aktivně do projektu vnášejí technické zdroje, například tím, že zaměstnávají vývojáře, koordinují vývojářské práce, provádějí revize kódu nebo kód slučují, spravují vydání nebo zpracovávají hlášení o zranitelnosti a zajišťují bezpečnostní opravy. Zatímco všechny právnické osoby, které podle aktu lze považovat za správce, jsou povinny plnit povinnosti stanovené v čl. 24 odst. 1 a 2, rozsah, v jakém se povinnosti stanovené v čl. 14 odst. 1, 3 a 8 vztahují na tyto právnické osoby, se liší v závislosti na typu podpory, kterou poskytují, v souladu s čl. 24 odst. 3.

80. Například správce, který poskytuje pouze netechnickou podporu, se ze své podstaty nepodílí na vývoji produktu s digitálními prvky, a proto není povinen hlásit aktivně zneužívané zranitelnosti. Tento správce rovněž neposkytuje žádné síťové a informační systémy pro vývoj takových produktů s digitálními prvky, a není tudíž povinen hlásit závažné incidenty agentuře ENISA, týmům pro reakce na počítačové bezpečnostní incidenty ani dotčeným uživatelům. Pokud se však správce dozví o aktivně zneužívané zranitelnosti (např. na základě hlášení z externích zdrojů, jako jsou bezpečnostní výzkumníci), měl by tuto informaci sdílet s osobami, které produkt s digitálními prvky udržují, v souladu se svou politikou kybernetické bezpečnosti. Osoby, které produkty s digitálními prvky udržují, a/nebo správci by rovněž měli zvážit, zda tuto zranitelnost nahlásí dobrovolně v souladu s článkem 15.

81. Na druhou stranu, pokud správce zajišťuje podkladovou IT infrastrukturu pro určité produkty s digitálními prvky, je povinen v souladu s čl. 14 odst. 3 oznámit agentuře ENISA a týmům pro reakce na počítačové bezpečnostní incidenty veškeré závažné incidenty související s touto infrastrukturou, které mají dopad na bezpečnost produktů s digitálními prvky. V příslušných případech je rovněž nutné informovat všechny uživatele (např. formou obecného oznámení). Jak bylo uvedeno v předchozím bodě, ačkoli správce není povinen hlásit aktivně zneužívané zranitelnosti, o nichž se dozví, měl by podporovat správné zacházení se zranitelnostmi a zvážit dobrovolné hlášení v souladu s článkem 15.

82. A konečně, pokud správce poskytuje technické zdroje také pro konkrétní produkty s digitálními prvky, je povinen: i) v souladu s čl. 14 odst. 1 oznámit aktivně zneužívané zranitelnosti, o nichž se dozví; a ii) v případě potřeby informovat všechny uživatele. V případě, že správce má rovněž přímý vztah k dotčeným uživatelům, je také v souladu s čl. 14 odst. 8 povinen informovat je o tom přímo.

83. Pokud subjekt přestane poskytovat systematickou a dlouhodobou podporu konkrétnímu svobodnému softwaru s otevřeným zdrojovým kódem, nemusí již splňovat definici správce, a nemusí proto být nadále vázán příslušnými povinnostmi. V takových případech se danému subjektu doporučuje, aby jasně informoval o změně svého postavení v souvislosti s tímto konkrétním svobodným softwarem s otevřeným zdrojovým kódem.

84. V určitých situacích se subjekt, který byl správcem konkrétního projektu, může rozhodnout tento projekt přímo zpeněžit, čímž uvede produkt s digitálními prvky na trh a mohou tak být uplatněny povinnost výrobce vyplývající z aktu. Za těchto okolností se tento subjekt považuje za výrobce produktu s digitálními prvky ode dne, kdy jej uvede na trh (nikoli však v případě dřívějších verzí, u nichž působil jako správce).

3.4 **Přispěvatelé a následná využití**

85. Jak bylo již uvedeno v oddíle *3.1 Určení, zda daná osoba odpovídá za* svobodný software s otevřeným zdrojovým kódem, akt objasňuje, že se nevztahuje „na fyzické ani právnické osoby, které přispívají zdrojovým kódem k produktům s digitálními prvky, jež jsou považovány za svobodný software s otevřeným zdrojovým kódem, za něž nenesou odpovědnost“ (18. bod odůvodnění).

86. Výrobci produktů s digitálními prvky, kteří do svých vlastních produktů s digitálními prvky začleňují komponenty svobodného softwaru s otevřeným zdrojovým kódem, se rovněž nestávají odpovědnými za to, zda tyto komponenty jednotlivě splňují požadavky aktu, a to ani v případě, že tito výrobci přispívají zdrojovým kódem k jejich údržbě.

87. Stejně tak pouhá skutečnost, že výrobci začleňují komponenty svobodného softwaru s otevřeným zdrojovým kódem do svých vlastních (zpeněžovaných) produktů s digitálními prvky, nemá žádný dopad na právní status dané komponenty podle aktu. Osoby, jež udržují komponenty svobodného softwaru s otevřeným zdrojovým kódem, které nejsou uváděny na trh, nemají žádné povinnosti vůči jiným subjektům, které mohou tyto komponenty začlenit do svých produktů s digitálními prvky. To, zda se na danou komponentu svobodného softwaru s otevřeným zdrojovým kódem vztahuje akt, závisí výhradně na tom, zda ji fyzická nebo právnická osoba, která ji zveřejňuje, uvádí na trh.

88. Výrobci produktů s digitálními prvky, které obsahují komponenty svobodného softwaru s otevřeným zdrojovým kódem, jsou nicméně povinni dodržovat ustanovení aktu u svých vlastních produktů s digitálními prvky. V souladu s čl. 13 odst. 5 mají rovněž povinnost náležité péče, pokud jde o komponenty svobodného softwaru s otevřeným zdrojovým kódem, které začleňují. Kromě toho jsou povinni hlásit zranitelnosti v začleněných komponentách a sdílet bezpečnostní opravy v souladu s čl. 13 odst. 6. Více pokynů k tomuto tématu najdete v oddíle *9.2.1 Podávání zpráv výše v řetězci a* sdílení bezpečnostních oprav.

3.5 **Ilustrativní scénáře**

89. Níže uvedené příklady jsou zcela hypotetické a jejich účelem je pouze ilustrovat různé případy vysvětlené ve výše uvedených oddílech.

Příklad 27: Individuální vývojář A vyvinul svobodný software s otevřeným zdrojovým kódem. Vývojář A zveřejní tento svobodný software s otevřeným zdrojovým kódem pod svým vlastním jménem nebo ochrannou známkou, ale za jeho používání neúčtuje žádnou cenu. Tento software je otevřeně sdílen a všichni k němu mají volný přístup a mohou jej používat, upravovat a redistribuovat. Vývojář A rovněž uvádí odkaz na platformu pro výběr dobrovolných darů.

Společnosti B, C a D začleňují tento svobodný software s otevřeným zdrojovým kódem do svých vlastních produktů s digitálními prvky. Za účelem podpory průběžné údržby poskytují společnosti B, C a D vývojáři A dobrovolné dary. Tyto mu umožňují projekt aktivně udržovat.

Tento svobodný software s otevřeným zdrojovým kódem není uváděn na trh ve smyslu aktu. Vývojář A nemá podle aktu žádné povinnosti. Společnosti B, C a D jsou v souladu s čl. 13 odst. 5 povinny při začleňování tohoto svobodného softwaru s otevřeným zdrojovým kódem do svých vlastních produktů s digitálními prvky postupovat s náležitou péčí.

Příklad 28: Nezisková nadace F zveřejňuje komponentu svobodného softwaru s otevřeným zdrojovým kódem určenou k začlenění do jiných komerčních produktů s digitálními prvky. Nadace F se zavazuje poskytovat tomuto svobodnému softwaru s otevřeným zdrojovým kódem dlouhodobou podporu, aby zajistila jeho životaschopnost a využívání. Společnosti A, B a C tento svobodný software s otevřeným zdrojovým kódem začleňují do svých vlastních produktů s digitálními prvky. Společnosti A a B dobrovolně přispívají částí času svých vývojářů k vývoji a údržbě projektů svobodného softwaru s otevřeným zdrojovým kódem v rámci nadace F, včetně tohoto svobodného softwaru.

Jelikož nadace F je nezisková organizace zřízená tak, že její výnosy po odečtení nákladů slouží k dosažení neziskových cílů, nepovažuje se svobodný software s otevřeným zdrojovým kódem za produkt uvedený na trh ve smyslu aktu. Nadace F je správcem svobodného softwaru s otevřeným zdrojovým kódem a vztahují se na ni odpovídající povinnosti stanovené v článku 24. Společnosti A, B a C jsou v souladu s čl. 13 odst. 5 povinny při začleňování tohoto svobodného softwaru s otevřeným zdrojovým kódem do svých vlastních produktů s digitálními prvky postupovat s náležitou péčí.

Příklad 29: Společnost A vyvinula komponentu svobodného softwaru s otevřeným zdrojovým kódem k začlenění do svých vlastních produktů s digitálními prvky. Tento svobodný software s otevřeným zdrojovým kódem také zveřejňuje samostatně pod svým vlastním názvem nebo ochrannou známkou a aktivně jej udržuje. Za jeho používání však neúčtuje žádné poplatky ani jej nezpeněžuje jinými způsoby. Společnosti B, C a D začleňují tento svobodný software s otevřeným zdrojovým kódem do svých vlastních produktů s digitálními prvky a dobrovolně přispívají částí času svých vývojářů k jeho údržbě.

Tento svobodný software s otevřeným zdrojovým kódem se nepovažuje za uvedený na trh ve smyslu aktu. Společnost A není jeho výrobcem, ale je jeho správcem. Společnosti B, C a D jsou v souladu s čl. 13 odst. 5 povinny při začleňování tohoto svobodného softwaru s otevřeným zdrojovým kódem do svých vlastních produktů s digitálními prvky postupovat s náležitou péčí.

Příklad 30: Společnost A zveřejní svobodný software s otevřeným zdrojovým kódem pod svým vlastním jménem nebo ochrannou známkou a nabízí jej jako placenou verzi, která zahrnuje určité výhody, například technickou podporu nebo optimalizaci výkonu. Vývojáři ze společností B, C a D přispívají k údržbě tohoto svobodného softwaru s otevřeným zdrojovým kódem, ten však zůstává pod kontrolou společnosti A.

Společnost A je považována za výrobce tohoto svobodného softwaru s otevřeným zdrojovým kódem ([15]). *Společnosti B, C a D nemají v souvislosti s tímto konkrétním svobodným softwarem s otevřeným zdrojovým kódem žádné povinnosti vyplývající z aktu. Pokud tento svobodný software s otevřeným zdrojovým kódem začleňují do svých vlastních produktů s digitálními prvky, jsou v souladu s čl. 13 odst. 5 povinny postupovat s náležitou péčí.*

Příklad 31: Společnost A zveřejňuje svobodný software s otevřeným zdrojovým kódem pod svým vlastním jménem nebo ochrannou známkou a zajišťuje jeho průběžnou údržbu, aby byla zaručena jeho dlouhodobá životaschopnost a aby bylo možné tento software začlenit do produktů s digitálními prvky od jiných společností. Společnost A neúčtuje za jeho používání žádné poplatky, nezpracovává osobní údaje, které shromažďuje prostřednictvím produktu s digitálními prvky, ani neprodává podpůrné služby spojené se zveřejňováním tohoto svobodného softwaru s otevřeným zdrojovým kódem.

Společnost B přispívá k údržbě tohoto svobodného softwaru s otevřeným zdrojovým kódem poskytováním kódu a času svých vývojářů, ale tento software komerčně nedistribuuje. Společnost B nabízí nezávisle na distribuci tohoto svobodného softwaru služby technické podpory. Společnost A je považována za správce tohoto softwaru, zatímco společnost B nemá podle aktu v souvislosti s tímto softwarem žádné povinnosti.

Příklad 32: Komponenta svobodného softwaru s otevřeným zdrojovým kódem je zveřejněna neziskovým subjektem zřízeným tak, aby bylo zajištěno, že veškeré výnosy po odečtení nákladů budou použity k dosažení neziskových cílů. Tento subjekt poskytuje dlouhodobou podporu s cílem zajistit dlouhodobou životaschopnost projektu. Údržba je financována z veřejných prostředků, například z výzkumných grantů. Další vývoj, včetně nových funkcí, je financován z darů a v rámci konkrétních projektů realizovaných v partnerství s výrobci, kteří tento svobodný software s otevřeným zdrojovým kódem začleňují do svých produktů s digitálními prvky. Tyto funkce jsou začleněny do kódové základny svobodného softwaru s otevřeným zdrojovým kódem.

Nezisková organizace, která daný svobodný software s otevřeným zdrojovým kódem zveřejňuje, je považována za správce této komponenty softwaru. Výrobce, který přispěl k vývoji některých funkcí, se nestává výrobcem této komponenty softwaru. Pokud výrobce začlení tuto komponentu softwaru do svého vlastního produktu s digitálními prvky, musí v souladu s čl. 13 odst. 5 postupovat s náležitou péčí.

Příklad 33: Neziskový subjekt zřízený tak, aby bylo zajištěno, že veškeré výnosy po odečtení nákladů budou použity k dosažení neziskových cílů, zveřejňuje sadu nástrojů pro vývoj softwaru (SDK), která je svobodným softwarem s otevřeným zdrojovým kódem, a zajišťuje její průběžnou údržbu. Sada SDK je otevřeně sdílena a všichni k ní mají volný přístup a mohou ji používat, upravovat a redistribuovat. Financování je zajištěno prostřednictvím členských příspěvků placených neziskovému subjektu a vývojáři zaměstnaní členskými organizacemi přispívají k vývoji sady SDK kódem a dalšími zdroji. Výrobci využívají sadu SDK jako komponentu k vývoji dalších produktů s digitálními prvky.

Nezisková organizace, která tuto sadu SDK zveřejňuje, je jejím správcem. Členové nadace nenesou odpovědnost za soulad sady SDK s aktem. Pokud výrobci využívají sadu SDK k vývoji vlastního produktu s digitálními prvky, musí v souladu s čl. 13 odst. 5 postupovat s náležitou péčí.

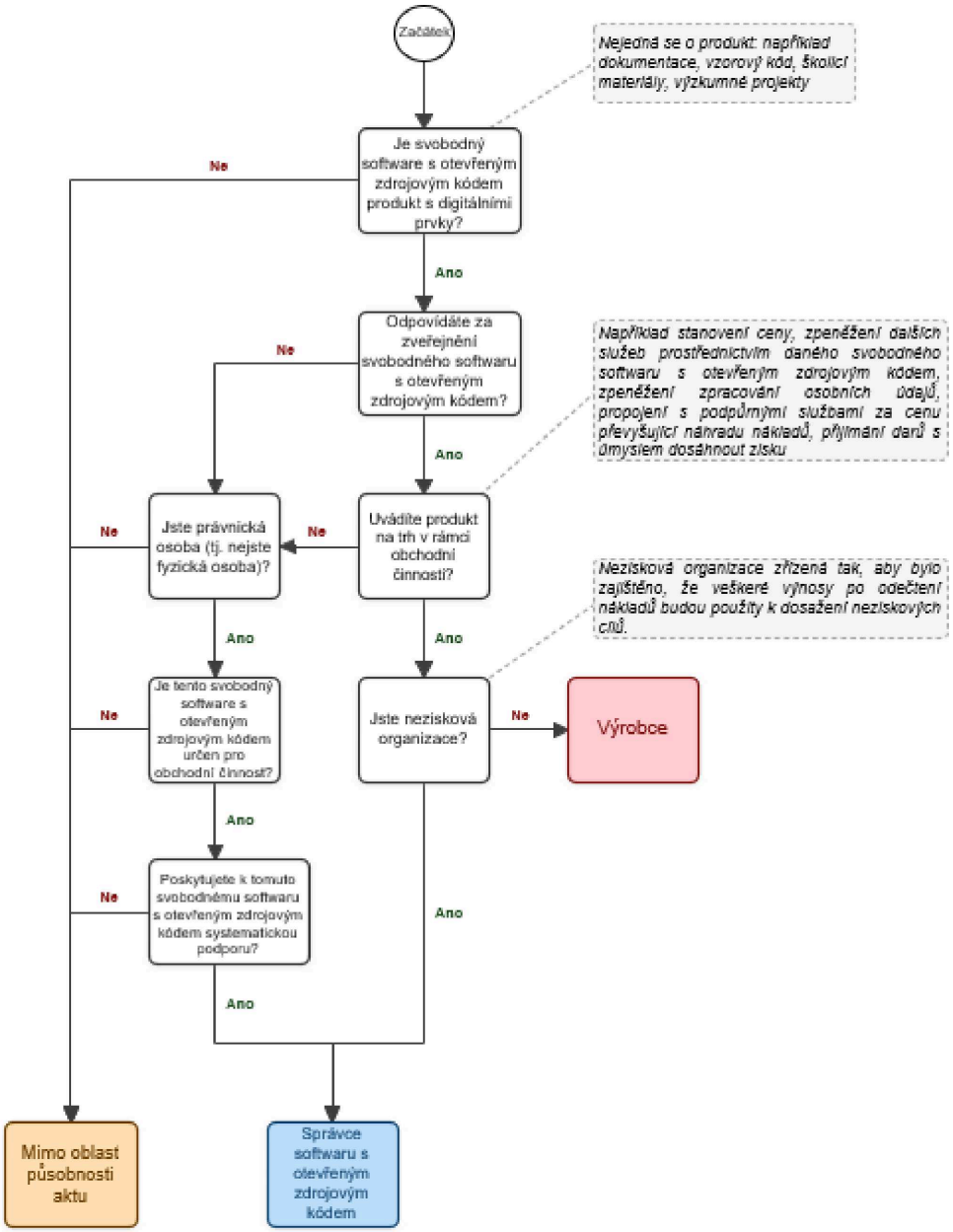
Příklad 34: Individuální vývojář zveřejní svobodnou softwarovou knihovnu s otevřeným zdrojovým kódem ve veřejném úložišti balíčků pro daný programovací jazyk a aktivně ji spravuje. Do dokumentace k balíčku vývojář doplní odkaz na výběr darů. Výrobce si tuto knihovnu bezplatně stáhne z úložiště a začlení ji do svého vlastního produktu s digitálními prvky.

Individuální vývojář ani úložiště balíčků nemají podle aktu žádné povinnosti. Výrobce, který tuto knihovnu začlení, musí v souladu s čl. 13 odst. 5 postupovat s náležitou péčí.

([15]) To neplatí, pokud je společnost A neziskovým subjektem zřízeným tak, aby bylo zajištěno, že veškeré výnosy po odečtení nákladů budou použity k dosažení neziskových cílů; v takovém případě by byla správcem daného svobodného softwaru s otevřeným zdrojovým kódem.

Obrázek 1:

Zjednodušené schéma znázorňující rozsah působnosti aktu v oblasti svobodného softwaru s otevřeným zdrojovým kódem



4. **PODSTATNÉ ZMĚNY A NÁHRADNÍ DÍLY**

90. V čl. 3 bodě 30 aktu je „podstatná změna“ definována jako změna produktu s digitálními prvky po jeho uvedení na trh, která i) ovlivňuje soulad produktu s digitálními prvky se základními požadavky stanovenými v části I přílohy I, nebo ii) která vede ke změně zamýšleného účelu, pro nějž bylo provedeno posouzení produktu s digitálními prvky.

91. Pojem „podstatná změna“ je relevantní pro určení povinností podle aktu v řadě případů, mimo jiné v těchto:

a) v souladu s článkem 21 je dovozce nebo distributor, který provede podstatnou změnu produktu s digitálními prvky již uvedeného na trh, považován za jeho výrobce;

b) v souladu s článkem 22 je každá fyzická nebo právnická osoba, která provede podstatnou změnu produktu s digitálními prvky a dodá jej na trh, považována za jeho výrobce;

c) v souladu s čl. 69 odst. 2 je každá fyzická nebo právnická osoba, která po 11. prosinci 2027 provede podstatnou změnu produktu s digitálními prvky uvedeného na trh před 11. prosincem 2027 a tento produkt uvede na trh, považována za jeho výrobce;

d) v případě výrobců produktů s digitálními prvky uvedených na trh po 11. prosinci 2027 s cílem určit, zda je u produktu s digitálními prvky nutné podstoupit nový postup posuzování shody v důsledku změn provedených po tomto datu, zejména s ohledem na povahu vývoje softwaru spočívající v opakovaných změnách.

92. Proto je důležité poskytnout pokyny, které pomohou hospodářským subjektům pochopit, kdy lze změny hardwaru či softwaru považovat za podstatné změny.

4.1 **Fyzické opravy**

93. Jak je uvedeno ve 42. bodě odůvodnění aktu, „[p]okud produkt s digitálními prvky podléhá ‚renovaci‘, ‚údržbě‘ a ‚opravě‘, jak jsou definovány v čl. 2 bodech 18, 19 a 20 nařízení Evropského parlamentu a Rady (EU) 2024/1781, nemusí to nutně vést k podstatné změně produktu, například pokud se nezmění zamýšlený účel a funkce a úroveň rizika zůstane nedotčena. Aktualizace produktu s digitálními prvky výrobcem by však mohla vést ke změnám v návrhu a vývoji tohoto produktu, a mohla by proto ovlivnit jeho zamýšlený účel a soulad s požadavky stanovenými v tomto nařízení“. To je v souladu s oddílem 2.1 Modré příručky, v němž se uvádí, že „[v]ýrobek, který byl podroben podstatným změnám nebo opravám poté, co byl uveden do provozu, je třeba považovat za nový výrobek, pokud: i) jeho původní výkonnost, účel nebo typ se mění, aniž by se s tím počítalo v počátečním posouzení rizik; ii) změnila se povaha nebezpečí nebo se zvýšila úroveň rizika s ohledem na příslušné harmonizační právní předpisy Unie a iii) výrobek je dodáván na trh (nebo uváděn do provozu, pokud se platné právní předpisy v rámci své oblasti působnosti vztahují i na uvedení do provozu). To je nutno posoudit v každém jednotlivém případě, zejména z hlediska cíle právních předpisů a typu výrobků spadajících do oblasti působnosti dotčeného právního předpisu“.

94. Renovace, údržba nebo opravy, které vedou k fyzickým změnám produktů s digitálními prvky, které již byly uvedeny na trh, nemusí nutně představovat podstatné změny. Mělo by se proto provést posouzení v jednotlivých případech, aby se zjistilo, zda taková fyzická úprava ovlivňuje soulad produktu s digitálními prvky se základními požadavky části I přílohy I nebo zda vede ke změně zamýšleného účelu produktu, na který se vztahuje posouzení kybernetických bezpečnostních rizik.

95. Nahrazení vadných nebo opotřebovaných dílů díly s lepšími vlastnostmi (např. z důvodu technického pokroku nebo proto, že se starý díl již nevyrábí) samo o sobě nepředstavuje podstatnou změnu opraveného produktu s digitálními prvky. K tomu dochází pouze v případě, že změna výkonnosti nebo způsobu fungování opraveného produktu s digitálními prvky i) ovlivňuje jeho soulad se základními požadavky nebo ii) vede ke změně zamýšleného účelu, která nebyla zahrnuta v posouzení rizik.

Příklad 35: Výrobce počítačového serveru provádí opravu, při které nahradí vadnou paměť RAM novou s vyšším výkonem. To nemá vliv na soulad serveru se základními požadavky. Server vykazuje lepší výkon, avšak jeho nový výkon se stále pohybuje v rámci zamýšleného využití serveru zohledněného v posouzení kybernetických bezpečnostních rizik. Počítačový server se nepovažuje za podstatně změněný.

4.2 **Náhradní díly**

96. Ustanovení čl. 2 odst. 6 aktu stanoví, že do oblasti působnosti aktu nespadají náhradní díly určené k nahrazení totožných komponent a vyrobené podle stejných specifikací jako tyto komponenty. Ve 29. bodě odůvodnění se dále uvádí, že výjimka se vztahuje jak na náhradní komponenty pro produkty s digitálními prvky, které byly dodány přede dnem použitelnosti aktu, tak na náhradní komponenty, které již prošly postupy posuzování shody podle nařízení.

97. Výjimku uvedenou v čl. 2 odst. 6 aktu je třeba chápat tak, že se vztahuje pouze na případy, kdy je náhradní díl dodáván výslovně za účelem opravy nebo prodloužení životnosti produktu s digitálními prvky, který již byl uveden na trh (před 11. prosincem 2027 nebo po tomto datu). Je-li produkt s digitálními prvky dodáván jako samostatný produkt, bez jakékoli souvislosti s údržbou nebo opravou již existujícího produktu s digitálními prvky, je uveden na trh ve smyslu aktu a neměl by být považován za náhradní díl spadající do oblasti působnosti čl. 2 odst. 6. Účel údržby nebo opravy by měl být zřejmý z kontextu dodávky, například na základě identifikace produktu s digitálními prvky nebo produktové řady v objednávce či obchodní nabídce, případně na základě dodávky prostřednictvím poprodejních nebo servisních kanálů. Důkazy, které to potvrzují, by měly být rovněž k dispozici orgánům dozoru nad trhem. Skutečnost, že produkt s digitálními prvky by z technického hlediska mohl být použit jako náhrada za určitou komponentu, sama o sobě nestačí k tomu, aby spadal do oblasti působnosti výjimky, nejsou-li doloženy výše uvedené skutečnosti.

98. V souladu s tím platí, že pokud je náhradní díl totožný s komponentou, která je již součástí produktu s digitálními prvky, jenž byl uveden na trh buď před datem použitelnosti aktu, nebo jenž byl uveden na trh v souladu s aktem, tento náhradní díl sám o sobě aktu nepodléhá.

99. Při posuzování, zda by náhradní díl měl být považován za totožný s danou komponentou, je třeba se zaměřit na jeho funkční úlohu v produktu s digitálními prvky a na charakteristiky, které mohou mít význam pro kybernetickou bezpečnost. Ačkoli je vždy nutné posouzení každého jednotlivého případu zvlášť, rozdíly, které nemají vliv na bezpečnostní charakteristiky ani na profil kybernetických bezpečnostních rizik dané komponenty, samy o sobě nebrání tomu, aby daný náhradní díl spadal do oblasti působnosti čl. 2 odst. 6 aktu.

100. Naopak rozdíly v charakteristikách souvisejících s kybernetickou bezpečností dané komponenty, jako jsou algoritmy, protokoly, kryptografické mechanismy, funkce řízení přístupu nebo jiné charakteristiky související s bezpečností, mohou znamenat, že nový díl nelze považovat za totožný s komponentou, kterou má nahradit.

101. Pokud náhradní díl není totožný s původní komponentou, představuje tento náhradní díl samostatný produkt s digitálními prvky, a proto se na něj akt vztahuje. V takových případech je třeba posoudit soulad se základními požadavky s ohledem na zamýšlený účel výměnné komponenty. Zvláště důležitá je funkce výměnné komponenty, která spočívá v zajištění kompatibility nebo interoperability se stávajícím produktem s digitálními prvky, a to i v případě, že se jedná o produkt s digitálními prvky, který byl uveden na trh před datem použitelnosti aktu. Pokud nelze některé základní požadavky z důvodu zamýšleného účelu nebo technických omezení rozumně splnit, musí to výrobce zohlednit v posouzení kybernetických bezpečnostních rizik a zavést vhodná alternativní nebo kompenzační opatření ke snížení rizik, aby nedošlo k ohrožení bezpečnosti produktu s digitálními prvky. Jak je rovněž rozebráno v oddíle *2.6 Složité systémy*, klíčovou roli hrají jak technická dokumentace, tak informace a pokyny pro uživatele, které transparentně popisují zjištěná omezení, související kybernetická bezpečnostní rizika a zavedená opatření ke zmírnění těchto rizik. Jak je vysvětleno v oddíle *4.1 Fyzické opravy*, nahrazení vadných nebo opotřebovaných dílů díly s lepšími vlastnostmi samo o sobě nepředstavuje podstatnou změnu opraveného produktu s digitálními prvky.

Příklad 36: Výrobce uvedl na trh EU propojené řídicí jednotky. V jednom případě byla řídicí jednotka uvedena na trh v roce 2026, tedy před datem použitelnosti aktu. V jiném případě byla tato řídicí jednotka uvedena na trh v roce 2028 v souladu s aktem. V roce 2028 dojde k poruše digitálního komunikačního modulu v obou typech řídicích jednotek. Výrobce dodá jako náhradní díl náhradní modul, který je totožný s originálem a je vyroben podle stejných specifikací.

V obou případech spadá náhradní modul do rozsahu výjimky uvedené v čl. 2 odst. 6. Náhradní díl sám o sobě nepodléhá aktu, i když se jedná o produkt s digitálními prvky, protože nahrazuje totožnou komponentu v produktu s digitálními prvky. Tato oprava nepředstavuje podstatnou změnu produktu s digitálními prvky.

Příklad 37: Výrobce uvedl v roce 2026 na trh EU propojený průmyslový řídicí systém, a to před datem použitelnosti aktu. V roce 2028 dojde k poruše komunikačního čipu v tomto řídicím systému. Jelikož výrobce tento čip již nevyrábí, dodá jako náhradní díl novější čip s rovnocennou funkčností, avšak s odlišným kryptografickým provedením a aktualizovaným mechanismem bezpečného spouštění, a to za účelem zachování kompatibility a dalšího provozu.

V tomto případě nelze náhradní čip považovat za totožný, jelikož rozdíly v kryptografickém provedení a mechanismu bezpečného spouštění ovlivňují vlastnosti čipu z hlediska kybernetické bezpečnosti. Nespadá tudíž pod výjimku uvedenou v čl. 2 odst. 6 a představuje produkt s digitálními prvky, na který se akt vztahuje. Soulad výměnného dílu je třeba posoudit s ohledem na jeho zamýšlený účel, včetně jeho úlohy při zajišťování interoperability s produktem s digitálními prvky, který byl uveden na trh před datem použitelnosti aktu.

Příklad 38: Výrobce uvede v roce 2028 na trh řídicí jednotku pro chytré budovy, která je v souladu s aktem. V roce 2029 se v této řídicí jednotce porouchá bezdrátový modul. Jelikož výrobce tento modul již nevyrábí, dodá jako náhradní díl nový modul, který plní stejnou funkci, přičemž používá stejné komunikační protokoly a bezpečnostní mechanismy, je však založen na jiné čipové sadě a obsahuje aktualizovaný firmware, který nemění charakteristiky, jež by mohly mít význam pro kybernetickou bezpečnost.

V tomto případě lze náhradní modul považovat za totožný. Tento modul tedy spadá pod výjimku uvedenou v čl. 2 odst. 6 a akt se na něj nevztahuje.

102. Výjimka pro náhradní díly platí bez ohledu na to, zda náhradní díl nahrazuje komponentu v rámci produktu s digitálními prvky, nebo zda nahrazuje celý produkt s digitálními prvky, který je sám součástí většího produktu, a to i v případě, že se tento větší produkt s digitálními prvky skládá z několika začleněných komponent, pokud je tento výměnný díl výslovně dodáván jako náhradní díl, jak je vysvětleno v předchozích odstavcích.

Příklad 39: V roce 2027 uvede výrobce na trh systém průmyslové automatizace, jehož jednou z komponent je programovatelný logický automat (PLC). V roce 2031 se porouchá centrální procesorová jednotka (CPU) PLC. Výrobce nabízí dvě možnosti opravy: i) dodání výměnné jednotky CPU, kterou lze považovat za totožnou s původně nainstalovanou CPU; nebo ii) dodání celého výměnného PLC, který lze považovat za totožný s původně nainstalovaným PLC. V každém případě je výměnný díl dodán prostřednictvím sítě poprodejního servisu výrobce jako náhradní díl a systém průmyslové automatizace, pro který je určen, je jasně identifikován. V obou případech spadá tento výměnný díl do rozsahu výjimky podle čl. 2 odst. 6, a to bez ohledu na to, zda se výměna týká komponenty v rámci jednotky PLC, nebo PLC jako celku.

4.3 **Aktualizace softwaru jako podstatné změny**

103. Vývoj softwaru je založen na opakovaných změnách, přičemž softwarové produkty s digitálními prvky, které jsou již uvedeny na trh, jsou často a průběžně aktualizovány. V této souvislosti je užitečné poskytnout podrobnější pokyny, které pomohou určit, kdy lze software považovat za podstatně změněný. Účelem těchto pokynů je zejména pomoci výrobcům softwarových produktů s digitálními prvky, kteří provádějí změny ve svých vlastních produktech, určit, zda tyto změny představují podstatnou změnu.

104. Ve 39. bodě odůvodnění se uvádí, že produkt s digitálními prvky je podstatně změněn, pokud změna mění úroveň kybernetického bezpečnostního rizika a pokud výrobce toto změněné či dodatečné riziko nezohlednil ve svém posouzení rizik, a v důsledku toho ani při plnění základních požadavků. Výrobce by proto měl v každém jednotlivém případě posoudit, zda aktualizace softwaru zavádí nová nebo zvýšená kybernetická bezpečnostní rizika a zda byla tato rizika již zohledněna v jeho posouzení rizik.

105. Pokud výrobce zavede do produktu s digitálními prvky nové funkce, které vedou ke změně zamýšleného účelu produktu jako celku, je pravděpodobné, že tyto změny ve svém posouzení rizik nezohlednil. Za těchto okolností by se tato změna obecně považovala za podstatnou změnu.

Příklad 40: Výrobce uvádí na trh řídicí panel, který shromažďuje data ze strojů a zobrazuje trendy a výstrahy, aniž by měl možnost tyto stroje ovládat. Výrobce následně vyvine novou verzi tohoto řídicího panelu a zavede do něj funkce, které mu umožňují ovládat stroje, mimo jiné úpravou provozních parametrů a restartováním strojů po poruchových stavech. V důsledku těchto změn se zamýšlený účel řídicího panelu posunul nad rámec toho, co bylo předpokládáno v posouzení rizik, a z nástroje pro přehled o situaci se stal produkt s digitálními prvky, jehož účelem je provádět provozní řízení jiných zařízení. Řídicí panel byl proto podstatně změněn.

Příklad 41: Výrobce uvede na trh spotřebitelskou softwarovou aplikaci, jejímž účelem je organizovat a zobrazovat osobní údaje, jako jsou e-maily, zprávy nebo dokumenty, a podporovat základní funkce vyhledávání a filtrování. Výrobce následně vydá aktualizaci, která aplikaci umožní automaticky analyzovat uživatelský obsah za účelem vytváření profilů chování a přijímání automatizovaných rozhodnutí ovlivňujících upřednostňování, potlačování nebo doporučování obsahu bez zásahu uživatele. V důsledku této změny se zamýšlený účel softwaru přesune z nástroje pro správu informací ovládaného uživatelem na automatizovaný systém pro rozhodování, což nebylo v posouzení rizik zohledněno. Aplikace byla proto podstatně změněna.

106. Zároveň je však možné, že výrobce postupně zavádí nové funkce, které již byly zahrnuty do jeho posouzení rizik nebo které samy o sobě nemění profil kybernetických bezpečnostních rizik produktu s digitálními prvky. To může platit například v případě, kdy výrobce předvídal vývoj těchto funkcí, již popsal a posoudil související rizika a zavedl vhodná opatření ke snížení rizik, aby zajistil trvalé plnění základních požadavků. To může platit i v případě, kdy nové funkce nezavádějí změny, které by s sebou přinesly nová nebo zvýšená rizika. Aktualizace této povahy by proto neměly být považovány za podstatné změny, jelikož nezvyšují kybernetická bezpečnostní rizika, a v důsledku toho nemění plnění základních požadavků.

Příklad 42: Aplikace pro zasílání zpráv je zpočátku vydána s funkcí omezenou na zasílání zpráv mezi dvěma uživateli. Posouzení rizik provedené výrobcem zahrnuje i pozdější zavedení skupinových zpráv, včetně například zvýšené složitosti směrování zpráv. V následující aktualizaci výrobce přidá funkci skupinového chatu spolu s nástroji pro správu a moderování, které byly již v původním návrhu předpokládány a posouzeny. Tato aktualizace zavádí funkce, které spadají do rozsahu původního zamýšleného účelu a posouzení rizik. Aplikace pro zasílání zpráv tedy nebyla podstatně změněna.

Příklad 43: Systém monitorování výroby je uveden na trh s řídicími panely aktivovanými pouze pro čtení, přičemž funkce automatického řízení jsou sice součástí architektury systému, zůstávají však deaktivovány. Posouzení rizik provedené výrobcem výslovně zahrnuje budoucí aktivaci automatizovaných regulačních smyček, včetně kybernetických bezpečnostních rizik spojených s regulací v uzavřené smyčce, jakož i ochranná opatření, jako jsou mechanismy manuálního zásahu operátora a bezpečné stavy při poruše. V pozdější aktualizaci výrobce zpřístupní funkce automatického řízení a aktivuje bezpečnostní opatření v souladu s původním posouzením. Systém monitorování výroby tedy nebyl podstatně změněn.

107. Naopak značná kybernetická bezpečnostní rizika, která mají dopad na dodržování základních požadavků, mohou představovat i omezené či zdánlivě nevýznamné nové funkce. Posouzení podstatné změny by se proto nemělo zakládat na rozsahu či složitosti dané změny, ale na jejím potenciálním nepříznivém dopadu na profil kybernetických bezpečnostních rizik produktu s digitálními prvky, a v důsledku toho na plnění základních požadavků.

Příklad 44: Výrobce vydá aktualizaci softwarové aplikace, která přidává funkci „zapamatovat si mě“ neboli trvalého přihlášení, jež s cílem zvýšit pohodlí uživatelů ukládá lokálně autentizační tokeny. Ačkoli je rozsah této funkce omezený, přináší s sebou nová rizika související s krádeží tokenů, neoprávněným přístupem a únosem relace, která nebyla v posouzení rizik zohledněna. Tato aktualizace má proto vliv na soulad se základními požadavky. Softwarová aplikace byla podstatně změněna.

Příklad 45: Výrobce doplní stávající softwarový produkt s digitálními prvky o novou funkci protokolování a diagnostiky, která umožňuje export podrobných systémových protokolů pro účely řešení problémů. Ačkoli se tato funkce jeví jako nepodstatná, vede ke shromažďování a ukládání citlivých provozních dat v nešifrovaném formátu, čímž vzniká riziko úniku dat, které dosud nebylo posouzeno ani zmírněno. Tato změna proto může mít významný dopad na profil kybernetických bezpečnostních rizik produktu s digitálními prvky. Softwarový produkt s digitálními prvky byl podstatně změněn.

108. V souladu s 39. bodem odůvodnění aktu se bezpečnostní aktualizace obecně nepovažují za podstatné změny, jelikož jejich primárním účelem je snížit úroveň kybernetického bezpečnostního rizika spojeného s produktem s digitálními prvky. Bezpečnostní aktualizace, která nemění zamýšlený účel daného produktu a nezpůsobuje nová kybernetická bezpečnostní rizika, by proto neměla být považována za podstatnou změnu, a to ani v případě, že tato aktualizace může přinést významné technické změny. To se týká i případů, kdy jsou určité funkce změněny nebo omezeny výhradně za účelem zmírnění zjištěných zranitelností a zajištění trvalého souladu se základními požadavky.

Příklad 46: Výrobce vydá bezpečnostní aktualizaci, která řeší zranitelnost v kódové základně produktu s digitálními prvky, a to buď opravou chyby při ověřování vstupů, která by mohla vést k přetečení vyrovnávací paměti, nebo opravou logické chyby umožňující obejít autentizaci tím, že by byl nesprávně ověřen token relace. Tato aktualizace mění vnitřní implementaci softwaru, aniž by to mělo vliv na zamýšlený účel daného produktu nebo vedlo ke vzniku nové expozice. Cílem této aktualizace je výhradně snížit kybernetické bezpečnostní riziko. Tuto bezpečnostní aktualizaci nelze považovat za podstatnou změnu.

Příklad 47: Výrobce zavádí bezpečnostní aktualizaci, která posiluje stávající bezpečnostní konfigurace, například zpřísněním pravidel firewallu, deaktivací nepoužívaných síťových portů, změnou výchozích zásad pro hesla správců nebo zavedením povinného vícefaktorového ověřování tam, kde byla tato funkce již k dispozici nebo se s ní počítalo. Ačkoli tato aktualizace může ovlivnit způsob, jakým uživatelé produkt s digitálními prvky konfigurují nebo jakým k němu mají přístup, nemění jeho zamýšlený účel a slouží výhradně ke zvýšení jeho bezpečnostní úrovně. Tuto bezpečnostní aktualizaci nelze považovat za podstatnou změnu.

Příklad 48: Výrobce uvádí na trh softwarový produkt s digitálními prvky, který zabezpečuje komunikaci pomocí konfigurovatelného šifrovacího rámce podporujícího více kryptografických algoritmů a velikostí klíčů, jak je popsáno v technické dokumentaci produktu a v posouzení rizik. Posouzení rizik zahrnuje všechny kryptografické možnosti, které produkt s digitálními prvky nabízí, a počítá s tím, že některé algoritmy budou v budoucnu vyřazeny z používání. Součástí posouzení rizik jsou také opatření k jejich zmírnění, jako je kryptografická agilita, interní správa klíčů a testování kompatibility. V reakci na nové kryptografické pokyny zavádí výrobce bezpečnostní aktualizaci, která deaktivuje zastaralý algoritmus a aktivuje silnější, již podporovanou alternativu, aniž by docházelo k zavedení nových externích závislostí nebo ke změnám v toku dat. Jelikož tato aktualizace zavádí bezpečnostní opatření, které bylo předvídáno a posouzeno v rámci původního návrhu, a nezpůsobuje žádná nová kybernetická bezpečnostní rizika, neměla by být považována za podstatnou změnu.

109. Naproti tomu, bezpečnostní aktualizace může být považována za podstatnou změnu, pokud navzdory svému bezpečnostnímu cíli vede k tomu, že zamýšlený účel produktu s digitálními prvky je změněn nad rámec toho, co bylo původně předpokládáno nebo pokud s sebou přináší nová či zvýšená kybernetická bezpečnostní rizika. Tak tomu může být například v situaci, kdy aktualizace významně změní hranice daného produktu nebo strukturu jeho závislostí způsobem, který nebyl v posouzení rizik předvídán, např. významnou změnou toků dat nebo přidáním nových externě přístupných rozhraní.

Příklad 49: Výrobce uvede na trh softwarový produkt s digitálními prvky, jehož účelem je zajistit lokální šifrování souborů pro data uložená na zařízení uživatele, což uživatelům umožňuje soubory šifrovat a dešifrovat podle potřeby. V návaznosti na odhalení zranitelnosti v procesu šifrování výrobce zavede bezpečnostní aktualizaci, která zruší funkci lokálního šifrování a místo toho vyžaduje, aby všechny soubory byly nahrány, uloženy a zpracovány prostřednictvím vzdálené šifrovací služby provozované výrobcem. V důsledku této změny produkt s digitálními prvky již neprovádí lokální šifrování, jak bylo původně zamýšleno, ale funguje jako služba vzdáleného šifrování a zpracování dat. Ačkoli je tato aktualizace zavedena z bezpečnostních důvodů, zásadním způsobem mění zamýšlený účel daného produktu způsobem, který nebyl v posouzení rizik předvídán, a proto se jedná o podstatnou změnu.

Příklad 50: Výrobce uvede na trh softwarový produkt s digitálními prvky, který k zabezpečení komunikace mezi komponentami produktu s digitálními prvky využívá zavedený šifrovací protokol a interně spravovaný životní cyklus klíčů. V reakci na nově zjištěné kryptografické slabiny zavede výrobce bezpečnostní aktualizaci, která nahrazuje stávající šifrovací mechanismus jiným protokolem, jenž vyžaduje využití externí služby pro správu klíčů provozované třetí stranou. V důsledku této změny dochází k významné změně závislostí a toků dat produktu s digitálními prvky, což s sebou nese zavedení nových externích rozhraní a závislosti na službách třetí strany, které nebyly v posouzení rizik zohledněny. Ačkoli je tato aktualizace zaměřena na bezpečnost, přináší s sebou nová kybernetická bezpečnostní rizika, a proto ji lze považovat za podstatnou změnu.

110. Jak je uvedeno v bodě 104 výše, otázku, zda aktualizace softwaru představuje podstatnou změnu, je třeba posuzovat v každém případu zvlášť. Při provádění tohoto posouzení mohou výrobci mimo jiné zvážit, zda aktualizace softwaru:

a) přináší nové vektory hrozeb, jako jsou další rozhraní, komunikační kanály, prováděcí prostředí nebo externí závislosti, jejichž prostřednictvím by se hrozby mohly projevit;

b) umožňuje nové scénáře útoků, včetně například nových způsobů, jak by mohlo reálně dojít k neoprávněnému přístupu k produktu s digitálními prvky či k datům, která produkt zpracovává, k manipulaci s nimi, k zásahu do nich nebo k jejich zneužití;

c) mění pravděpodobnost dříve identifikovaných scénářů útoků, například tím, že snižuje míru úsilí nebo odborných znalostí potřebných k jejich zneužití, zvyšuje expozici vůči nedůvěryhodným aktérům nebo oslabuje stávající ochranná opatření;

d) mění potenciální dopad dříve identifikovaných scénářů útoků, včetně například rozsahu dotčených dat či funkcí, závažnosti provozních, bezpečnostních či ekonomických důsledků nebo schopnosti incident odhalit, omezit jeho šíření či se z něj zotavit.

111. V některých případech aktualizace softwaru nepřináší nové vektory hrozeb, neumožňuje nové scénáře útoků a významně nemění pravděpodobnost ani dopad dříve identifikovaných scénářů útoků. To může naznačovat, že aktualizace nepřináší žádná nová ani zvýšená kybernetická bezpečnostní rizika, pokud předpoklady a opatření ke zmírnění rizik, z nichž vycházelo posouzení rizik, zůstávají platné a účinné. Je proto pravděpodobné, že tuto aktualizaci nelze považovat za podstatnou změnu.

112. Na druhou stranu aktualizace softwaru může přinést nové vektory hrozeb, umožnit nové scénáře útoků nebo významně změnit pravděpodobnost či dopad stávajících scénářů útoků. V takových případech by měl výrobce znovu posoudit kybernetická bezpečnostní rizika produktu s digitálními prvky a zjistit, zda jsou i nadále dodržovány základní požadavky, a to včetně toho, zda aktualizace přináší nová nebo zvýšená rizika, která nebyla v posouzení rizik předvídána.

113. To, zda lze aktualizaci softwaru považovat za podstatnou změnu, je relevantní při určování, zda se uplatňují určité povinnosti podle aktu, jak je uvedeno v bodě 91. Bez ohledu na tuto kvalifikaci však výrobci nadále nesou odpovědnost za zajištění bezpečnosti softwarových aktualizací a svého produktu s digitálními prvky po dobu trvání podpory, a to v souladu s požadavky na řešení zranitelností stanovenými v části II přílohy I aktu. Navíc bez ohledu na to, zda se aktualizace softwaru považují za podstatné změny či nikoli, jsou výrobci v souladu s čl. 13 odst. 7 a čl. 31 odst. 2 povinni zajistit, aby posouzení rizik a technická dokumentace byly přesné a úplné a aby byly průběžně aktualizovány.

4.4 **Důsledky podstatné změny**

114. Důsledky podstatné změny provedené jiným aktérem než původním výrobcem produktu s digitálními prvky, který již byl uveden na trh, jsou upraveny v článcích 21 a 22 aktu. Článek 21 se týká dovozců a distributorů, zatímco článek 22 se týká jakékoli fyzické nebo právnické osoby jiné než výrobce, dovozce nebo distributora.

115. Pokud podstatnou změnu provádí původní výrobce produktu s digitálními prvky, vyplývají důsledky z obecně zavedeného pojmu „podstatná změna“, na který odkazuje 41. bod odůvodnění aktu a který je podrobněji rozveden v oddíle 2.1 Modré příručky. V tomto oddíle je uvedeno, že produkt, který po uvedení na trh prošel významnými změnami nebo opravou, se považuje za nový produkt, pokud došlo ke změně jeho původní výkonnosti, účelu nebo typu, změnila se povaha nebezpečí nebo se zvýšila úroveň rizika a pokud je tento produkt s digitálními prvky dodáván na trh.

116. Z toho obecně vyplývá, že pokud je změna produktu s digitálními prvky považována za podstatnou a změněný produkt s digitálními prvky je dodáván na trh, je třeba jej pro účely aktu považovat za nový produkt s digitálními prvky. V důsledku toho představuje dodávání podstatně změněného produktu na trh nové uvedení na trh. To platí bez ohledu na to, zda podstatnou změnu provádí původní výrobce, nebo jiná osoba. Aby bylo zajištěno jednotné a přiměřené uplatňování aktu u různých kategorií aktérů, kteří mohou provést podstatnou změnu, zabývají se následující pododdíly výslednými povinnostmi osoby provádějící podstatnou změnu v případě, že je podstatně změněný produkt s digitálními prvky uveden na trh. Důsledky pro dobu podpory produktu s digitálními prvky jsou řešeny v oddíle *5 Doba podpory*.

4.4.1 *Podstatné změny provedené jinou osobou než původním výrobcem*

117. V souladu s články 21 a 22 platí, že pokud podstatnou změnu produktu s digitálními prvky, který již byl uveden na trh, provede fyzická nebo právnická osoba jiná než výrobce tohoto produktu s digitálními prvky, osoba, která tuto podstatnou změnu provede a dodá změněný produkt s digitálními prvky na trh, se považuje za výrobce změněného produktu s digitálními prvky, a to bez ohledu na to, zda se tato osoba podílela na původním návrhu nebo uvedení tohoto produktu na trh.

118. Článek 22 dále upřesňuje, že na osobu provádějící změnu se vztahují povinnosti stanovené v článcích 13 a 14 pouze ohledně té části produktu s digitálními prvky, která je touto podstatnou změnou ovlivněna, pokud tato změna nemá dopad na kybernetickou bezpečnost produktu s digitálními prvky jako celku.

119. Pokud podstatná změna ovlivňuje dodržování základních požadavků, avšak nemá negativní dopad na kybernetickou bezpečnost produktu s digitálními prvky jako celku, vztahuje se na osobu provádějící tuto změnu článek 13 (včetně povinnosti zajistit dodržování základních požadavků a provést postup posuzování shody) a článek 14 (povinnosti podávat zprávy) pouze ve vztahu k té části produktu s digitálními prvky, která byla podstatně změněna ([16]). Kromě toho se povinnosti původního výrobce podle aktu i nadále vztahují na původní produkt s digitálními prvky uvedený na trh, čímž je zajištěna kontinuita při řešení zranitelností a zajišťování souladu u nezměněných částí.

120. Případ podstatné změny by neměl být zaměňován s případy začlenění, při nichž osoba sestavuje komponenty (v případě potřeby včetně jejich změny) do nového produktu s digitálními prvky, který sama uvádí na trh. V takových případech ten, kdo produkt kompletuje, nemění produkt s digitálními prvky, který již uvedl na trh jiný výrobce; nýbrž uvádí na trh nový vlastní produkt s digitálními prvky. Z hlediska aktu je ten, kdo produkt kompletuje, výrobcem tohoto nového produktu s digitálními prvky a je povinen dodržovat nařízení v plném rozsahu, pokud jde o produkt s digitálními prvky jako celek. Pokud výrobce do svých produktů začleňuje komponenty, na které se vztahuje akt, může se při zajišťování vlastního souladu s aktem opírat o opatření k zajištění souladu přijatá výrobci těchto komponent.

Příklad 51: Společnost nakupuje od externích dodavatelů hotové moduly mikrořadičů a komponenty pro připojení, vyvíjí vlastní firmware a sadu senzorů a sestavuje z nich propojený produkt pro zemědělské monitorování s digitálními prvky, který uvádí na trh pod svým vlastním jménem. Ačkoli společnost upravila podkladové moduly mikrořadiče a zkombinovala je s dalšími komponentami, nejedná se o podstatnou změnu produktu s digitálními prvky, který je již uveden na trh; nýbrž společnost na trh uvádí nový produkt s digitálními prvky. Společnost je pro účely aktu výrobcem zemědělského monitorovacího systému a je povinna dodržovat nařízení, pokud jde o tento zemědělský monitorovací systém jako celek.

([16]) V souladu s oddílem 2.1 Modré příručky „[n]ení nutné opakovat zkoušky a vytvářet novou dokumentaci, pokud jde o aspekty, na něž úprava nemá vliv. Je na fyzické nebo právnické osobě, která provádí změny výrobku nebo nechala takovéto změny provést, aby prokázala, že není nutné aktualizovat všechny prvky technické dokumentace. Fyzická nebo právnická osoba, která provádí nebo nechá provést změny výrobku, odpovídá za shodu upraveného výrobku a vypracuje prohlášení o shodě, a to i v případě, že použije stávající zkoušky a technickou dokumentaci“.

121. Pokud podstatná změna provedená jinou osobou než původním výrobcem negativně ovlivňuje kybernetickou bezpečnost produktu s digitálními prvky jako celku, například proto, že se tato změna již nezaměřuje ani neomezuje na konkrétní komponentu nebo dílčí systém, měl by být změněný produkt s digitálními prvky dodávaný na trh považován za nový produkt s digitálními prvky, na který se akt vztahuje v plném rozsahu. V takových případech se změnil celkový profil kybernetických bezpečnostních rizik daného produktu a tuto změnu nelze posoudit, aniž by byl produkt s digitálními prvky brán v úvahu jako celek. Na osobu provádějící změnu se vztahují povinnosti výrobce stanovené v článcích 13 a 14 ohledně změněného produktu s digitálními prvky jako celku.

4.4.2 *Podstatné změny provedené původním výrobcem*

122. Pokud podstatnou změnu provede původní výrobce, a to i v rámci vývoje softwarových produktů s digitálními prvky založeného na opakovaných změnách, zůstává tento výrobce výrobcem pro účely aktu. Podstatně změněný produkt s digitálními prvky je však třeba považovat za produkt nově uvedený na trh.

123. V souladu s oddílem 2.1 Modré příručky může původní výrobce, který uvádí na trh podstatně změněný produkt s digitálními prvky, znovu použít stávající dokumentaci a zkoušky, pokud jde o aspekty tohoto produktu, na něž podstatná změna nemá vliv. Zejména v případech, kdy výrobce uvádí na trh podstatně změněné verze téhož produktu s digitálními prvky, by se postup posuzování shody měl zaměřit na podstatně změněné části produktu s digitálními prvky. Podobně v případě, že je prováděno posouzení shody třetí stranou, měl by subjekt posuzování shody zaměřit své posouzení na podstatně změněné části. U nezměněných částí produktu s digitálními prvky lze znovu použít stávající dokumentaci a výsledky zkoušek.

124. Úvahy o proporcionalitě uvedené v předchozím pododdíle platí stejně i pro podstatné změny provedené původním výrobcem produktu s digitálními prvky, který byl uveden na trh před 11. prosincem 2027. Taková podstatná změna provedená původním výrobcem sama o sobě neznamená, že by výrobce byl povinen uvést celý produkt s digitálními prvky, který byl uveden na trh před tímto datem, do plného souladu s aktem, ledaže by tato změna měla negativní dopad na kybernetickou bezpečnost produktu s digitálními prvky jako celku. Pokud změna nemá vliv na kybernetickou bezpečnost produktu s digitálními prvky jako celku, měly by se povinnosti původního výrobce v souvislosti s touto změnou omezit pouze na podstatně změněné části.

5. **DOBA PODPORY**

125. Ustanovení čl. 13 odst. 8 aktu ukládá výrobcům povinnost stanovit dobu podpory, během níž budou zranitelnosti produktu s digitálními prvky, včetně jeho komponent, řešeny účinně a v souladu se základními požadavky stanovenými v části II přílohy I. Doba podpory odráží období, během něhož se předpokládá používání produktu s digitálními prvky (očekávaná doba použití), a měla by být určena s ohledem na kritéria uvedená v čl. 13 odst. 8, zejména přiměřená očekávání uživatelů, povahu produktu s digitálními prvky, včetně jeho zamýšleného účelu, jakož i příslušné právní předpisy Unie, které stanovují životnost produktů s digitálními prvky ([17]). Celkově je třeba tato kritéria zohlednit tak, aby byla při určování doby podpory zajištěna proporcionalita.

([17]) Další kritéria, která lze v souladu s čl. 13 odst. 8 rovněž zohlednit, zahrnují dobu podpory produktů s digitálními prvky, které nabízejí podobnou funkci a byly uvedeny na trh jinými výrobci, dostupnost provozního prostředí, dobu podpory začleněných komponent, které zajišťují klíčové funkce a pocházejí od třetích stran, stejně jako příslušné pokyny, které poskytla skupina pro správní spolupráci podle aktu (ADCO) a Komise.

126. Ustanovení čl. 13 odst. 8 dále stanoví, že doba podpory musí trvat nejméně pět let, ledaže by se předpokládalo, že produkt s digitálními prvky bude používán po dobu kratší než pět let; v takovém případě odpovídá doba podpory očekávané době použití. Minimální doba podpory tedy slouží pouze jako záruka, která zajišťuje, že budou zranitelnosti řešeny po dostatečně dlouhou dobu, a zároveň umožňuje výrobcům zohlednit produkty s digitálními prvky, u nichž je očekávaná doba použití skutečně kratší. 60. bod odůvodnění poskytuje v tomto ohledu další pokyny a upřesňuje, že pokud je důvodně očekávaná doba použití produktů s digitálními prvky delší než pět let, měly by mít odpovídajícím způsobem delší dobu podpory. Pětileté období podpory proto nelze považovat za standardní pro všechny produkty s digitálními prvky. Výrobce by měl místo toho stanovit přiměřenou dobu podpory s ohledem na kritéria uvedená v čl. 13 odst. 8.

127. Ustanovení čl. 13 odst. 19 ukládá výrobcům povinnost v době nákupu jasně a srozumitelně uvést datum ukončení doby podpory (alespoň měsíc a rok). Dále se od výrobců vyžaduje, aby po uplynutí doby podpory zobrazili uživatelům oznámení, je-li to s ohledem na povahu produktu s digitálními prvky technicky proveditelné. Cílem této povinnosti je zajistit uživatelům transparentnost ohledně doby, po kterou lze očekávat bezpečnostní podporu.

128. V případě softwarových produktů s digitálními prvky, které jsou často vyvíjeny a vydávány na základě opakujících se změn a u nichž mohou být v průběhu času často uváděny na trh podstatně změněné verze, je třeba dobu podpory chápat s ohledem na tento model vývoje. Každá podstatně změněná verze softwarového produktu s digitálními prvky uvedená na trh musí mít deklarovanou dobu podpory, která je v souladu s čl. 13 odst. 8. To zahrnuje minimální dobu podpory v délce nejméně pěti let, ledaže by byla očekávaná doba použití dané verze prokazatelně kratší, jak je rovněž upřesněno v 60. bodě odůvodnění. Oddíl *5.1 Podstatné změny a doba podpory* dále vyjasňuje, že pokud podstatná změna nevede ke změnám faktorů, které původně určovaly očekávanou dobu použití produktu s digitálními prvky, zůstává původní doba podpory nedotčena (tj. včetně případů, kdy zbývající doba podpory je kratší než pět let).

129. Ustanovení čl. 13 odst. 10 poskytuje flexibilitu v případě softwarových produktů s digitálními prvky tím, že výrobcům za určitých podmínek umožňuje zajistit soulad s požadavkem na řešení zranitelností stanoveným v bodě 2 části II přílohy I (řešení a náprava zranitelností) pouze pro verzi softwarového produktu s digitálními prvky, která byla na trh uvedena jako poslední. To je přípustné, pokud mají uživatelé dříve uvedených verzí bezplatný přístup k verzi, která byla uvedena na trh jako poslední, a nevznikají jim žádné dodatečné náklady na úpravu hardwarového a softwarového prostředí, v němž používají původní verzi tohoto produktu.

130. Pro účely čl. 13 odst. 10 by měl být pojem „dodatečné náklady“ vykládán praktickým a přiměřeným způsobem s přihlédnutím k běžným a očekávaným postupům v oblasti údržby a provozu softwaru. Nezahrnuje to přiměřené provozní úsilí, které je neodmyslitelně spojeno s instalací softwarových aktualizací nebo udržováním bezpečného provozního prostředí, jako je například čas zaměstnanců, rutinní testování, úpravy konfigurace nebo aktualizace podkladových softwarových závislostí, které jsou nezbytné k řešení problémů s komponentami na konci životnosti nebo známých bezpečnostních zranitelností. Naopak pojem „dodatečné náklady“ označuje zátěž, která přesahuje rámec toho, co lze v souvislosti s aktualizacemi softwaru běžně očekávat, jako jsou například povinné nákupy nového hardwaru, výměna infrastruktury nebo zásadní změny v provozním prostředí.

131. V případě neustále se vyvíjejících softwarových produktů s digitálními prvky mohou výrobci uvádět na trh v relativně krátkých intervalech po sobě jdoucí podstatně změněné verze a očekávat, že uživatelé budou pravidelně provádět aktualizace. V takových případech musí deklarovaná doba podpory pro každou podstatně změněnou verzi v době jejího uvedení na trh splňovat požadavky čl. 13 odst. 8. Jinými slovy, výrobce musí pro tuto podstatně změněnou verzi deklarovat novou dobu podpory. Výrobci se však mohou odvolat na čl. 13 odst. 10 a přestat řešit a odstraňovat zranitelnosti u starších verzí, jakmile budou mít uživatelé možnost bezplatně a bez dodatečných

nákladů, jak je uvedeno výše, přejít na novější verzi, a to i v případě, že to povede ke zkrácení faktické doby podpory pro tyto starší verze ([18]). Výrobce je i nadále povinen dodržovat další požadavky na řešení zranitelností uvedené v části II přílohy I, jakož i povinnosti podávat zprávy podle článku 14. Jak je rovněž vysvětleno ve 40. bodě odůvodnění, tyto požadavky zahrnují mimo jiné u všech následných podstatně změněných verzí softwarového produktu s digitálními prvky uvedených na trh: i) uplatňování politiky koordinovaného zveřejňování zranitelností a ii) opatření na usnadnění sdělování informací o potenciálních zranitelnostech ([19]).

Příklad 52: Výrobce uvede model chytrého telefonu na trh EU a deklaruje dobu podpory v délce X let od data uvedení na trh, během níž bude poskytovat bezpečnostní aktualizace řešící zranitelnosti. Během tohoto období výrobce vydává pravidelné aktualizace softwaru a podstatně změněné verze operačního systému, které si uživatelé mohou nainstalovat zdarma, aniž by k tomu potřebovali nový hardware.

Výrobce může v souladu s čl. 13 odst. 10 řešit zranitelnosti a zjednávat jejich nápravu v nejnovější verzi operačního systému, která je pro daný model chytrého telefonu dodávána, za předpokladu, že starší verze lze bezplatně a bez dodatečných nákladů aktualizovat. Po celou dobu trvání podpory se na výrobce i nadále vztahují další požadavky na řešení zranitelností, jako jsou opatření týkající se koordinovaného zveřejňování zranitelností a sdílení informací.

Příklad 53: Výrobce uvádí na trh podnikový softwarový produkt s digitálními prvky a jednou za několik měsíců vydává podstatně změněné verze, které odrážejí bezpečnostní vylepšení, nové funkce a kompatibilitu s aktualizovanými operačními systémy a platformami. Každá verze je uvedena na trh s deklarovanou dobou podpory v souladu s čl. 13 odst. 8. Výrobce očekává, že uživatelé budou v rámci běžného provozu pravidelně provádět aktualizace, a poskytuje bezplatný přístup k nejnovější verzi. Provádění aktualizací může vyžadovat přiměřené provozní úsilí, jako je testování nebo úpravy konfigurace, nevyžaduje však žádné dodatečné náklady, jako je nákup nového hardwaru nebo zásadní změny infrastruktury. V této souvislosti se může výrobce opřít o čl. 13 odst. 10 a přestat řešit a napravovat zranitelnosti u starších verzí, jakmile budou mít uživatelé možnost provést aktualizaci na nejnovější verzi, přičemž bude i nadále plnit ostatní požadavky na řešení zranitelností u všech následujících podstatně změněných verzí.

5.1 **Podstatné změny a doba podpory**

132. Jak je uvedeno v oddíle *4.4 Důsledky podstatné změny,* pokud změna produktu s digitálními prvky je považována za podstatnou změnu a změněný produkt s digitálními prvky je dodáván na trh, je třeba jej pro účely aktu považovat za nový produkt a dodávání podstatně změněného produktu s digitálními prvky na trh představuje nové uvedení na trh. Je proto užitečné objasnit, jaký vliv má toto nové uvedení na trh na dobu podpory podstatně změněného produktu s digitálními prvky.

133. Doba podpory podstatně změněného produktu s digitálními prvky by měla být určena s ohledem na očekávanou dobu použití tohoto produktu, a to na základě kritérií stanovených v čl. 13 odst. 8 aktu. Podstatná změna by proto měla vyžadovat nové posouzení podle těchto kritérií, avšak nevede automaticky k obnovení doby podpory ani k jejímu prodloužení. Rozhodující otázkou je, zda podstatná změna ovlivňuje faktory, které původně určily očekávanou dobu použití daného produktu, a tím i původní dobu podpory.

([18]) Mělo by být připomenuto, že čl. 13 odst. 19 požaduje, aby výrobci, je-li to s ohledem na povahu produktu s digitálními prvky technicky proveditelné, zobrazovali uživatelům oznámení, kterým je informují o tom, že jejich produktu s digitálními prvky končí doba podpory. Proto se v případech, kdy je ukončeno řešení a odstraňování zranitelností u starších verzí, očekává, že uživatelé, kteří neprovedli aktualizaci na nejnovější verzi, budou informováni, pokud to bude technicky proveditelné.

([19]) Je třeba poznamenat, že v případech, kdy mohou uživatelé bez dodatečných nákladů přejít na nejnovější verzi softwaru, se výrobci mohou i přesto rozhodnout pokračovat v řešení a nápravě zranitelností ve starších verzích tohoto softwaru, a to i za poplatek nebo na základě jiných obchodních ujednání. Akt nevyžaduje, aby výrobci poskytovali bezpečnostní aktualizace pro tyto starší verze zdarma.

134. Pokud podstatná změna tyto faktory neovlivňuje, kritéria stanovená v čl. 13 odst. 8 i nadále udávají stejnou očekávanou dobu použití, jaká byla původně určena, a doba podpory změněného produktu s digitálními prvky by měla odpovídat zbývající očekávané době použití produktu tak, jak byl původně uveden na trh. K tomu obvykle dochází v případech, kdy byla očekávaná doba použití určena především faktory, které daná změna nemění, jako je například fyzická životnost hardwarových komponent, přičemž podstatná změna se týká pouze funkčnosti softwaru nebo backendových služeb.

Příklad 54: Výrobce uvede na trh robotický vysavač s očekávanou dobou použití X let, která byla určena na základě povahy produktu s digitálními prvky, včetně fyzické odolnosti a charakteristik opotřebení hardwarových komponent, a s přihlédnutím k přiměřeným očekáváním uživatelů ohledně životnosti tohoto produktu. Výrobce stanoví dobu podpory na X let. Po Y letech vydá softwarovou aktualizaci, která představuje podstatnou změnu a přidává nové režimy úklidu a navigační funkce. Softwarová aktualizace nemá vliv na fyzickou odolnost hardwaru a nemění přiměřená očekávání uživatelů ohledně životnosti daného produktu. Kritéria podle čl. 13 odst. 8 tedy i nadále udávají stejnou očekávanou dobu použití. Doba podpory změněného produktu s digitálními prvky odpovídá zbývající, původně určené, očekávané době použití.

Příklad 55: Výrobce uvádí na trh složitý průmyslový strojní produkt s digitálními prvky, jehož cloudový backend představuje řešení pro zpracování dat na dálku. Očekávaná doba použití činí X let a byla určena s ohledem na přiměřená očekávání uživatelů a povahu produktu s digitálními prvky, jako je například fyzická odolnost hardwaru strojního zařízení a očekávané opotřebení. Doba podpory je stanovena tak, aby odpovídala očekávané době použití, která činí X let. Po Y letech výrobce přepracuje architekturu cloudového backendu (řešení pro zpracování dat na dálku) a zavede nová API a datové toky, a to způsobem, který je považován za podstatnou změnu produktu s digitálními prvky, aniž by však došlo ke změně povahy tohoto produktu nebo k ovlivnění očekávání uživatelů. Kritéria podle čl. 13 odst. 8 tedy i nadále udávají stejnou očekávanou dobu použití. Doba podpory změněného produktu s digitálními prvky odpovídá zbývající, původně určené, očekávané době použití.

135. Pokud podstatná změna ovlivňuje faktory, které původně určovaly očekávanou dobu použití produktu s digitálními prvky, měl by výrobce přepočítat dobu podpory tak, aby odrážela novou očekávanou dobu použití, a to s odpovídajícím uplatněním kritérií uvedených v čl. 13 odst. 8. To se může týkat například modernizačních hardwarových změn, které prodlužují životnost daného produktu, nebo podstatného přeprogramování či přepracování základního softwaru daného produktu, které významně mění jeho očekávanou dobu použití ([20]).

Příklad 56: Výrobce uvádí na trh programovatelný logický automat (PLC) s očekávanou dobou použití X let, která byla určena především na základě povahy produktu s digitálními prvky a životnosti podkladového hardwaru. Doba podpory je stanovena odpovídajícím způsobem. Několik let po prvním uvedení na trh provede výrobce podstatnou změnu spočívající v nahrazení vestavěné výpočetní platformy automatu PLC, včetně procesoru, paměti a běhového prostředí, komponentami nové generace, které jsou navrženy pro výrazně delší provozní životnost. V důsledku této změny se mění přiměřená očekávání uživatelů a povaha produktu s digitálními prvky: Uživatel PLC může nyní důvodně očekávat, že PLC bude díky nové výpočetní platformě nadále produktivně využíván i po uplynutí původně deklarované očekávané doby použití. Kritéria uvedená v čl. 13 odst. 8 tedy naznačují delší očekávanou dobu použití a výrobce podle toho přepočítá dobu podpory pro daný konkrétní PLC.

6. **DŮLEŽITÉ A KRITICKÉ PRODUKTY S DIGITÁLNÍMI PRVKY**

136. Ustanovení čl. 7 odst. 1 aktu stanoví, že produkty s digitálními prvky, jejichž klíčová funkce odpovídá produktové kategorii uvedené v příloze III tohoto nařízení, se považují za „důležité produkty s digitálními prvky“. Příloha III dále rozděluje důležité produkty s digitálními prvky na třídu I a třídu II. Podobně čl. 8 odst. 1 stanoví, že produkty s digitálními prvky, jejichž klíčová funkce odpovídá produktové kategorii uvedené v příloze IV aktu, se považují za „kritické produkty s digitálními prvky“ ([21]).

([20]) Je třeba připomenout, že jak je uvedeno v oddíle *4.1 Fyzické opravy,* renovace, údržba nebo opravy se obecně nepovažují za podstatné změny.

([21]) Prováděcí nařízení Komise (EU) 2025/2392 stanoví technický popis kategorií důležitých a kritických produktů.

137. Zařazení produktu s digitálními prvky do kategorie důležitých nebo kritických produktů či naopak do kategorie „standardní“ ([22]) má význam při určování postupu posuzování shody, který musí výrobce v souladu s článkem 32 dodržet předtím, než bude moci tento produkt s digitálními prvky uvést na trh. Je třeba poznamenat, že u produktů s digitálními prvky zařazených do standardní kategorie lze vždy uplatnit postup interní kontroly podle modulu A („vlastní posouzení“) ([23]). Důležité produkty s digitálními prvky třídy I nebo II a kritické produkty s digitálními prvky podléhají přísnějším postupům posuzování shody. To se nevztahuje na důležité produkty s digitálními prvky třídy I nebo II, které jsou považovány za svobodný software s otevřeným zdrojovým kódem a jsou uvedeny na trh; v jejich případě se výrobci mohou v souladu s čl. 32 odst. 5 řídit postupy stanovenými pro standardní kategorii.

138. Pojem klíčové funkce je pro výrobce tudíž zásadní při určování příslušného režimu posuzování shody. Tento pojem však není v aktu výslovně definován. Produkty s digitálními prvky mohou plnit celou řadu funkcí, z nichž některé mohou být doplňkové ke klíčové funkci daného produktu, a neměly by mít vliv na zařazení produktu mezi standardní produkty / důležité produkty třídy I / důležité produkty třídy II / kritické produkty. Je proto užitečné poskytnout výrobcům více pokynů, které jim pomohou správně provádět příslušné postupy posuzování shody, a podpořit orgány dozoru nad trhem při zajišťování harmonizovaného prosazování aktu v celé EU.

6.1 **Klíčová funkce**

139. Klíčová funkce produktu s digitálními prvky se vztahuje k jeho hlavním funkcím a technickým schopnostem, bez nichž by produkt nemohl plnit svůj zamýšlený účel. Lze to posoudit s ohledem na konkrétní kontext daného produktu a podmínky jeho používání, přičemž je třeba zohlednit mimo jiné informace, které výrobce uvádí v návodu k použití, v propagačních či prodejních materiálech a prohlášeních, jakož i v technické dokumentaci.

Příklad 57: Softwarový produkt s digitálními prvky poskytuje abstrakční vrstvu nad podkladovým hardwarem a řídí provádění softwarových komponent. Mezi jeho hlavní funkce patří inicializace hardwaru a periferií, správa procesů a paměti, řízení vstupů a výstupů, plánování, přidělování zdrojů a zpřístupňování systémových služeb a rozhraní pro programování aplikací (API), jejichž prostřednictvím aplikace interagují s hardwarovými a softwarovými zdroji zařízení. Z technické dokumentace vyplývá, že tento produkt s digitálními prvky koordinuje výpočetní zdroje, zajišťuje dodržování systémových konfigurací a poskytuje standardizovaná rozhraní pro softwarové moduly a propojená periferní zařízení. Výrobce zdůrazňuje, že díky těmto schopnostem může platforma sloužit jako centrální softwarové prostředí, ve kterém mohou aplikace běžet spolehlivě. Tento produkt s digitálními prvky má klíčovou funkci operačního systému, jak je popsáno v příloze I bodě 11 prováděcího nařízení (EU) 2025/2392.

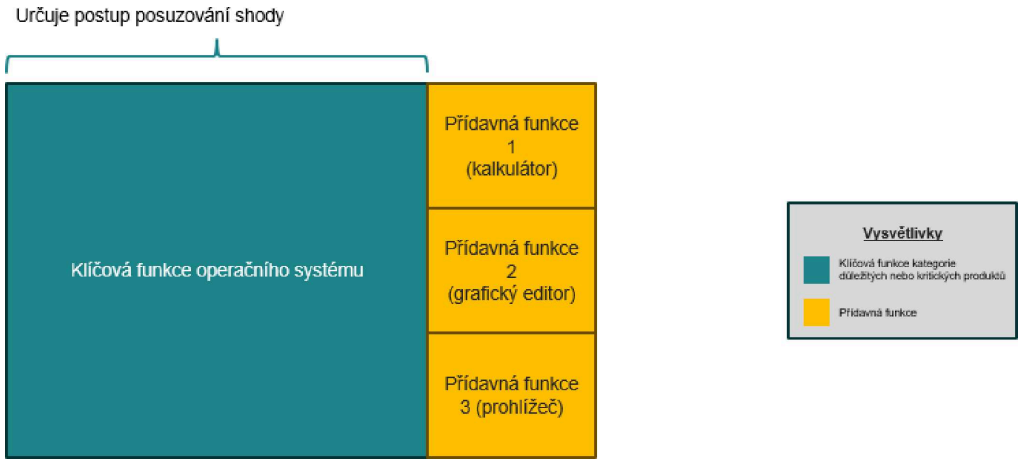
140. Funkčnost produktu s digitálními prvky se málokdy omezuje výhradně na jeho klíčovou funkci, neboť produkty s digitálními prvky často – ne-li vždy – plní i další funkce, které ke klíčové funkci produktu nepřispívají. To může zahrnovat i začlenění komponent, které samy o sobě plní funkci jiného důležitého či kritického produktu s digitálními prvky. Skutečnost, že produkt s digitálními prvky plní jiné nebo doplňkové funkce než ty, které jsou podrobně popsány v technických popisech důležitých nebo kritických produktů s digitálními prvky, však sama o sobě nebrání tomu, aby tento produkt měl jednu takovou klíčovou funkci.

([22]) Pojem „standardní“ kategorie není v aktu definován. V tomto dokumentu se tento pojem používá pro produkty s digitálními prvky, které nemají klíčovou funkci produktové kategorie stanovené v přílohách III nebo IV aktu, a na které se proto vztahuje režim posuzování shody stanovený v čl. 32 odst. 1.

([23]) Výrobce se nicméně může kdykoli rozhodnout, že použije přísnější postup posuzování shody, jak je stanoveno v čl. 32 odst. 1.

Obrázek 2:

Ilustrace toho, jak o použitém postupu posuzování shody rozhoduje klíčová funkce, a nikoli funkce doplňkové



141. Produkt s digitálními prvky může být schopen plnit funkce kategorie důležitých nebo kritických produktů, nicméně jeho klíčová funkce se od funkce této produktové kategorie liší. V takových případech by se tento produkt s digitálními prvky nepovažoval za důležitý ani kritický produkt s digitálními prvky. Jak je výslovně uvedeno v čl. 7 odst. 1 aktu pro důležité produkty s digitálními prvky (a při uplatnění stejné logiky i pro kritické produkty s digitálními prvky), pouhé začlenění důležitého nebo kritického produktu s digitálními prvky samo o sobě neznamená, že se produkt s digitálními prvky stává důležitým nebo kritickým produktem s digitálními prvky.

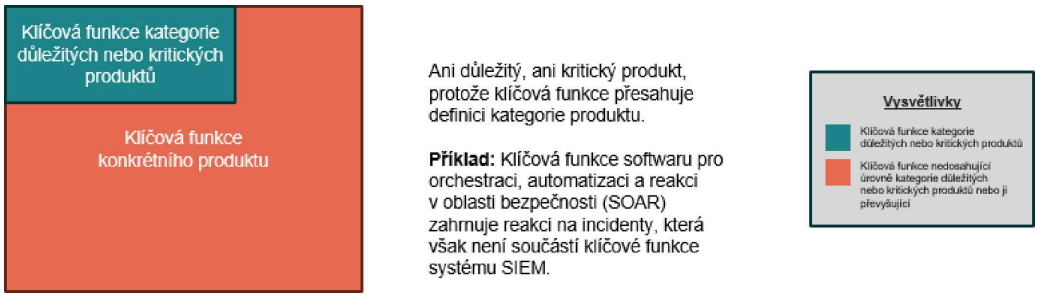
Příklad 58: Chytrý telefon obsahuje operační systém, který poskytuje funkce popsané v příloze I bodě 11 prováděcího nařízení (EU) 2025/2392. Zatímco operační systém umožňuje správu hardwarových zdrojů a provádění softwarových aplikací, chytrý telefon jako celek má odlišnou klíčovou funkci (např. umožňuje uživatelům komunikovat a mít přístup k informacím a službám). Samotné začlenění operačního systému neznamená, že chytrý telefon disponuje klíčovou funkcí operačního systému.

142. Některé produkty s digitálními prvky se mohou podobat kategorii důležitých nebo kritických produktů nebo mohou patřit do stejné obecné produktové řady, avšak jejich klíčová funkce může podstatně převyšovat klíčovou funkci dané kategorie nebo naopak může za ní podstatně zaostávat. To neplatí v případě, kdy produkt s digitálními prvky obsahuje další funkce, které pouze doplňují nebo vylepšují klíčovou funkci, jež sama o sobě odpovídá klíčové funkci kategorie důležitých nebo kritických produktů; v takových případech si produkt s digitálními prvky zachovává klíčovou funkci dané kategorie a je podle toho zařazen. Toto posouzení by mělo vycházet z hlavních funkcí a technických schopností daného produktu, které je třeba objektivně posoudit s ohledem na jeho zamýšlený účel, a nikoli ze způsobu, jakým je produkt s digitálními prvky popsán nebo propagován, pokud tento popis neodráží skutečné technické charakteristiky produktu.

Příklad 59: Software pro orchestraci, automatizaci a reakci v oblasti bezpečnosti (SOAR) je často schopen plnit funkce produktů s digitálními prvky v kategorii „systémy řízení bezpečnostních informací a událostí (SIEM)“, tj. sbírat data z více zdrojů, analyzovat je, dávat je do vzájemného vztahu a prezentovat je jako využitelné informace pro bezpečnostní účely. Klíčová funkce tohoto softwaru však zásadně přesahuje možnosti systému SIEM, neboť jako klíčové prvky svých technických schopností zahrnuje i služby, jako je reakce na incidenty. Proto se obecně má za to, že software SOAR nedisponuje klíčovou funkcí systémů SIEM.

Obrázek 3:

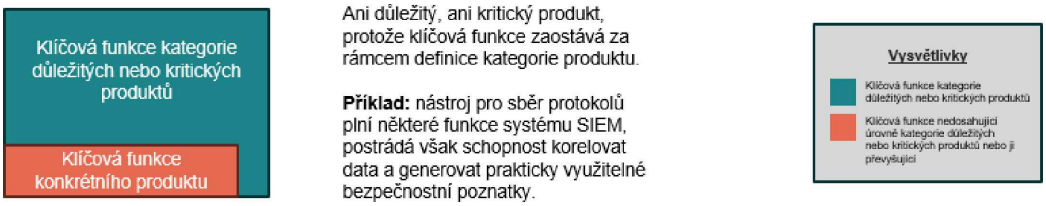
Ilustrace klíčové funkce produktu s digitálními prvky výrazně přesahující rámec definice kategorie důležitého nebo kritického produktu



Příklad 60: Některé nástroje pro sběr a vizualizaci protokolů dokážou načítat data z protokolů a zobrazovat základní řídicí panely s událostmi systému. Ačkoli tyto nástroje mohou podporovat činnosti v oblasti monitorování bezpečnosti, jejich klíčová funkce nedosahuje úrovně systémů SIEM, protože neprovádějí korelaci dat ani neposkytují prakticky využitelné bezpečnostní poznatky. Tyto nástroje se proto obecně nepovažují za nástroje disponující klíčovou funkcí systémů SIEM.

Obrázek 4:

Ilustrace klíčové funkce produktu s digitálními prvky výrazně zaostávající za rámcem definice kategorie důležitého nebo kritického produktu

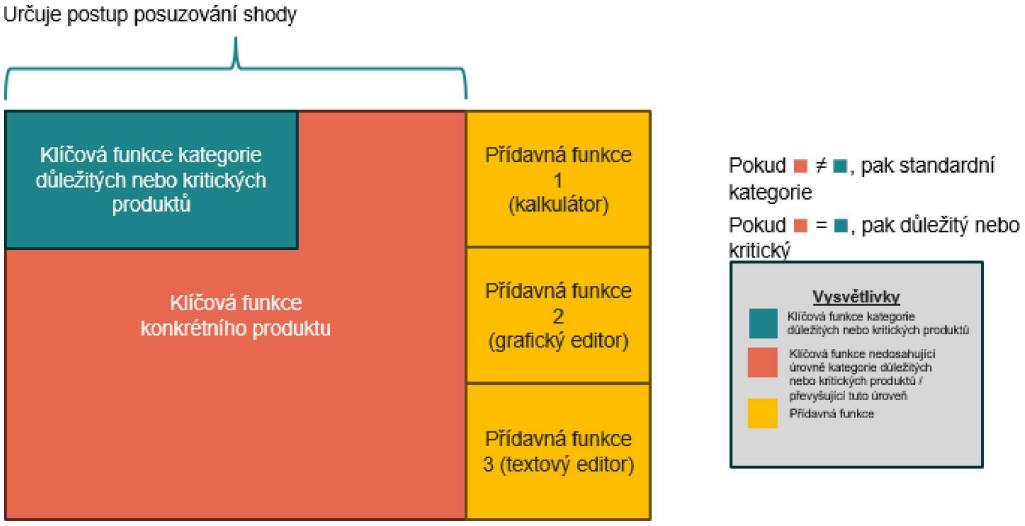


143. Výrobce nesmí uvádět zavádějící informace o klíčové funkci svého produktu s digitálními prvky, aby se vyhnul režimu posuzování shody příslušnému pro důležité nebo kritické produkty s digitálními prvky, např. tím, že by nadměrně zdůrazňoval nebo naopak bagatelizoval úlohu některých funkcí, takže by produkt klíčovou funkci podstatně překonával nebo by za ní zaostával. To by platilo například v případě, kdy existují zjevné nesrovnalosti mezi propagačními materiály, návody k použití a technickou dokumentací.

144. Produkt s digitálními prvky nesmí mít pro účely určení příslušného režimu posuzování shody více než jednu klíčovou funkci. V souladu s přílohou VII aktu jsou výrobci povinni v rámci technické dokumentace k produktu popsat zamýšlený účel svého produktu s digitálními prvky a postup posuzování shody, kterým se řídili. Je proto třeba jasně určit klíčovou funkci produktu. To umožňuje správně určit příslušný režim posuzování shody a dává orgánům dozoru nad trhem možnost vykonávat dozor a kontrolovat, zda je nařízení uplatňováno správně.

Obrázek 5:

Ilustrace toho, jak klíčová funkce konkrétního produktu s digitálními prvky určuje třídu produktu, a tím i příslušný postup posuzování shody



145. Některé produkty s digitálními prvky jsou uváděny na trh jako samostatné produkty s digitálními prvky, skládají se však z jednotlivých modulů s oddělenými funkcemi. Pokud výrobce tyto moduly dodává na trh také samostatně, například v případě, že jsou nabízeny k samostatnému zakoupení, na základě licence nebo v rámci předplatného, představují tyto moduly samy o sobě samostatné produkty s digitálními prvky. Proto je třeba je klasifikovat na základě jejich příslušných klíčových funkcí (a tudíž podléhají příslušnému režimu posuzování shody na základě klíčové funkce každého modulu). Tím nejsou dotčeny moduly dodávané výhradně jako komponenty integrovaného produktu s digitálními prvky a nedodávané samostatně; v takových případech se klíčová funkce určuje na úrovni integrovaného produktu s digitálními prvky.

Příklad 61: Výrobce uvádí na trh ucelenou bezpečnostní sadu, která spojuje několik modulů, včetně systému SIEM, systému detekce narušení a analytického modulu. Výrobce tyto moduly nabízí také v rámci samostatných předplatných. V tomto scénáři představuje každý modul samostatný produkt s digitálními prvky a je klasifikován na základě své vlastní klíčové funkce. Modul SIEM podléhá režimu posuzování shody pro důležité produkty s digitálními prvky třídy I, jelikož jeho klíčovou funkcí je funkce produktů kategorie „systémy řízení bezpečnostních informací a událostí (SIEM)“. Systém detekce narušení podléhá režimu posuzování shody pro důležité produkty s digitálními prvky třídy II, jelikož jeho klíčovou funkcí je funkce produktů kategorie „firewally, systémy detekce narušení a prevence“. Analytický modul podléhá režimu posuzování shody pro „standardní“ produkty s digitálními prvky, jelikož jeho klíčová funkce nespadá do kategorie důležitých nebo kritických produktů.

146. Nedodržení povinností stanovených v článku 32 aktu může vést k uložení správních pokut v souladu s čl. 64 odst. 3.

6.2 Posuzování shody u důležitých a kritických produktů s digitálními prvky

147. Jakmile výrobce určí klíčovou funkci svého produktu s digitálními prvky, musí provést jeden z příslušných postupů posuzování shody. Výrobce musí zajistit, aby produkt s digitálními prvky jako celek splňoval základní požadavky, přičemž musí v příslušných případech zohlednit bezpečnost komponent nebo funkcí, které jsou do něj začleněny.

148. U důležitých produktů s digitálními prvky třídy II (s výjimkou těch, které jsou v souladu s čl. 32 odst. 5 považovány za svobodný software s otevřeným zdrojovým kódem) a u kritických produktů s digitálními prvky je povinné přísnější posuzování shody za účasti třetí strany (na základě modulu B+C, modulu H nebo schémat certifikace kybernetické bezpečnosti) ([24]). Naopak důležité produkty s digitálními prvky třídy I (s výjimkou těch, které jsou v souladu s čl. 32 odst. 5 považovány za svobodný software s otevřeným zdrojovým kódem) musí projít postupem posuzování shody za účasti třetí strany pouze v případě, že výrobce nepoužil nebo použil pouze zčásti příslušné harmonizované normy, na něž byly zveřejněny odkazy v *Úředním věstníku Evropské unie* (dále jen „harmonizované normy"), společné specifikace nebo evropská schémata certifikace kybernetické bezpečnosti na úrovni záruky alespoň „významná" ([25]).

149. Aby tedy důležitý produkt s digitálními prvky třídy I byl způsobilý pro postup interní kontroly, i) je třeba uplatnit všechny použitelné požadavky příslušné harmonizované normy a ii) rozsah normy musí zahrnovat alespoň všechna kybernetická bezpečnostní rizika spojená s klíčovou funkcí daného produktu.

150. Rozsah produktu s digitálními prvky může být širší než rozsah stanovený příslušnou harmonizovanou normou a tyto dodatečné funkce mohou představovat odlišná či další kybernetická bezpečnostní rizika. Výrobce je vždy povinen provést posouzení rizik podle čl. 13 odst. 2, a měl by proto ověřit, zda zavedení harmonizované normy pokrývá všechna rizika spojená s produktem s digitálními prvky. Pokud zavedení normy všechna rizika nepokrývá, měl by výrobce jinými prostředky zajistit, aby jeho produkt s digitálními prvky splňoval základní požadavky.

151. Pokud tedy výrobce důležitého produktu s digitálními prvky třídy I použil příslušnou harmonizovanou normu, která pokrývá rizika spojená s klíčovou funkcí tohoto produktu, může se rozhodnout využít postup interní kontroly k prokázání shody svého produktu. V rámci činností při posuzování shody bude výrobce i nadále povinen prokázat, že jsou řešena všechna rizika, která se vztahují k jeho produktu s digitálními prvky. Pokud tedy existuje rozdíl mezi rozsahem působnosti harmonizované normy a rozsahem produktu s digitálními prvky jako celku, musí výrobce i nadále zdokumentovat, jaká dodatečná opatření přijal k řešení těchto rizik.

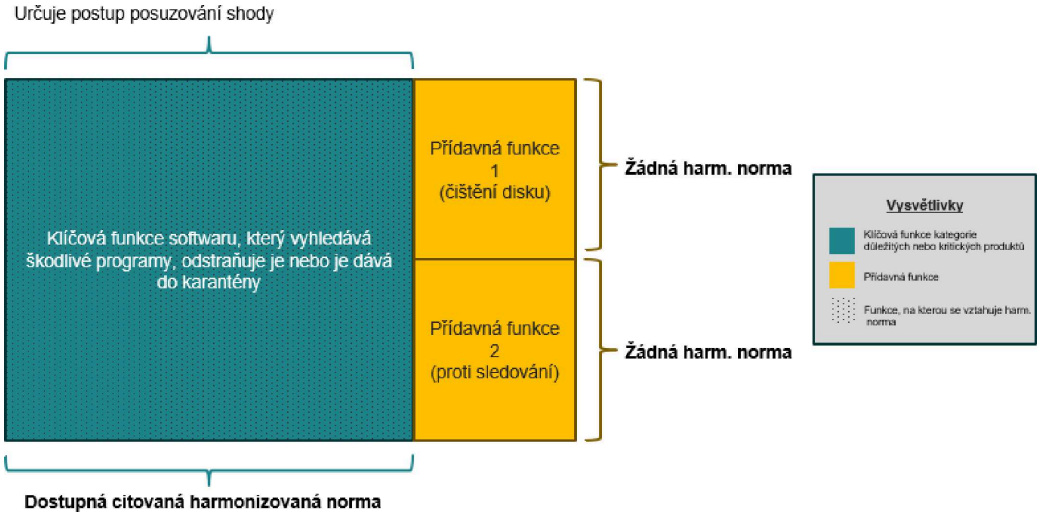
Příklad 62: Antivirový software má klíčovou funkci softwaru, který vyhledává škodlivé programy, odstraňuje je nebo je dává do karantény, jak je popsáno v příloze I bodě 4 prováděcího nařízení (EU) 2025/2392. Tento produkt s digitálními prvky obsahuje také další funkce, a to konkrétně funkci čištění disku a funkci proti sledování, která chrání uživatele při procházení internetu. Výrobce provádí posouzení rizik, které se vztahuje na celý produkt s digitálními prvky, včetně klíčové funkce antivirového programu, funkcí pro čištění disku a funkcí proti sledování. Uplatňuje harmonizovanou normu, která pokrývá rizika spojená s klíčovou funkcí antivirového programu, a dodatečná opatření k řešení rizik vyplývajících z dodatečných funkcí. Výrobce může pro posouzení shody využít postup interní kontroly, který se vztahuje na produkt s digitálními prvky jako celek, včetně funkcí čištění disku a funkcí proti sledování.

([24]) To platí i v případě, že se využije evropské schéma certifikace kybernetické bezpečnosti alespoň na úrovni záruky „významná", jelikož je vyžadována účast nezávislého certifikačního orgánu.

([25]) Z důvodu stručnosti se zbývající část tohoto oddílu vztahuje pouze na harmonizované normy, na něž byly zveřejněny odkazy v *Úředním věstníku Evropské unie*. Tyto pokyny se však vztahují také na společné specifikace přijaté v souladu s čl. 27 odst. 2 a na evropská schémata certifikace kybernetické bezpečnosti, pokud je Komise upřesní prostřednictvím aktů v přenesené pravomoci v souladu s čl. 27 odst. 9.

Obrázek 6:

Ilustrace toho, jak použití citované harmonizované normy, která se vztahuje pouze na klíčovou funkci, určuje příslušný postup posuzování shody



152. To platí i v případě, kdy produkt s digitálními prvky začleňuje dodatečnou funkci, která sama o sobě představuje funkci jiného důležitého nebo kritického produktu s digitálními prvky. Ve skutečnosti je to právě klíčová funkce produktu s digitálními prvky jako celku, a nikoli funkce jednotlivých začleněných komponent posuzovaná samostatně, co určuje, zda produkt s digitálními prvky spadá do kategorie důležitých nebo kritických produktů (a tedy i do příslušného režimu posuzování shody). Například pokud má produkt s digitálními prvky klíčovou funkci důležitého produktu s digitálními prvky třídy I, vztahuje se na tento produkt jako celek režim posuzování shody použitelný pro důležité produkty s digitálními prvky třídy I, i když začleňuje komponentu, která je sama o sobě kritickým produktem s digitálními prvky. V těchto případech, kdy výrobce uplatňuje harmonizovanou normu pokrývající rizika spojená s klíčovou funkcí daného produktu, je povoleno využít postup interní kontroly.

Příklad 63: Hardwarový produkt s digitálními prvky má klíčovou funkci směrovače, jak je popsáno v příloze I bodě 12 prováděcího nařízení (EU) 2025/2392. Tento produkt s digitálními prvky obsahuje také další funkce, včetně funkcí firewallu, jelikož je do něj začleněná firewallová komponenta. Výrobce provádí posouzení rizik, které se vztahuje na celý produkt s digitálními prvky, včetně klíčové funkce směrovače a funkce firewallu. Uplatňuje harmonizovanou normu, která pokrývá rizika spojená s klíčovou funkcí směrovače, a dodatečná opatření k řešení rizik vyplývajících z dodatečných funkcí. Výrobce může například uplatnit harmonizovanou normu pro firewally, aby pokryl rizika spojená s funkcí firewallu. Výrobce může pro posouzení shody využít postup interní kontroly, který se vztahuje na produkt s digitálními prvky jako celek, včetně funkce firewallu.

6.3 Důsledky pro předpoklad shody

153. Ustanovení čl. 27 odst. 1 aktu stanoví, že se předpokládá, že produkty s digitálními prvky a postupy zavedené výrobcem, které jsou ve shodě s harmonizovanými normami nebo jejich částmi, na něž byly zveřejněny odkazy v *Úředním věstníku Evropské unie (Úřední věstník)*, jsou ve shodě se základními požadavky aktu, na které se tyto

normy nebo jejich části vztahují ([26]). Ustanovení čl. 27 odst. 5 rozšiřuje tento předpoklad shody na produkty s digitálními prvky a postupy zavedené výrobcem, které jsou ve shodě se společnými specifikacemi přijatými Komisí prostřednictvím prováděcích aktů, a čl. 27 odst. 8 stanoví předpoklad shody pro produkty s digitálními prvky a postupy zavedené výrobcem, pro něž bylo vydáno EU prohlášení o shodě nebo certifikát v rámci evropského schématu certifikace kybernetické bezpečnosti přijatého podle nařízení (EU) 2019/881, pokud to bylo upřesněno prostřednictvím aktů v přenesené pravomoci v souladu s čl. 27 odst. 9 ([27]).

154. Pokud tedy výrobce použil harmonizovanou normu, na kterou byl zveřejněn odkaz v Úředním věstníku, platí pro něj předpoklad shody, pokud jde o rizika, na která se tato norma vztahuje. To by mohlo platit například v případě, kdy harmonizovaná norma, na kterou bylo odkázáno, pokrývá všechna rizika spojená s klíčovou funkcí produktu s digitálními prvky a neexistují žádné další funkce, které by představovaly kybernetická bezpečnostní rizika. Očekává se například, že harmonizovaná norma pro směrovače bude řešit alespoň rizika spojená s klíčovou funkcí těchto produktů s digitálními prvky. Pokud takový produkt neobsahuje žádné další funkce nebo pokud tyto další funkce nepředstavují rizika, na která norma nebere ohled, lze u produktu s digitálními prvky uplatnit předpoklad shody.

155. V případech rozebraných v bodech 151 a 152 může výrobce použít postup interní kontroly, protože harmonizovaná norma pokrývá rizika spojená s klíčovou funkcí produktu s digitálními prvky. Produkty s digitálními prvky popsané v těchto příkladech však mohou přesahovat rozsah působnosti harmonizovaných norem a jejich další funkce mohou představovat kybernetická bezpečnostní rizika, na která se taková harmonizovaná norma nevztahuje. U těchto produktů s digitálními prvky proto nemusí platit předpoklad shody, pokud jde o tyto další funkce.

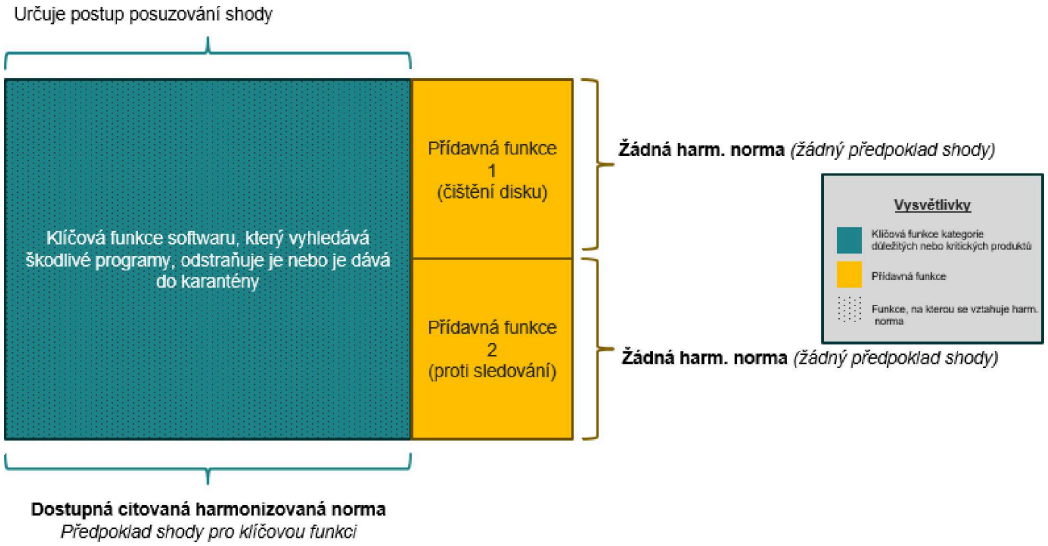
Příklad 64: Antivirový software má klíčovou funkci softwaru, který vyhledává škodlivé programy, odstraňuje je nebo je dává do karantény, a rizika spojená s touto klíčovou funkcí pokrývá harmonizovaná norma. Tento produkt s digitálními prvky obsahuje také další funkce, a to konkrétně funkci čištění disku a funkci proti sledování, která chrání uživatele při procházení internetu, přičemž rizika spojená s těmito funkcemi nejsou pokryta harmonizovanou normou. V případě použití harmonizované normy může výrobce pro posouzení shody využít postup interní kontroly. Na tento produkt se bude vztahovat předpoklad shody, pokud jde o rizika spojená s jeho klíčovou funkcí, nikoli však o rizika spojená s dalšími funkcemi.

([26]) Jak je jasně uvedeno v oddíle 4.1.2.2 Modré příručky, „[v] harmonizačních právních předpisech týkajících se rizik […] výrobci, i když používají harmonizované normy, na něž byl zveřejněn odkaz v *Úředním věstníku Evropské unie*, jsou i nadále plně odpovědní za posouzení všech rizik svého výrobku a určení toho, které základní (či jiné) požadavky jsou relevantní. Po tomto posouzení se pak může výrobce rozhodnout, že technické specifikace uvedené v harmonizovaných normách, na něž byl zveřejněn odkaz v *Úředním věstníku Evropské unie*, použije k provedení ‚opatření ke snížení rizika', která jsou v harmonizovaných normách stanovena".

([27]) Stejně jako výše z důvodu stručnosti se zbývající část tohoto oddílu vztahuje pouze na harmonizované normy, na něž byly zveřejněny odkazy v *Úředním věstníku Evropské unie*. Tyto pokyny se však vztahují i na společné specifikace a na evropská schémata certifikace kybernetické bezpečnosti.

Obrázek 7:

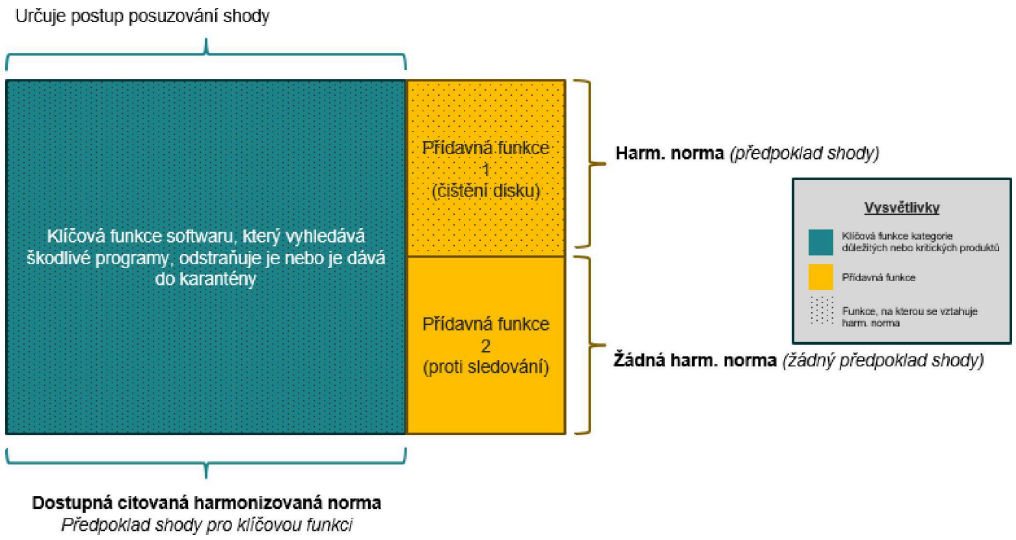
Harmonizovaná norma poskytuje předpoklad shody pro klíčovou funkci, jelikož řeší všechna rizika s ní spojená, nikoli však pro další funkce.



Příklad 65: Ve stejném scénáři jako v předchozím příkladu byla harmonizovaná norma nyní aktualizována tak, aby zahrnovala také rizika spojená s jednou z dalších funkcí, a to konkrétně s funkcí čištění disku, nikoli však s druhou funkcí (tj. funkcí proti sledování). V případě použití harmonizované normy může výrobce pro posouzení shody využít postup interní kontroly. Na tento produkt se bude vztahovat předpoklad shody, pokud jde o rizika spojená s jeho klíčovou funkcí a funkcí čištění disku, nikoli však o rizika spojená s funkcí proti sledování.

Obrázek 8:

Harmonizovaná norma poskytuje předpoklad shody pro klíčovou funkci a přídavnou funkci 1, jelikož řeší všechna rizika spojená s těmito dvěma funkcemi, nikoli však pro přídavnou funkci 2.



7. **POSOUZENÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH RIZIK A ZAČLENĚNÍ PRODUKTŮ S DIGITÁLNÍMI PRVKY A KOMPONENT**

7.1 **O hodnocení a řešení kybernetických bezpečnostních rizik**

156. Posouzení kybernetických bezpečnostních rizik stanovené v čl. 13 odst. 2 aktu ukládá výrobcům povinnost identifikovat příslušná rizika a posoudit jejich potenciální dopad na produkt s digitálními prvky. V souladu se základními požadavky přílohy I musí výrobci rovněž zavést vhodná opatření k řešení těchto rizik.

157. V rámci řízení rizik v organizaci se rizika obvykle posuzují podle kritérií přijatelnosti, která vycházejí z interních cílů organizace nebo z její ochoty podstupovat riziko. Naopak podle aktu by mělo být zbytkové kybernetické bezpečnostní riziko posuzováno s ohledem na požadavek, aby produkt s digitálními prvky uvedený na trh zajišťoval přiměřenou úroveň kybernetické bezpečnosti s ohledem na rizika, přičemž je třeba zohlednit jeho zamýšlený účel a rozumně předvídatelné použití.

158. V souladu s tím není při určování, zda byla rizika náležitě řešena, relevantní ani vnitřní míra tolerance rizika výrobce, ani jeho obchodní strategie, ani pouhé zohlednění nákladů. Pro účely čl. 13 odst. 2 a 3 musí být výrobci schopni určit, zda byla zjištěná kybernetická bezpečnostní rizika dostatečně řešena zavedením základních požadavků části I přílohy I, a to s ohledem na zamýšlený účel, rozumně předvídatelné použití a podmínky použití, včetně, je-li to relevantní, provozního prostředí (například zamýšlených uživatelů produktu s digitálními prvky) a aktiv, která mají být chráněna, přičemž se zohlední očekávaná doba použití produktu s digitálními prvky.

159. Zbytkové kybernetické bezpečnostní riziko je neodmyslitelným výsledkem posouzení rizik a jejich řešení. Je všeobecně známo, že kybernetická bezpečnostní rizika nelze v praxi zcela odstranit. Existence zbytkového rizika však neznamená, že by výrobce mohl podle vlastního uvážení akceptovat jakékoli riziko. Produkt s digitálními prvky smí být uveden na trh pouze tehdy, jsou-li zbytková rizika po přijetí vhodných opatření dostatečně řešena dodržením základních požadavků, a to s přihlédnutím k zamýšlenému účelu a rozumně předvídatelnému použití produktu s digitálními prvky.

160. V souladu s čl. 13 odst. 3 jsou výrobci v případě zjištění kybernetických bezpečnostních rizik povinni tato rizika řešit pomocí vhodných opatření, a to i na úrovni produktu. V závislosti na okolnostech to může znamenat například zmenšení plochy pro útoky, zavedení technických ochranných opatření, omezení či přizpůsobení funkce nebo přesnější vymezení zamýšleného účelu produktu s digitálními prvky. Výrobci mohou rovněž podniknout kroky k formování rozumně předvídatelného způsobu použití produktu s digitálními prvky, například prostřednictvím informování o rizicích, pokynů pro uživatele nebo návrhu uživatelského rozhraní, s cílem nasměrovat chování uživatelů k bezpečným vzorcům použití.

161. Akt nestanoví převod kybernetických bezpečnostních rizik ani odpovědnosti na uživatele či třetí strany za účelem kompenzace nedostatků v návrhu produktu nebo jako ospravedlnění toho, že kybernetická bezpečnostní rizika zůstanou neřešena. Povinnost uvést na trh bezpečný produkt s digitálními prvky a prokázat jeho shodu se základními požadavky zůstává na výrobci.

162. Informace a pokyny poskytované uživatelům mohou být využity k podpoře bezpečného nasazení a provozu produktu s digitálními prvky, a to i v případech, kdy se výrobce rozhodl omezit zamýšlený účel daného produktu na důvěryhodná prostředí, a k informování uživatelů o zbytkových rizicích, a to způsobem, který je vhodný pro povahu produktu s digitálními prvky a jeho zamýšlené uživatele.

Příklad 66: Výrobce vyvíjí průmyslový senzor určený pro použití v důvěryhodných prostředích. Aby senzor správně plnil svou funkci, výrobce nezavádí žádná opatření na ochranu před fyzickými útoky na samotný senzor. Za účelem zmírnění souvisejících rizik zjištěných při posouzení rizik omezí výrobce zamýšlený účel senzoru výhradně na důvěryhodná prostředí, v nichž je zabráněno neoprávněnému fyzickému přístupu k produktu s digitálními prvky. Informace a pokyny pro uživatele uvádějí jasné informace o těchto omezeních při používání senzoru způsobem, který je vhodný pro povahu produktu s digitálními prvky a jeho zamýšlené uživatele.

Příklad 67: Výrobce vyvíjí softwarovou aplikaci pro profesionální použití ve spravovaných stolních počítačích a mobilních zařízeních. Aplikace zpracovává lokálně uložená citlivá data a obsah vytvořený uživatelem. V rámci posouzení rizik výrobce identifikuje riziko neoprávněného přístupu k těmto datům, jsou-li uložena v zařízení v otevřeném textu. Místo toho, aby výrobce navrhl a zavedl vlastní šifrovací mechanismus přímo v aplikaci, rozhodl se využít funkce šifrování a správy klíčů, které nativně poskytuje operační systém, na kterém má aplikace běžet, jelikož vestavěné kryptografické služby tohoto operačního systému jsou vyspělé a pravidelně udržované.

163. Pokud posouzení kybernetických bezpečnostních rizik zjistí rizika, která nelze přiměřeně řešit pomocí vhodných opatření, může být v souladu s aktem nutné provést změny v návrhu, funkci nebo zamýšleném účelu produktu s digitálními prvky. Úvahy týkající se výhradně nákladů nebo obchodní proveditelnosti nepředstavují dostatečný důvod k tomu, aby se taková rizika neřešila, pokud by v důsledku toho produkt s digitálními prvky nesplňoval základní požadavky.

7.2 Navrhování, vývoj a výroba produktů s digitálními prvky tak, aby byla zajištěna odpovídající úroveň kybernetické bezpečnosti zohledňující rizika

164. Základní požadavek na kybernetickou bezpečnost, na který odkazuje bod 1 části I přílohy I aktu, stanoví, že produkty s digitálními prvky musí být navrženy, vyvinuty a vyrobeny tak, aby zajišťovaly odpovídající úroveň kybernetické bezpečnosti zohledňující rizika.

165. Cílem tohoto základního požadavku je řešit všechna kybernetická bezpečnostní rizika, která byla zjištěna v rámci jejich posouzení. Jedná se zejména o kybernetická bezpečnostní rizika, která nejsou jinak přiměřeně řešena v rámci provádění základních požadavků části I přílohy I jiných než uvedených v bodě 1. Tento základní požadavek se liší od zákonné povinnosti provést posouzení kybernetických bezpečnostních rizik, které se provádí podle čl. 13 odst. 2.

166. Jsou-li všechna relevantní kybernetická bezpečnostní rizika související s produktem s digitálními prvky řešena zavedením přiměřených opatření ke splnění příslušných základních požadavků jiných než uvedených v bodě 1, považuje se základní požadavek uvedený v bodě 1 části I přílohy I za splněný. Naopak, pokud posouzení kybernetických bezpečnostních rizik odhalí další rizika, která tato opatření plně neřeší, jsou výrobci povinni zavést u produktů s digitálními prvky vhodná opatření k řešení těchto rizik, aby splňovaly základní požadavek uvedený v bodě 1 části I přílohy I. V praxi se ve většině případů očekává, že splnění ostatních základních požadavků povede k splnění i tohoto požadavku.

7.3 Posouzení rizik a náležitá péče v souvislosti s externími závislostmi a začleněnými komponentami

167. Akt stanoví pro výrobce dvě odlišné, avšak vzájemně se doplňující povinnosti v souvislosti s řízením kybernetických bezpečnostních rizik. Zaprvé, čl. 13 odst. 2 ukládá výrobcům povinnost provést u samotného produktu s digitálními prvky posouzení kybernetických bezpečnostních rizik. Zadruhé, čl. 13 odst. 5 ukládá povinnost postupovat v souvislosti se začleňovanými komponentami s náležitou péčí. Cílem těchto dvou povinností je společně zajistit, aby produkt s digitálními prvky zůstal bezpečný, a to i v případech, kdy využívá řešení pro zpracování dat na dálku, vzdálené služby nebo softwarové či hardwarové komponenty třetích stran.

168. Posouzení kybernetických bezpečnostních rizik se týká určení a řízení relevantních rizik, která mohou mít dopad na produkt s digitálními prvky, včetně rizik vznikajících externě, tedy mimo samotný produkt, jako jsou externí sítě, faktory prostředí nebo jiné vnější aspekty, které by mohly produkt s digitálními prvky ovlivnit nebo na něž se tento produkt spoléhá. V případě těchto vnějších rizik akt nevyžaduje, aby výrobci kontrolovali či řídili vnější prostředí. Výrobci jsou naopak povinni tato rizika zjistit a zmírnit je již v rámci samotného návrhu a vývoje produktu s digitálními prvky. Součástí toho bude zavedení odpovídajících základních požadavků stanovených v části I přílohy I a v případě potřeby poskytnutí informací a pokynů uživatelům ohledně rizik spojených se začleněním nebo zavedením.

169. Výrobce může například zjistit riziko, že neoprávněné osoby mohou během provozu produktu s digitálními prvky získat přístup k backendovým systémům, které nejsou součástí samotného produktu, a pokusí se do tohoto produktu odeslat škodlivé příkazy. Takové backendové systémy, které nejsou navrženy a vyvinuty výrobcem nebo pod jeho odpovědností, nebo které nepodporují žádnou z funkcí produktu s digitálními prvky, nepředstavují řešení pro zpracování dat na dálku, a proto pro účely aktu nespadají do rozsahu produktu s digitálními prvky. Akt nicméně vyžaduje, aby výrobce řešil rizika, která mohou z těchto systémů plynout, prostřednictvím opatření na úrovni produktu, jako je například požadavek na kryptografické ověřování vzdálených příkazů, ověřování integrity změn konfigurace nebo generování bezpečnostních protokolů či výstrah v případě zjištění neobvyklého chování. Podobně v případě, že výrobce zjistí riziko vyplývající z nedostupnosti takové externí služby, například v důsledku výpadků napájení nebo poruch infrastruktury, může akt požadovat opatření ke zmírnění těchto kybernetických bezpečnostních rizik na úrovni produktu, např. zajištění, aby výpadek nezpůsobil, že se produkt s digitálními prvky dostane do nezabezpečeného stavu. V takových případech akt upravuje, jak má produkt s digitálními prvky reagovat na tato vnější rizika; nestanoví žádné povinnosti ohledně toho, jak má být backendová infrastruktura organizována, personálně obsazena nebo provozována, ani tuto infrastrukturu nepovažuje za součást produktu s digitálními prvky.

170. Náležitá péče se vztahuje na prvky, které jsou součástí samotného produktu s digitálními prvky, zejména na začleněné softwarové nebo hardwarové komponenty poskytované třetí stranou. Výrobci jsou povinni přijmout vhodná opatření, aby zajistili, že tyto komponenty neohrozí soulad produktu s digitálními prvky se základními požadavky. Toho lze dosáhnout pouze určením, co produkt s digitálními prvky požaduje od svých komponent, aby byly splněny jeho kybernetické bezpečnostní cíle, a ověřením na základě posouzení rizik, zda jsou tyto komponenty v souladu s potřebami produktu, jak je rovněž uvedeno v 34. bodě odůvodnění.

171. V souladu s posouzením kybernetických bezpečnostních rizik musí výrobce určit požadavky, které by začleněná komponenta měla splňovat. Pokud například produkt s digitálními prvky využívá kryptografické funkce, mechanismy aktualizace nebo zabezpečenou komunikaci poskytované určitou součástí, musí výrobce v rámci své náležité péče tyto potřeby určit a ověřit, zda je daná komponenta splňuje. Důkazy pro tento účel může tvořit dokumentace získaná od výrobce komponenty, jako jsou technické specifikace, bezpečnostní dokumentace nebo příslušná dokumentace o shodě či záruce. V případě potřeby může výrobce rovněž provést zkoušky s cílem ověřit, zda tyto komponenty plní příslušné funkce dostatečně. Ačkoli je náležitá péče samostatnou zákonnou povinností, podporuje a posiluje schopnost výrobce prokázat soulad se základními požadavky na produkt s digitálními prvky jako celek.

172. Při posuzování rizik pro produkt s digitálními prvky jako celek je třeba v rámci posouzení kybernetických bezpečnostních rizik zohlednit i prvky mimo produkt, jako jsou prvky prostředí, vnější infrastruktura, jiné systémy nebo sítě, a v příslušných případech je řešit prostřednictvím opatření na úrovni produktu, aby byl zajištěn soulad produktu s digitálními prvky se základními požadavky. V rámci posouzení rizik je třeba zohlednit i komponenty, které jsou fyzicky či logicky začleněny do produktu s digitálními prvky, avšak pocházejí od třetí strany. Pro účely souladu by však výrobce měl tyto komponenty, jejichž vlastnosti jsou ověřovány v rámci náležité péče při začleňování, považovat za komponenty dodané externě, jelikož je možné, že je výrobce znovu nenavrhl ani nevyvinul.

173. Stejná logika platí i při vývoji a začleňování komponent. Pokud výrobce vyvíjí funkce sám, musí základní požadavky zavést přímo. Pokud výrobce začleňuje komponenty vyvinuté jinými subjekty, musí prostřednictvím náležité péče zajistit, aby tyto komponenty bylo možné použít tak, aby produkt s digitálními prvky jako celek splňoval příslušné požadavky. V obou případech zůstává cíl stejný: aby produkt s digitálními prvky, uvedený na trh, dosahoval odpovídající úrovně kybernetické bezpečnosti požadované aktem, a to s přihlédnutím k rizikům zjištěným při posouzení kybernetických bezpečnostních rizik.

7.4 **Opětovné použití posouzení rizik a dokumentace o shodě pro řady produktů s digitálními prvky**

174. Výrobci mohou uvádět na trh produkty s digitálními prvky, které si jsou podobné, například různé varianty, modely nebo konfigurace téže produktové řady. Pokud mají takové produkty s digitálními prvky stejnou architekturu, návrh z hlediska bezpečnosti a zamýšlený účel a jsou vystaveny stejným kybernetickým bezpečnostním rizikům, akt nevyžaduje, aby výrobci pro účely posouzení rizik a posouzení shody zacházeli s každou variantou jako se zcela samostatným produktem s digitálními prvky.

175. V takových případech, za předpokladu, že jsou všechny dotčené varianty z hlediska příslušných rizik a základních požadavků přiměřeně pokryty, se výrobci mohou opírat o: i) jediné posouzení kybernetických bezpečnostních rizik provedené v souladu s čl. 13 odst. 2 aktu; ii) jediný soubor technické dokumentace a iii) jediný postup posuzování shody. To rovněž umožňuje vydat jediné EU prohlášení o shodě pro skupinu produktů s digitálními prvky, pokud v něm jsou jasně uvedeny varianty produktů, na které se vztahuje.

176. Rozhodujícím faktorem je, zda jsou rozdíly mezi jednotlivými variantami relevantní pro kybernetickou bezpečnost. Variace, které nemají vliv na vlastnosti produktu s digitálními prvky z hlediska kybernetické bezpečnosti, jako jsou rozdíly v barvě, tvaru, velikosti paměti nebo jiné charakteristiky, které nesouvisejí s bezpečností, nevyžadují samostatná posouzení rizik ani posouzení shody. Naopak v některých případech se varianty mohou lišit v aspektech, které mají vliv na plnění základních požadavků, například prostřednictvím odlišných komunikačních rozhraní, softwarových balíčků, mechanismů aktualizace nebo vzdáleného připojení. V takových případech se tyto rozdíly musí projevit v posouzení rizik a v případě potřeby také v posouzení shody a v technické dokumentaci.

177. Výrobci jsou i nadále povinni zajistit, aby posouzení rizik a související dokumentace přesně odrážely produkty s digitálními prvky uváděné na trh. Pokud nová varianta přináší nová kybernetická bezpečnostní rizika nebo mění způsob, jakým jsou plněny základní požadavky, je nutné stávající posouzení rizik a dokumentaci o shodě odpovídajícím způsobem aktualizovat. Spoléhat se na jediné posouzení shody je možné pouze za předpokladu, že produkty s digitálními prvky nevykazují rozdíly ve vlastnostech z hlediska kybernetické bezpečnosti.

8. **ZPRACOVÁNÍ DAT NA DÁLKU**

178. V čl. 3 bodě 1 aktu je produkt s digitálními prvky definován jako „softwarový nebo hardwarový produkt a jeho řešení pro zpracování dat na dálku, včetně softwarových nebo hardwarových komponent, které jsou uváděny na trh samostatně“. V tomto kontextu musí výrobce posuzovat produkt s digitálními prvky jako celek, včetně řešení pro zpracování dat na dálku. Například při prokazování toho, že produkt s digitálními prvky splňuje základní požadavky stanovené v příloze I, je třeba zohlednit řešení pro zpracování dat na dálku, a to již od fáze posouzení rizik (čl. 13 odst. 2). Totéž platí i při posuzování povinností v rámci celého životního cyklu, jako je například oznamování aktivně zneužívaných zranitelností a závažných incidentů (článek 14).

179. Účelem těchto pokynů je poskytnout výrobcům další podporu při určování, zda jejich produkt s digitálními prvky má řešení pro zpracování dat na dálku podle aktu, a informace o tom, jak plnit v tomto ohledu jejich povinnosti týkající se souladu. Po úvodní analýze definic a bodů odůvodnění stanovených v aktu budou tyto pokyny obsahovat otázky, které výrobcům pomohou objasnit, zda jejich produkt s digitálními prvky obsahuje řešení pro zpracování dat na dálku (viz oddíl *8.1 Co se považuje za řešení pro zpracování dat na dálku u produktu s digitálními* prvky?). Následně se budou zabývat technickými dopady řešení pro zpracování dat na dálku a tím, jak posuzovat soulad s aktem (viz oddíl *8.2 Praktické a technické důsledky řešení pro zpracování dat na dálku a využívání řešení třetích* stran).

180. Ustanovení čl. 3 bodu 2 totiž definuje pojem „zpracování dat na dálku“ jako „zpracování dat na dálku, pro které výrobce navrhuje a vyvíjí software nebo za jehož návrh a vývoj výrobce odpovídá, přičemž neexistence tohoto softwaru by bránila tomu, aby produkt s digitálními prvky plnil některou ze svých funkcí“. Řešení pro zpracování dat na dálku se proto definuje jako softwarové prvky („část elektronického informačního systému, která sestává z počítačového kódu“, jak je definováno v čl. 3 bodě 4) zpracování dat na dálku. Do rozsahu produktu s digitálními prvky nemá být zahrnut hardware, na němž může být zpracování dat na dálku založeno.

181. V 11. a 12. bodě odůvodnění jsou uvedena další vysvětlení toho, jak by měl být tento pojem vykládán. V 11. bodě odůvodnění je upřesněno, že cílem zahrnutí řešení pro zpracování dat na dálku je, aby „produkty byly jejich výrobci odpovídajícím způsobem zabezpečeny v celém rozsahu bez ohledu na to, zda jsou data zpracovávána nebo uchovávána lokálně v zařízení uživatele, nebo na dálku výrobcem“. Také uvádí, že „požadavky týkající se řešení pro zpracování dat na dálku, která spadají do oblasti působnosti tohoto nařízení, proto nezahrnují technická, provozní nebo organizační opatření, jejichž cílem je řídit bezpečnostní rizika, jimž jsou vystaveny sítě a informační systémy výrobce jako celek“.

182. Z 11. bodu odůvodnění tedy vyplývá, že záměrem není, aby se požadavky aktu vztahovaly na celou IT infrastrukturu organizace, nýbrž pouze na softwarové komponenty, které umožňují provoz řešení pro zpracování dat. Za řešení pro zpracování dat na dálku by neměly být považovány například interní systémy týkající se vlastních lidských zdrojů výrobce, mzdového účetnictví, řízení vztahů se zákazníky, procesů průběžné integrace a průběžného dodávání (CI/CD) či distribuce bezpečnostních aktualizací do okrajových lokalit. Stejně tak systémy spojené s činnostmi auditu a zkoušek, jako je penetrační testování, vyhledávání hrozeb a red teaming, nespadají do rozsahu produktu s digitálními prvky, na který se vztahuje akt. Je důležité poznamenat, že ačkoli provádění účinných a pravidelných zkoušek a přezkumů bezpečnosti produktu s digitálními prvky představuje základní požadavek stanovený v bodě 3 části II přílohy I aktu, neznamená to, že tyto činnosti mají být považovány za řešení pro zpracování dat na dálku pro daný produkt s digitálními prvky.

183. 12. bod odůvodnění se zaměřuje na cloudové služby a podrobněji rozebírá okolnosti, za nichž by cloudové služby mohly být pokládány za řešení pro zpracování dat na dálku. V závěru tento bod odůvodnění připomíná, že služby cloud computingu a modely cloudových služeb spadají do oblasti působnosti směrnice (EU) 2022/2555 (NIS 2) ([28]), která stanoví požadavky na řízení kybernetických bezpečnostních rizik pro poskytovatele služeb cloud computingu. Tyto požadavky jsou blíže specifikovány prováděcím nařízením Komise (EU) 2024/2690 ([29]).

8.1 **Co se považuje za řešení pro zpracování dat na dálku u produktu s digitálními prvky?**

184. Definice zpracování dat na dálku uvedená v čl. 3 bodě 2 se tedy opírá o tři prvky: i) zda se zpracování dat provádí „na dálku“; ii) zda by neexistence takového zpracování dat bránila tomu, aby produkt s digitálními prvky plnil některou ze svých funkcí, a iii) zda byl software navržen a vyvinut výrobcem nebo zda za návrh a vývoj výrobce odpovídá. Každému z těchto prvků je věnována větší pozornost v následujících třech pododdílech.

([28]) 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, ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27).

([29]) Prováděcí nařízení Komise (EU) 2024/2690 ze dne 17. října 2024, kterým se stanoví pravidla pro uplatňování směrnice (EU) 2022/2555, pokud jde o technické a metodické požadavky na opatření k řízení kybernetických bezpečnostních rizik a bližší upřesnění případů, v nichž se incident považuje za významný, pokud jde o provozovatele DNS, registry domén nejvyšší úrovně, poskytovatele služeb cloud computingu, poskytovatele služeb datových center, poskytovatele sítí pro doručování obsahu, poskytovatele řízených služeb, poskytovatele řízených bezpečnostních služeb, poskytovatele on-line tržišť, internetových vyhledávačů a služeb platforem sociálních sítí a poskytovatele služeb vytvářejících důvěru (Úř. věst. L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

8.1.1 *Pojem „na dálku“*

185. Pojem „na dálku“, který uvádí čl. 3 bod 2, je sice významný, ale nestačí k určení, zda produkt s digitálními prvky zahrnuje řešení pro zpracování dat na dálku. Vzhledem k rozmanitosti řešení, která by mohla spadat pod tento pojem, navíc nelze poskytnout vyčerpávající definici spojení „na dálku“. Je nutné, aby výrobce posoudil každý případ individuálně.

186. V 11. bodě odůvodnění aktu se hovoří o datech zpracovávaných nebo uchovávaných „na dálku výrobcem“ na rozdíl od dat zpracovávaných nebo uchovávaných „lokálně v zařízení uživatele“. Zpracování dat na dálku se obvykle odehrává mimo uživatelské prostředí produktu s digitálními prvky nebo mimo provozní prostředí organizace (v případě profesionálního uživatele). To však nebrání tomu, aby ke zpracování docházelo také v blízkosti zařízení („na okraji sítě“). Přenos dat může probíhat kabelově (např. ethernetovým kabelem) nebo bezdrátově (např. přes Wi-Fi, Bluetooth). Typický příklad zpracování dat, k němuž dochází „na dálku“, představuje cloud computing, včetně výpočetních operací na okraji sítě (edge computing). Například v případě cloudové funkce, ke které má uživatel přístup z mobilní aplikace, se část zpracování dat odehrává v cloudu, mimo prostředí uživatele.

187. Je důležité si uvědomit, že řešení pro zpracování dat na dálku nemusí být nutně provozováno na cloudové infrastruktuře třetí strany. Řešení pro zpracování dat na dálku může představovat i zpracování dat na dálku probíhající na lokálních serverech v prostorách výrobce. Jinými slovy, řešení provozované v lokálním prostředí a v soukromém cloudu může splňovat kritéria pro zařazení mezi řešení pro zpracování dat na dálku stejně jako řešení provozované ve veřejném cloudu a mimo lokální prostředí.

188. Obě rozhodující a kumulativní otázky, které určují, zda se akt vztahuje na zpracování dat jako řešení pro zpracování dat na dálku, jsou uvedeny níže v oddílech *8.1.2* a *8.2*. Jsou-li obě otázky zodpovězeny kladně, lze zpracování dat na dálku považovat za řešení pro zpracování dat na dálku.

8.1.2 *Bránila by neexistence takového zpracování dat tomu, aby produkt s digitálními prvky plnil některou ze svých funkcí?*

189. Jak stanoví definice pojmu „zpracování dat na dálku“ uvedená v čl. 3 bodě 2, aby bylo zpracování dat na dálku považováno za řešení pro zpracování dat na dálku, musela by jeho neexistence bránit produktu s digitálními prvky ve výkonu jedné z jeho funkcí. Pojem „funkce“ obsažený v této definici se neomezuje pouze na „klíčovou funkci“ či „zamýšlený účel“ produktu s digitálními prvky, jelikož akt takové omezení nestanovuje. Funkce spadající do oblasti působnosti aktu zahrnují jak funkce, které přímo naplňují zamýšlený účel produktu s digitálními prvky z pohledu uživatelů, tak funkce, které podporují celkovou výkonnost produktu.

190. Mezi příklady funkcí, u nichž může docházet ke zpracování dat na dálku a jejichž neexistence by bránila produktu s digitálními prvky ve výkonu jedné z jeho funkcí, patří například: i) odesílání příkazů do zařízení; ii) synchronizace souborů; iii) registrace uživatele; iv) konfigurace (přizpůsobení produktu s digitálními prvky); v) automatická distribuce aktualizací, včetně aktualizace funkcí a bezpečnostních oprav; vi) správa identit a řízení přístupu.

191. V některých případech může uživatel danou funkci ovládat jak na dálku, tak ručně (např. zapínat žárovku pomocí aplikace nebo ručně). Existence této možnosti nevylučuje, aby zpracování dat související s výkonem funkce na dálku bylo považováno za řešení pro zpracování dat na dálku. Provádění této funkce na dálku je rovněž považováno za součást funkcí, které nabízí produkt s digitálními prvky.

192. Naopak, pokud neexistence určitého zpracování dat nebrání produktu s digitálními prvky v plnění žádné z jeho funkcí, nepokládá se takové zpracování za řešení pro zpracování dat na dálku ve smyslu aktu. To zahrnuje například vzdálenou analýzu telemetrických dat shromážděných výhradně pro statistické účely nebo pro budoucí vývoj produktů.

193. Nicméně i když zpracování dat nepodporuje funkci produktu s digitálními prvky, může být nutné, aby výrobci v rámci svého posouzení kybernetických bezpečnostních rizik zvážili, zda tyto vzdálené komponenty představují pro produkt s digitálními prvky riziko (např. s ohledem na provozní prostředí produktu), a tato rizika odpovídajícím způsobem zmírnili (např. opatřeními na úrovni produktu).

194. Specifický případ, který si zaslouží bližší vysvětlení, jak je také uvedeno v *oddíle 2.1 Uvádění na trh*, představují internetové stránky. Jak je vysvětleno v 11. bodě odůvodnění aktu, internetové stránky nespadají do rozsahu řešení pro zpracování dat na dálku, pokud nepodporují funkci produktu s digitálními prvky. K tomu, aby internetové stránky spadaly do rozsahu řešení pro zpracování dat na dálku, nestačí, že obsahují informace o produktu s digitálními prvky, a to ani v případě, že daný produkt na takové internetové stránky odkazuje. Například přesměrování uživatelů na externí webovou stránku, která jim poskytuje informace a pokyny, se nepovažuje za řešení pro zpracování dat na dálku. Naopak internetové stránky mohou spadat do rozsahu řešení pro zpracování dat na dálku, pokud umožňují nebo podporují funkci produktu s digitálními prvky. Například autentizační portál, který vydává přihlašovací údaje nebo tokeny potřebné k fungování produktu s digitálními prvky, by byl považován za řešení pro zpracování dat na dálku (za předpokladu, že jsou splněna i ostatní kritéria definice).

8.1.3 *Byl software navržen a vyvinut výrobcem nebo odpovídá výrobce za jeho návrh a vývoj?*

195. Definice pojmu „zpracování dat na dálku“ uvedená v čl. 3 bodě 2 aktu dále upřesňuje, že software pro takové zpracování dat na dálku musí být navržen a vyvinut výrobcem nebo výrobce za jeho návrh a vývoj odpovídá. Zpracování dat na dálku, které bylo zcela vyvinuto a navrženo výrobcem (vlastními silami), by se přirozeně dalo považovat za řešení pro zpracování dat na dálku. To by platilo i v případě, že by se výrobci při vývoji a návrhu řešení spoléhali na externího poskytovatele služeb (tj. „odpovídá“). Spojení „výrobce odpovídá“ se vztahuje na řešení pro zpracování na dálku, která jsou přizpůsobena konkrétnímu výrobci. Jedná se o případy, kdy se výrobce neomezuje na získání licence na stávající produkt s digitálními prvky nebo službu, kterou poskytovatel služeb nabízí svým zákazníkům, nebo na jejich mírně upravené verze. „[V]ýrobce odpovídá“ znamená, že software je vyvinut výhradně výrobcem nebo jeho jménem na základě návrhů a specifikací, které poskytl.

196. Při chápání řešení pro zpracování dat na dálku není rozhodujícím faktorem „kdo řešení provozuje“, jelikož definice v aktu odkazuje pouze na návrh a vývoj řešení pro zpracování dat na dálku. To je v souladu s přístupem aktu, podle něhož se požadavky a povinnosti vztahují na výrobce, a nikoli na provoz produktu s digitálními prvky. Pokud výrobci navrhují a vyvíjejí řešení, která následně provozuje třetí strana, zůstávají i nadále odpovědni za dodržování základních požadavků aktu na produkt s digitálními prvky, který uvádějí na trh.

197. Je třeba rozlišovat mezi případy, kdy návrh a vývoj provádějí výrobci (nebo za ně odpovídají), a případy, kdy se využívá řešení třetích stran, která výrobci nenavrhli ani nevyvinuli (ani za jejich návrh a vývoj neodpovídají). Jako příklad je přínosné uvést nejběžnější modely cloudových služeb, které zajišťují různou míru kontroly ze strany uživatelů a které jsou rovněž uvedeny ve 12. bodě odůvodnění aktu, a to konkrétně software jako služba (SaaS), platforma jako služba (PaaS) a infrastruktura jako služba (IaaS).

198. V případě řešení IaaS třetí strany výrobce nespravuje ani neřídí podkladové fyzické a virtuální zdroje (jako je například podkladový hardware a hypervizor poskytovatele cloudových služeb), je však schopen pomocí těchto zdrojů zavádět a provozovat libovolný software, například operační systémy a aplikace. Takový software je navržen a vyvinut výrobcem nebo za jeho návrh a vývoj odpovídá výrobce, a může být proto považován za řešení pro zpracování dat na dálku (pokud splňuje i ostatní prvky definice).

199. V případě řešení PaaS třetí strany zavádí výrobce svou vlastní (vytvořenou nebo zakoupenou) aplikaci s využitím programovacích jazyků a prováděcích prostředí dodávaných poskytovatelem cloudových služeb a začleňuje tuto aplikaci do svého produktu s digitálními prvky. Výrobce má kontrolu nad aplikací a případně i nad konfiguračními nastaveními prováděcího prostředí. Aplikace je navržena a vyvinuta výrobcem nebo za její návrh a vývoj odpovídá výrobce, a může být proto považována za řešení pro zpracování dat na dálku (pokud splňuje i ostatní prvky definice).

200. V případě řešení SaaS třetí strany nabízí poskytovatel SaaS výrobci plně vyvinutou aplikaci, kterou výrobce může začlenit do svého produktu s digitálními prvky. Pokud jde o správu uživatelských nastavení konfigurace aplikace, má výrobce omezené možnosti. Aplikaci tedy nenavrhl a nevyvinul výrobce ani za její návrh a vývoj neodpovídá.

201. Nicméně v případech, kdy některé prvky nejsou považovány za řešení pro zpracování dat na dálku (např. hypervizor v případě infrastruktury IaaS třetí strany, operační systém v případě řešení PaaS třetí strany nebo aplikace SaaS třetí strany), ale jsou do produktu s digitálními prvky začleněny způsobem, který ovlivňuje jeho bezpečnost, měla by být taková řešení považována za podobná komponentám třetích stran. Výrobce je povinen určit a posoudit rizika spojená se začleněním těchto prvků a řešit je tak, že splní základní požadavky kladené na samotný produkt s digitálními prvky. V příslušných případech lze toto podpořit bezpečnostními funkcemi, které poskytovatel cloudových služeb dodává v rámci svého modelu sdílené odpovědnosti, přičemž výrobce tyto funkce využívá nebo konfiguruje za účelem řešení zjištěných rizik. Kromě toho se od výrobce očekává, že bude plnit povinnost podobnou povinnosti postupovat s náležitou péčí podle čl. 13 odst. 5, pokud jde o bezpečnost těchto komponent, a to způsobem přiměřeným riziku, které dané vzdálené řešení představuje pro bezpečnost produktu s digitálními prvky.

202. Lze tedy shrnout, že:

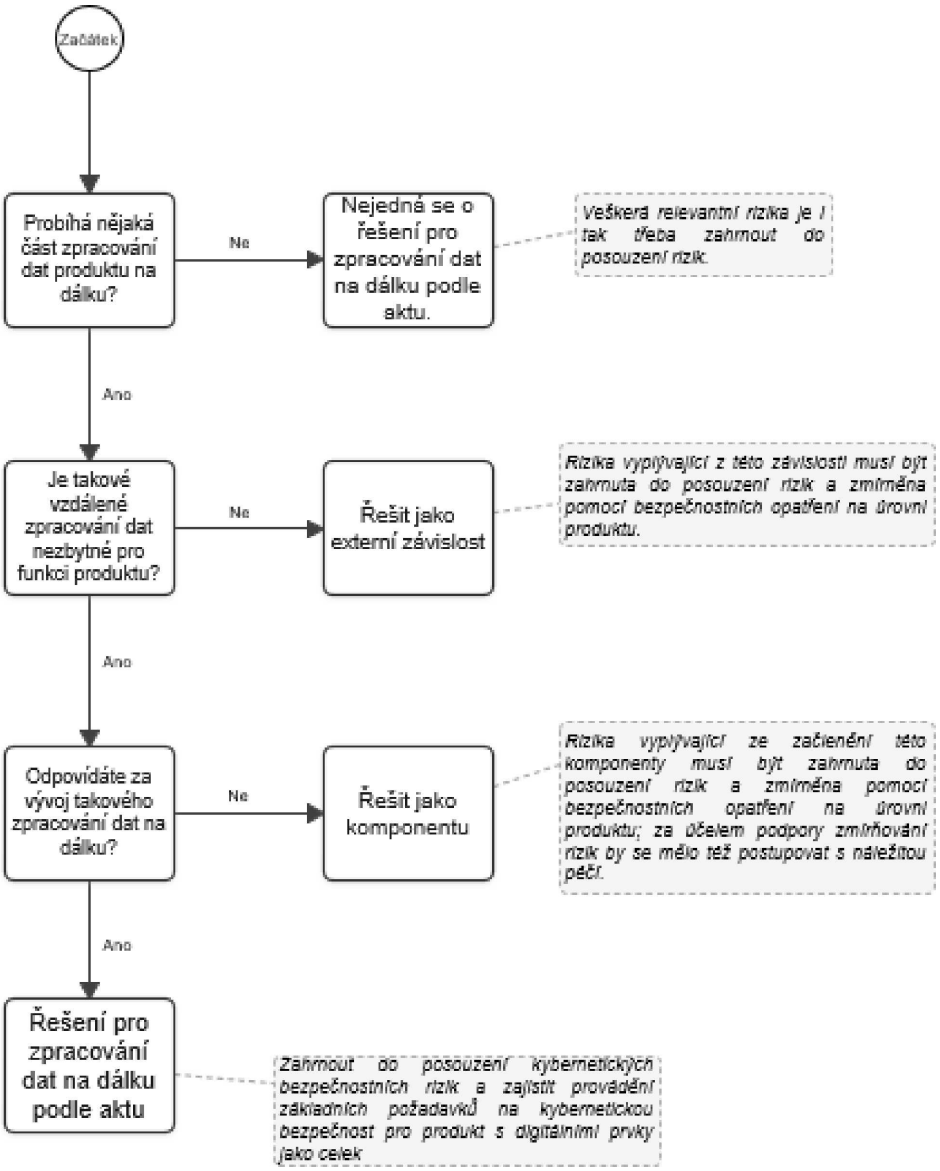
a) Aby bylo zpracování dat považováno za řešení pro zpracování dat na dálku, musí být odpověď na obě otázky položené v oddílech *8.1.2 Bránila by neexistence takového zpracování dat tomu, aby produkt s digitálními prvky plnil některou ze svých funkcí?* a *8.1.3 Byl software navržen a vyvinut výrobcem nebo odpovídá výrobce za jeho návrh a vývoj?* kladná.

b) Pokud je odpověď na otázku v oddíle *8.1.2 Bránila by neexistence takového zpracování dat tomu, aby produkt s digitálními prvky plnil některou ze svých funkcí?* záporná, měli by výrobci v rámci svého posouzení rizik vyhodnotit rizika vyplývající z existence takového zpracování dat.

c) Pokud je odpověď na otázku v oddíle *8.1.2 Bránila by neexistence takového zpracování dat tomu, aby produkt s digitálními prvky plnil některou ze svých funkcí?* kladná, ale odpověď na otázku v oddíle *8.1.3 Byl software navržen a vyvinut výrobcem nebo odpovídá výrobce za jeho návrh a vývoj?* je záporná, měli by výrobci přistupovat k řešení třetí strany jako ke komponentě. V rámci posouzení rizik by výrobci měli vyhodnotit rizika vyplývající ze začlenění takového řešení a odpovídajícím způsobem je zmírnit. Kromě toho by výrobci měli postupovat s náležitou péčí.

Obrázek 9

Stylizovaný vývojový diagram pro určení, zda produkt s digitálními prvky obsahuje řešení pro zpracování dat na dálku



8.2 Praktické a technické důsledky řešení pro zpracování dat na dálku a využívání řešení třetích stran

203. Akt se řídí přístupem založeným na riziku, který je zakotven v čl. 13 odst. 2 a 3, jakož i v prvním základním požadavku části I přílohy I, podle něhož „[p]rodukty s digitálními prvky musí být navrženy, vyvinuty a vyrobeny tak, aby zajišťovaly odpovídající úroveň kybernetické bezpečnosti zohledňující rizika“. Při uplatňování požadavků aktu na řešení pro zpracování dat na dálku a při zacházení s riziky, která plynou ze služeb třetích stran začleněných do produktu s digitálními prvky, by tudíž měl být zohledněn přístup založený na riziku.

204. Zaprvé by výrobci měli i) v technické dokumentaci uvést, že jejich produkt s digitálními prvky má řešení pro zpracování dat na dálku nebo se opírá o vzdálená řešení třetích stran, a ii) taková řešení popsat. Pokud stejné řešení pro zpracování dat na dálku podporuje několik produktů s digitálními prvky, je nutné jej uvést v technické dokumentaci každého z těchto produktů. Dokumentaci týkající se řešení pro zpracování dat na dálku, které se vztahuje na několik produktů s digitálními prvky, lze znovu použít při posuzování shody u jiného produktu.

205. Jak je uvedeno v 11. bodě odůvodnění, řešení pro zpracování dat na dálku, která jsou součástí produktu s digitálními prvky a na která se proto vztahuje posuzování shody produktu, by se měla omezit na ty softwarové moduly, které zajišťují funkčnost produktu s digitálními prvky, a na rozhraní, která tyto moduly používají s externími službami. Další backendové systémy, které provádějí následné zpracování a s nimiž produkt s digitálními prvky přímo neinteraguje, se nepovažují za řešení pro zpracování dat na dálku.

206. Tyto backendové systémy však i nadále představují externí závislosti, které je třeba vyhodnotit v rámci posouzení kybernetických bezpečnostních rizik a které je třeba zmírnit opatřeními na úrovni produktu. Posouzení rizik provedené výrobcem by mělo ve skutečnosti zohlednit: i) rizika související s řešením pro zpracování dat na dálku; ii) rizika spojená s využíváním vzdálených řešení třetích stran (podobně jako u komponent třetích stran) a iii) rizika související s prostředím produktu (např. s podkladovým hardwarem). Výrobci by měli u produktů s digitálními prvky zavést bezpečnostní opatření, aby tato rizika zmírnili.

207. Dále lze v rámci posuzování shody a/nebo plnění povinností náležité péče spojených se vzdálenými službami třetích stran použít na podporu posouzení prováděného výrobcem opět následující neúplný seznam dokladů o zajištění bezpečnosti:

a) doklad o splnění povinností podle prováděcího nařízení Komise (EU) 2024/2690;

b) doklad o splnění povinností podle nařízení (EU) 2022/2554 (DORA);

c) prohlášení o shodě nebo certifikát získaný v rámci evropského schématu certifikace kybernetické bezpečnosti (přijatého na základě nařízení (EU) 2019/881 – aktu o kybernetické bezpečnosti);

d) doklad o shodě s normou ISO/IEC 27017:2015 nebo ISO/IEC 27001:2022.

208. A konečně, při svých interakcích s poskytovateli vzdálených služeb třetích stran musí výrobci zavést nejvhodnější bezpečnostní opatření na základě svého posouzení rizik (a případně s oporou v modelu sdílené odpovědnosti daného poskytovatele). Tato zmírňující opatření by měla zahrnovat bezpečnostní opatření u jejich produktů s digitálními prvky a ověřování bezpečnostních opatření, která poskytují samotní externí poskytovatelé (náležitá péče). Jedním z nástrojů ke zmírnění těchto rizik může být začlenění bezpečnostních záruk do smluv o úrovni služeb (SLA) uzavíraných s externími poskytovateli, včetně záruk, že poskytovatelé přiměřeně nakládají se zranitelnostmi. Významná změna v řešeních poskytovaných externími poskytovateli vzdálených služeb by neměla být považována za podstatnou změnu produktu s digitálními prvky, jelikož za tyto prvky nenese odpovědnost výrobce. V rámci svých povinností náležité péče a za účelem správného zmírnění rizik plynoucích z využívání služeb externích poskytovatelů jsou však výrobci vybízeni k zajištění, aby je jejich externí poskytovatelé cloudových služeb přiměřeně informovali o změnách, které ve svých řešeních zavádějí. Na základě těchto informací budou výrobci možná muset revidovat své posouzení rizik. Aktualizované posouzení rizik by mělo zohlednit, zda externí poskytovatelé služeb stále poskytují dostatečné záruky v oblasti kybernetické bezpečnosti a zda jsou bezpečnostní opatření na úrovni produktu stále přiměřená. V některých případech může být nutné, aby výrobci tato opatření upravili nebo změnili externí poskytovatele služeb.

8.3 **Případy použití pro řešení pro zpracování dat na dálku**

S cílem poskytnout výrobcům další praktické pokyny představuje tento oddíl řadu fiktivních případů použití, které popisují typické produkty s digitálními prvky opírající se o zpracování dat na dálku a ilustrují, zda lze takové zpracování považovat za řešení pro zpracování dat na dálku ve smyslu aktu.

8.3.1 *Aplikace pro mobilní bankovnictví*

Finanční subjekt uvede na trh aplikaci pro mobilní bankovnictví. Backendové systémy této aplikace podporují mimo jiné ověřování totožnosti, autorizaci, správu účtů a platby. S cílem podpořit funkce aplikace využívá finanční subjekt hybridní strategii, kdy se opírá jak o vlastní infrastrukturu, tak o vzdálená řešení třetích stran. Patří mezi ně:

Vlastní infrastruktura vyvinutá finančním subjektem:

— Zákazník otevře aplikaci pro mobilní bankovnictví a jeho totožnost je ověřena prostřednictvím bankovního rozhraní, což je řešení provozované na vlastním serveru, které daný finanční subjekt vyvinul a které přijímá požadavky aplikace a vrací odpovídající odpovědi. Bankovní rozhraní ověřuje totožnost zákazníka dotazem na systém správy účtů a uděluje přístup k aplikaci.

— Zákazník zahájí prostřednictvím aplikace převod. Aplikace předá pokyn do bankovního rozhraní, které odešle odpovídající požadavek do systému účetní knihy.

— Transakci zaznamená systém pro správu účtů a systém účetní knihy, které jsou sice provozovány na vlastním serveru, ale logicky odděleny od bankovního rozhraní.

— Systém účetní knihy vrací stav transakce do bankovního rozhraní, které výsledek zobrazí zákazníkovi.

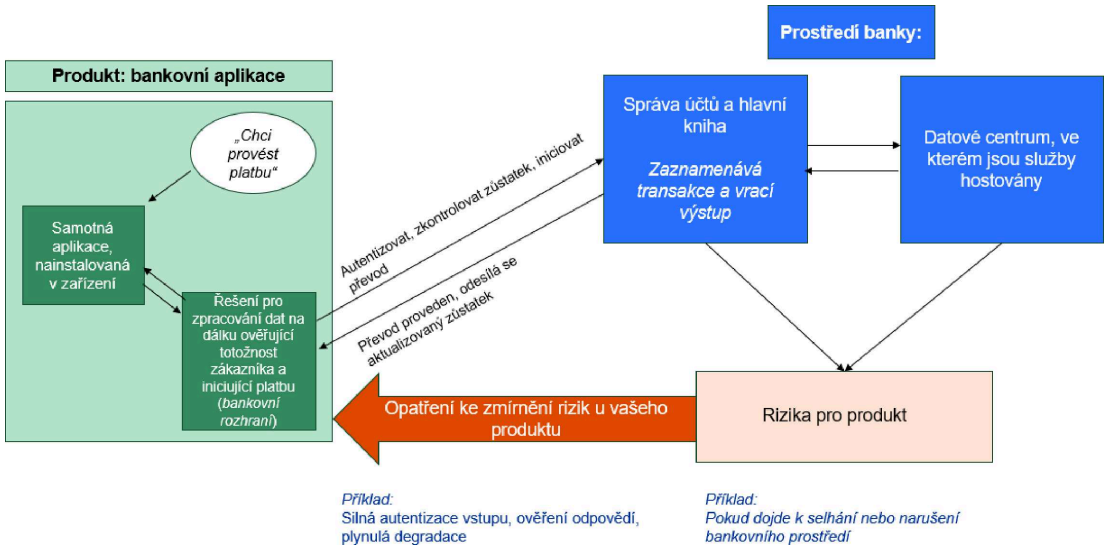
Důsledky pro řešení pro zpracování dat na dálku:

— Bankovní rozhraní je nezbytné k tomu, aby aplikace mohla vykonávat své funkce, konkrétně ověřování zákazníka, odesílání jeho pokynů, včetně platebních a převodních příkazů, a vracení výsledného stavu. Za návrh a vývoj bankovního rozhraní odpovídá výrobce. Jelikož odpověď na obě otázky uvedené v předchozích oddílech je kladná, je třeba bankovní rozhraní považovat za řešení pro zpracování dat na dálku. Musí být proto zahrnuto do posouzení kybernetických bezpečnostních rizik a do provádění základních požadavků na produkt s digitálními prvky jako celek. Následné zpracování již odeslaného příkazu, zejména zaevidování transakce v systému pro správu účtů a v systému účetní knihy, vypořádání a zúčtování, probíhá prostřednictvím systémů, s nimiž aplikace neinteraguje přímo, a z tohoto důvodu se nejedná o řešení pro zpracování dat na dálku.

— Systém správy účtů a systém účetní knihy nejsou považovány za řešení pro zpracování dat na dálku pro bankovní aplikaci. Aplikace s nimi neinteraguje přímo (místo toho interaguje s bankovním rozhraním, které se zase spoléhá na ně). Ačkoli může být jejich dostupnost nezbytná pro splnění určité funkce, akt se vztahuje pouze na ty části systému, které přímo interagují s produktem s digitálními prvky. Z tohoto důvodu nespadají do definice řešení pro zpracování dat na dálku pro účely aktu. Tyto systémy však představují externí závislosti, které mohou pro produkt s digitálními prvky představovat významná kybernetická bezpečnostní rizika. Například narušení systému účetní knihy by mohlo útočníkovi umožnit ovlivnit výsledky transakcí, které se následně zobrazí v aplikaci. Výrobce je proto povinen tato rizika určit a posoudit v rámci posouzení kybernetických bezpečnostních rizik a zmírnit je opatřeními na úrovni produktu, jako je silná autentizace backendových rozhraní, ochrana integrity transakčních dat, zabezpečené komunikační kanály a ověřování odpovědí přijatých aplikací.

Obrázek 10:

Stylizované znázornění bankovní aplikace využívající řešení pro zpracování dat na dálku



SaaS třetí strany pro zákaznickou podporu:

— Finanční subjekt začlení do své aplikace řešení pro chat se zákaznickou podporou, které vyvinul a provozuje externí poskytovatel; externí poskytovatel napsal kód chatového serveru, vytvořil uživatelské rozhraní a provozuje infrastrukturu, na které je chat nasazen (tj. model SaaS).

— Jakmile zákazník iniciuje žádost o podporu, aplikace ho propojí se službou třetí strany za účelem navázání chatové relace a zajištění toku zpráv, aniž by této třetí straně poskytla přístup k hlavním bankovním systémům.

Důsledky pro řešení pro zpracování dat na dálku:

— Řešení chatu podpory je nezbytné pro to, aby produkt s digitálními prvky mohl plnit jednu ze svých funkcí, není však navrženo ani vyvinuto finančním subjektem, a finanční subjekt ani neodpovídá za jeho návrh a vývoj; nejedná se tedy o řešení pro zpracování dat na dálku. Mělo by se s ním však zacházet jako s komponentou třetí strany. Využití této služby třetí strany může pro bankovní aplikaci představovat kybernetická bezpečnostní rizika, například pokud by útočník využil chatový kanál k tomu, aby se vydával za banku nebo aby uživatelům doručoval škodlivý obsah. Finanční subjekt musí tato rizika zohlednit při posuzování kybernetických bezpečnostních rizik a musí je zmírnit pomocí opatření na úrovni produktu, jako je izolování chatové funkce od klíčových bankovních funkcí, kontrola toků dat a ověřování obsahu. S náležitou péčí je rovněž třeba postupovat u služby SaaS.

8.3.2 *Chytrý termostat*

Chytrý termostat umožňuje uživatelům regulovat teplotu v jejich domovech přes mobilní aplikaci. Mobilní aplikace a chytrý termostat využívají zpracování dat na dálku k výměně dat (např. požadavek na zvýšení teploty) a k ukládání dat (např. uživatelská nastavení). Za vývoj a návrh těchto funkcí odpovídá výrobce, ale funkce běží na podkladové fyzické a virtuální infrastruktuře poskytované třetí stranou (IaaS třetí strany).

Jelikož by chytrý termostat nebyl bez tohoto zpracování dat na dálku schopen vykonávat své chytré funkce, neexistence tohoto zpracování by bránila produktu s digitálními prvky vykonávat jednu nebo více jeho funkcí. Za návrh a vývoj softwaru navíc odpovídá výrobce chytrého termostatu. Zpracování dat na dálku se tedy považuje za řešení pro zpracování dat na dálku definované v aktu.

Za účelem dodržení požadavků aktu musí výrobce chytrého termostatu v technické dokumentaci k produktu s digitálními prvky zdokumentovat řešení pro zpracování dat na dálku i využívání služeb IaaS třetí strany, včetně podrobností o sjednané službě. Výrobce musí tyto prvky zohlednit v posouzení rizik, které zahrnuje zamýšlený účel a rozumně předvídatelné použití produktu s digitálními prvky. Výrobce zavádí základní požadavky aktu na základě rizik spojených s řešením pro zpracování dat na dálku. V případě IaaS třetí strany musí výrobce zajistit, aby bezpečnostní opatření poskytovaná externím poskytovatelem byla přiměřená, a/nebo musí přijmout příslušná opatření týkající se této infrastruktury. V prvním případě by výrobce mohl například požadovat doklad o splnění povinností podle směrnice NIS 2.

8.3.3 *Čtečka elektronických knih*

Výrobce softwaru pro čtečky elektronických knih využívá službu úložiště SaaS třetí strany k ukládání elektronických knih zakoupených zákazníky a k tomu, aby jim umožnil přístup k těmto knihám. Neexistence této služby úložiště by bránila produktu s digitálními prvky vykonávat jednu z jeho funkcí, avšak službu úložiště SaaS třetí strany nevyvinul výrobce ani za její vývoj nenese odpovědnost; poskytovatel služby SaaS ji zákazníkům zpřístupňuje pro jakékoli použití.

Služba úložiště SaaS nesplňuje definici řešení pro zpracování dat na dálku. Výrobce čteček elektronických knih se však při fungování svého produktu s digitálními prvky opírá o tuto externí službu, a proto musí při posuzování kybernetických bezpečnostních rizik zohlednit související rizika. Výrobce čteček elektronických knih by měl se službou SaaS zacházet jako s komponentou. Výrobce musí zavést vhodná bezpečnostní opatření na úrovni produktu, jako je bezpečné ověřování, šifrování a ochrana integrity komunikace se službou úložiště. Plnění povinností výrobce podpoří též náležitá péče při výběru a začlenění poskytovatele SaaS, aby produkt s digitálními prvky jako celek mohl splňovat základní požadavky.

8.3.4 *Průmyslový robot*

Úkolem průmyslového robota je sbírat součástky. Robot odesílá informace shromážděné pomocí kamer do vzdálené služby, kterou navrhl a vyvinul výrobce. Tato služba běží na podkladové fyzické a virtuální infrastruktuře poskytované externím poskytovatelem služby (IaaS třetí strany). Cloudová služba vypočítává polohu součástky na základě záběrů z kamery a odesílá zpět příkazy robotovi, aby součástky uchopil.

Neexistence tohoto zpracování dat by průmyslovému robotovi bránila v tom, aby uchopoval součástky, a tudíž by nemohl vykonávat jednu ze svých funkcí. Kromě toho software, který běží na této infrastruktuře, navrhl a vyvinul sám výrobce. Software navržený a vyvinutý výrobcem splňuje definici řešení pro zpracování dat na dálku.

Výrobce průmyslového robota musí v technické dokumentaci k produktu s digitálními prvky zdokumentovat řešení pro zpracování dat na dálku i využívání služeb IaaS třetí strany (včetně podrobností o sjednané službě). Výrobce též musí tyto prvky zohlednit v posouzení rizik, které zahrnuje zamýšlený účel a rozumně předvídatelné použití produktu s digitálními prvky. Výrobce na základě rizik uplatňuje základní požadavky stanovené v aktu na produkt s digitálními prvky, včetně jeho řešení pro zpracování dat na dálku. Plnění povinností výrobce podpoří též náležitá péče při výběru poskytovatele IaaS. Výrobce by například mohl požadovat doklad o splnění povinností podle směrnice NIS 2.

8.3.5 *Mobilní síť*

Chytrý telefon využívá síť 5G k tomu, aby svým uživatelům poskytoval připojení k internetu, telefonní hovory a zprávy (mobilní konektivita). Mobilní síť vyvíjejí a navrhují telekomunikační operátoři. Síť se skládá z malých buněk, vysílačů a dalších síťových zařízení.

Produkt s digitálními prvky by měl být schopen se správně připojit k síti; to je jedna z jeho funkcí. To, zda je tato síť v provozu, či nikoli, však není pro zjištění správné funkce produktu s digitálními prvky relevantní. Síť je pouze komunikační kanál a není nezbytná k tomu, aby produkt s digitálními prvky vykonával svou funkci „správného připojení k síti“. Podobně ethernetový kabel, směrovač nebo signál Wi-Fi nejsou považovány za zpracování dat, jehož neexistence by bránila produktu s digitálními prvky v plnění jedné z jeho funkcí, ale spíše za prostředek umožňující komunikaci/konektivitu.

V důsledku toho mobilní síť nesplňuje definici řešení pro zpracování dat na dálku. Síť by neměla být považována za komponentu třetí strany, jelikož do produktu s digitálními prvky není začleněn žádný software, produkt se místo toho o tuto síť pouze opírá. Z tohoto důvodu není nutné, aby výrobce vykonával povinnosti náležité péče vůči provozovateli sítě.

9. **DALŠÍ PRVKY**

9.1 **Povinnosti podávat zprávy**

209. Podle čl. 14 odst. 1 a 3 aktu je výrobce povinen oznámit současně týmu CSIRT určenému jako koordinátor a agentuře ENISA i) každou aktivně zneužívanou zranitelnost obsaženou v produktu s digitálními prvky, o níž se dozví, a ii) každý závažný incident, který má dopad na bezpečnost produktu s digitálními prvky, o němž se dozví.

210. V souladu s čl. 69 odst. 3 a čl. 71 odst. 2 druhou větou se povinnost dodržovat článek 14 vztahuje od 11. září 2026 na všechny produkty s digitálními prvky spadající do oblasti působnosti aktu, včetně produktů s digitálními prvky, které byly uvedeny na trh před 11. prosincem 2027. Navíc, na rozdíl od povinností týkajících se řešení zranitelností, které trvají pouze po dobu podpory pro daný produkt, povinnosti podávat zprávy zůstávají v platnosti i poté, co produkt s digitálními prvky již není podporován. Pokud byl produkt s digitálními prvky uveden na trh před 11. prosincem 2027 nebo pokud jeho doba podpory již uplynula, není výrobce povinen plnit povinnosti týkající se řešení zranitelností stanovené v části II přílohy I.

211. Je třeba připomenout, že povinnost oznámit takové události se uplatňuje v okamžiku, kdy se výrobce dozví, že je zranitelnost aktivně zneužívána nebo že došlo k závažnému incidentu, který vedl k narušení bezpečnosti jeho produktu s digitálními prvky. Pokyny k tomu, kdy se má za to, že se výrobce o dané skutečnosti dozvěděl, by proto měly výrobcům pomoci určit okamžik, kdy začínají příslušné lhůty pro podávání zpráv.

212. Na výrobce se mohou vztahovat srovnatelné povinnosti podávat zprávy vyplývající z různých aktů EU. Aby byl zajištěn jednotný výklad pojmu „dozví se“ a aby výrobci mohli snadněji plnit tyto povinnosti, jsou tyto pokyny v souladu s 31. bodem odůvodnění prováděcího nařízení Komise (EU) 2024/2690 a oddílem II(A) pokynů 9/2022 k ohlašování případů porušení zabezpečení osobních údajů podle obecného nařízení o ochraně osobních údajů.

213. V některých případech výrobce sám odhalí podezřelou událost nebo ho na potenciální incident či zranitelnost upozorní třetí strana, například fyzická osoba, zákazník, subjekt, orgán, mediální organizace či jiný zdroj. V takových případech by měl výrobce podezřelou událost neprodleně posoudit, aby určil, zda se jedná o aktivně zneužívanou zranitelnost nebo o závažný incident s dopadem na bezpečnost produktu s digitálními prvky. Má se tedy za to, že se výrobce o této skutečnosti dozvěděl v okamžiku, kdy po takovém počátečním posouzení získal přiměřenou míru jistoty, že: i) je zranitelnost obsažená v jeho produktu s digitálními prvky aktivně zneužívána nebo ii) došlo k závažnému incidentu, který vedl k narušení bezpečnosti jeho produktu s digitálními prvky.

214. Okamžik, od kterého lze předpokládat, že se výrobce o této skutečnosti dozvěděl, bude proto záviset na okolnostech konkrétní aktivně zneužívané zranitelnosti nebo závažného incidentu. V některých případech bude již od samého počátku relativně zřejmé, že je určitá zranitelnost aktivně zneužívána nebo že závažný incident má dopad na bezpečnost produktu s digitálními prvky. V jiných případech může chvíli trvat, než se zjistí, zda je produkt s digitálními prvky dotčen zranitelností a zda je tato zranitelnost zneužívána škodlivým aktérem nebo zda má incident dopad na bezpečnost produktu s digitálními prvky. Důraz by však měl být kladen na neprodlené provedení počátečního posouzení s cílem určit, zda jsou tyto podmínky skutečně splněny, zejména v případech, kdy by tato zranitelnost mohla představovat významné riziko, a pokud ano, přijmout nápravná opatření a informovat o tom v souladu s aktem.

215. Dále struktura povinností podávat zprávy vyžaduje, aby výrobci svá oznámení průběžně aktualizovali v závislosti na postupu svých interních vyšetřování a na tom, jak se jejich znalosti o aktivně zneužívané zranitelnosti či incidentu prohlubují. Výrobci jsou zejména povinni bez zbytečného odkladu, nejpozději však do 24 hodin od zjištění skutečnosti, předložit včasné varování obsahující omezené informace. V rámci oznámení jsou následně vyžadovány doplňující informace, které je třeba předložit bez zbytečného odkladu a v každém případě do 72 hodin od okamžiku, kdy se o dané skutečnosti dozví („oznámení do 72 hodin“). Úplná zpráva musí být předložena do 14 dnů od okamžiku, kdy začalo být u aktivně zneužívané zranitelnosti k dispozici nápravné nebo zmírňující opatření, nebo do jednoho měsíce od oznámení do 72 hodin v případě závažných incidentů.

216. Jak bylo rovněž připomenuto v oddíle *3.3.1 Dlouhodobá podpora a zajištění životaschopnosti svobodného softwaru* s otevřeným zdrojovým kódem, aktivně zneužívané zranitelnosti musí v souladu s čl. 24 odst. 3 oznámit i správci softwaru s otevřeným zdrojovým kódem ([30]). Tato povinnost vzniká v okamžiku, kdy se subjekt dozví o aktivně zneužívané zranitelnosti, a nikoli pouze v případě, že zranitelnost existuje v kódové základně svobodného softwaru s otevřeným zdrojovým kódem, jehož správcem tento subjekt je. Jelikož jsou komponenty svobodného softwaru s otevřeným zdrojovým kódem obvykle následně začleňovány do dalších produktů s digitálními prvky, v praxi se správce pravděpodobně dozví o aktivním zneužívání ze zpráv od třetích stran, které zjistí zneužívání komponent svobodného softwaru s otevřeným zdrojovým kódem začleněných do jiných produktů s digitálními prvky. To může být například případ, kdy výrobce produktu s digitálními prvky zjistí aktivní zneužívání v komponentě svobodného softwaru s otevřeným zdrojovým kódem, která je začleněna do jeho vlastního produktu, a oznámí to správci této komponenty; nebo když uživatel či bezpečnostní výzkumník objeví důkazy o zneužívání komponenty svobodného softwaru s otevřeným zdrojovým kódem začleněné do produktu s digitálními prvky a oznámí toto aktivní zneužívání správci této komponenty.

217. Je rovněž třeba upřesnit, že jelikož se povinnost oznamovat aktivně zneužívané zranitelnosti uplatňuje v okamžiku, kdy se výrobce o aktivním zneužívání dozví, není výrobce povinen oznamovat zranitelnosti, o jejichž aktivním zneužívání se dozvěděl již před 11. zářím 2026 (datum, od kterého začíná platit povinnost podávat zprávy). Akt proto nevyžaduje zpětné oznamování takových zranitelností. Naproti tomu tato povinnost platí v případě, že si výrobce byl vědom této zranitelnosti již před 11. zářím 2026, avšak v té době neměl informace o tom, že by byla aktivně zneužívána (ať už proto, že k tomu dosud nedošlo, nebo proto, že se o tom výrobce nedozvěděl). Pokud po 11. září 2026 dojde k aktivnímu zneužívání této zranitelnosti nebo se o něm výrobce dozví, považuje se tato zranitelnost za aktivně zneužívanou a podléhá povinnosti podat o ní zprávu.

218. Podobně je výrobce povinen oznámit pouze aktivně zneužívané zranitelnosti obsažené v jeho produktu s digitálními prvky. Pokud produkt s digitálními prvky obsahuje aktivně zneužívanou zranitelnost pocházející z komponenty třetí strany, je výrobce tohoto produktu s digitálními prvky povinen tuto aktivně zneužívanou zranitelnost oznámit. Pokud si však výrobce je vědom toho, že komponenta třetí strany obsahuje zranitelnost, ale tato zranitelnost buď i) nemůže být zneužita v jeho produktu s digitálními prvky (např. proto, že k zranitelnému kódu není přístup), nebo ii) nebyla v jeho produktu s digitálními prvky zneužita, nepovažuje se tato zranitelnost za aktivně zneužívanou zranitelnost obsaženou v jeho produktu s digitálními prvky, a tudíž se na tohoto výrobce povinnost podat zprávu nevztahuje. Tento výrobce může i přesto oznámit tuto zranitelnost v souladu s článkem 15 aktu dobrovolně. Je rovněž nutné dodržovat požadavky na řešení zranitelností uvedené v části II přílohy I aktu a nahlásit zranitelnost osobě nebo subjektu, který danou komponentu vyrábí nebo provádí její údržbu, v souladu s čl. 13 odst. 6, jak je dále vysvětleno v oddíle *9.2.1 Podávání zpráv výše v řetězci a* sdílení bezpečnostních oprav.

([30]) Pokud se správce podílí na vývoji produktu s digitálními prvky.

219. Jakmile se výrobci dozvědí o aktivně zneužívané zranitelnosti nebo závažném incidentu, jsou rovněž povinni v souladu s čl. 14 odst. 8 informovat dotčené uživatele a případně všechny uživatele. Pokud tak neučiní včas, mohou týmy CSIRT, které oznámení obdržely, tyto informace uživatelům poskytnout, je-li to považováno za přiměřené a nezbytné k předejití nebo zmírnění dopadu této zranitelnosti či incidentu.

220. V souladu s přístupem aktu založeným na riziku je třeba povinnost informovat uživatele stanovenou v čl. 14 odst. 8 uplatňovat způsobem založeným na riziku a přiměřeně. Zejména poskytnutí informací o aktivně zneužívané zranitelnosti nebo závažném incidentu neznamená, že tyto informace musí být zveřejněny nebo sděleny bez rozdílu. V případě potřeby a s ohledem na povahu produktu s digitálními prvky, dotčené uživatele a potenciální dopad zranitelnosti či incidentu mohou výrobci omezit sdělení podrobných informací pouze na příslušné dotčené uživatele nebo zákazníky. To platí zejména pro produkty s digitálními prvky, které se používají v citlivých nebo klíčových prostředích, kde by samotné zveřejnění technických podrobností mohlo zvýšit kybernetická bezpečnostní rizika nebo usnadnit další zneužívání.

221. Jakmile bude tato zranitelnost patřičně vyřešena nebo její dopad bude zmírněn, může být vhodné ji zveřejnit v širším měřítku. To by platilo například v případě, kdy zveřejnění přispívá ke zvýšení obecného povědomí nebo umožňuje uživatelům ověřit si, že jejich produkty s digitálními prvky již nejsou dotčeny. V takových případech by míra podrobnosti a načasování případného širšího zveřejnění měly zůstat přiměřené a měly by zohledňovat zbytková rizika zneužití, povahu produktu s digitálními prvky a zájmy dotčených uživatelů. Kromě toho bod 4 části II přílohy I ukládá výrobcům povinnost zveřejnit informace o opravených zranitelnostech, jakmile bude k dispozici bezpečnostní aktualizace.

9.2 **Řešení zranitelností**

9.2.1 *Podávání zpráv výše v řetězci a sdílení bezpečnostních oprav*

222. Ustanovení čl. 13 odst. 6 aktu ukládá výrobcům povinnost oznámit zranitelnosti v začleněných komponentách osobě nebo subjektu, který danou komponentu vyrábí nebo provádí její údržbu („podávání zpráv výše v řetězci“).

223. Výrobci jsou povinni podávat zprávy výše v řetězci pouze v případě té verze komponenty, kterou začleňují. Pokud osoba nebo subjekt, který danou komponentu vyrábí nebo provádí její údržbu, zavedl bezpečnostní politiky, koordinované postupy pro zveřejňování zranitelností nebo určil kanály pro oznamování zranitelností, měli by výrobci podávat zprávy v souladu s nimi, zejména v případech, kdy by předčasné zveřejnění neopravených zranitelností mohlo zvýšit kybernetická bezpečnostní rizika. Dále s cílem snížit zátěž pro ty výše v řetězci, kdo provádějí údržbu, zejména v rámci projektů s otevřeným zdrojovým kódem, nejsou výrobci povinni podávat zprávy výše v řetězci v případech, kdy mohou potvrdit, že osoba nebo subjekt, který danou komponentu vyrábí nebo provádí její údržbu, si je existence této zranitelnosti vědom. Výrobci jsou vybízeni, aby podnikli přiměřené kroky a zamezili podávání duplicitních zpráv, například tím, že před podáním zprávy výše v řetězci zkontrolují veřejně přístupné databáze zranitelností, bezpečnostní doporučení týkající se konkrétních projektů nebo zavedené systémy pro sledování problémů.

224. Výrobci jsou povinni oznamovat výše v řetězci pouze ty zranitelnosti, které se vyskytují v samotné začleněné komponentě, nikoli však zranitelnosti, které existují v důsledku propojení této komponenty s jiným kódem vyvinutým výrobcem nebo v důsledku začlenění jiných komponent. Přesto však mohou nastat situace, kdy začlenění komponenty do konkrétního produktu s digitálními prvky odhalí určité chování, interakce nebo bezpečnostní charakteristiky této komponenty, které nebyly zřejmé nebo nebyly snadno identifikovatelné, když byla komponenta používána samostatně. V takových případech jsou výrobci vybízeni, aby tyto informace sdělili osobě nebo subjektu, který danou komponentu vyrábí nebo provádí její údržbu, a to s cílem podpořit osvědčené postupy řešení zranitelností, jejichž cílem je usnadnit účinnou nápravu a zlepšit celkovou bezpečnost ekosystému dané komponenty.

225. A konečně, výrobci také nejsou povinni oznámit tuto zranitelnost výše v řetězci, pokud danou komponentu již nikdo neudržuje, nebo pokud se výrobce v nových verzích či bezpečnostních opravách již nespoléhá na toho, kdo údržbu prováděl původně. V takových případech je výrobce nicméně vybízen, aby uživatele dané komponenty informoval pomocí přiměřených alternativních opatření, např. prostřednictvím stávajících komunitních mechanismů (jako jsou seznamy pro rozesílání informací nebo hlášení problémů) nebo prostřednictvím veřejných záznamů o zranitelnostech.

226. Dále podle čl. 13 odst. 6 jsou výrobci, kteří vyvinuli softwarovou úpravu k řešení zranitelnosti v začleněné komponentě, povinni tuto softwarovou úpravu („bezpečnostní opravu“) sdílet s osobou nebo subjektem, který danou komponentu vyrábí nebo provádí její údržbu („sdílení v řetězci směrem nahoru“).

227. V případech, kdy jsou výrobci povinni sdílet bezpečnostní opravu podle čl. 13 odst. 6, měla by být tato oprava v příslušných případech poskytnuta ve strojově čitelném formátu a způsobem, který osobě nebo subjektu, který danou komponentu vyrábí nebo provádí její údržbu, umožňuje opravu snadno ověřit a v příslušných případech začlenit. Je-li daná komponenta svobodná a má otevřený zdrojový kód, měla by být bezpečnostní oprava sdílena způsobem, který je slučitelný s licencí této komponenty, například jejím sdílením pod stejnou licencí nebo pod licencí, která tomu, kdo provádí údržbu, umožňuje distribuovat opravu pod vlastní licencí. Pokud ten, kdo danou komponentu udržuje, stanovil pokyny ohledně sdílení bezpečnostních oprav, měl by se výrobce těmito pokyny řídit.

228. Akt však od výrobců nevyžaduje, aby zajistili, že jejich bezpečnostní opravy osoba nebo subjekt, který danou komponentu vyrábí nebo provádí její údržbu, skutečně přijmou. Rovněž nejsou povinni zajistit, aby byly tyto opravy nutně začleněny do úložiště kódů dané komponenty, například v případě, že ten, kdo provádí údržbu, upřednostňuje jinou možnost řešení daného problému. Stejně tak výrobci nejsou povinni přijmout navrhovanou opravu vyvinutou tím, kdo provádí údržbu komponenty, a mohou upřednostnit zmírnění problému jinými vhodnými způsoby.

229. V některých případech osoba nebo subjekt, který danou komponentu vyrábí nebo provádí její údržbu, bezpečnostní opravu k řešení této zranitelnosti možná již poskytly, avšak výrobce zavede odlišnou zmírňující strategii (například změnou jiné konfigurace). V takových případech akt nevyžaduje, aby výrobce sdílel změnu jiné části systému výše v řetězci. Výrobce je nicméně vybízen, aby tak učinil, pokud to může podpořit osobu nebo subjekt, který provádí údržbu komponenty.

9.2.2 *Známé zneužitelné zranitelnosti*

230. Jeden ze základních požadavků části I přílohy I aktu stanoví, že na základě posouzení kybernetického bezpečnostního rizika podle čl. 13 odst. 2 musí být v příslušných případech produkty s digitálními prvky dodávány na trh bez známých zneužitelných zranitelností.

231. Ustanovení čl. 3 bodu 41 definuje „zneužitelnou zranitelnost“ jako „zranitelnost, která může být za praktických provozních podmínek účinně zneužita nepřátelským subjektem“. Ne všechny zranitelnosti lze zneužít v reálných provozních podmínkách a některé zranitelnosti lze zneužít pouze za teoretických podmínek (např. v laboratoři nebo v simulaci) a/nebo nikoli za podmínek, které by nastaly v provozním prostředí produktu s digitálními prvky.

232. Akt požaduje, aby výrobci měli vhodnou politiku a postupy pro řešení a nápravu možných zranitelností hlášených z interních nebo externích zdrojů (čl. 13 odst. 8). Neuvádí však výslovně, kdy by měla být zneužitelná zranitelnost považována za známou výrobci, čímž by vznikla povinnost splnit tento základní požadavek již v okamžiku uvedení na trh.

233. Zranitelnost by měla být považována za známou, pokud je uvedena v příslušných veřejně přístupných databázích zranitelností, jako je například Evropská databáze zranitelností zřízená podle čl. 12 odst. 2 směrnice (EU) 2022/2555 nebo jiné významné databáze zranitelností.

234. Zranitelnost může být navíc známa i v případě, že o ní byl výrobce informován prostřednictvím neveřejných informací, například v rámci koordinovaného zveřejnění ze strany bezpečnostního výzkumníka nebo na základě vlastních interních zkoušek a analýz výrobce, včetně například využití služeb založených na umělé inteligenci. Stejně tak lze o zranitelnosti hovořit jako o známé, pokud o ní veřejně a se zdůrazněním informovala spolehlivá média, včetně odborných publikací zabývajících se kybernetickou bezpečností či obecně zaměřených sdělovacích prostředků.

235. Nicméně pouhá skutečnost, že byla oznámena nebo zjištěna zranitelnost, sama o sobě neznamená, že je v praxi zneužitelná nebo že se týká konkrétního dotčeného produktu s digitálními prvky. Výrobce ji bude muset prošetřit a potvrdit pravdivost těchto informací a to, zda se zranitelnost týká jeho vlastního produktu s digitálními prvky. Na základě toho může mezi prvním oznámením této zranitelnosti a jejím potvrzením uplynout omezená doba. Jak je uvedeno v oddíle *9.1 Povinnosti podávat* zprávy, je třeba klást důraz na rychlé kroky k prošetření a reakci.

236. Dále se povinnost výrobců dodržovat základní požadavky stanovené v části I přílohy I uplatňuje v souladu s čl. 13 odst. 1 v okamžiku uvedení na trh. V praxi se může stát, že nové potenciálně zneužitelné zranitelnosti budou odhaleny v závěrečných fázích vývojového cyklu produktu s digitálními prvky, a to i krátce předtím, než se tento produkt dostane do distribučního řetězce (a bude tedy uveden na trh).

237. Jelikož povinnost uvádět na trh produkt s digitálními prvky bez známých zneužitelných zranitelností je povinností založenou na riziku, je na výrobci, aby na základě posouzení kybernetických bezpečnostních rizik určil, zda lze produkt s digitálními prvky bezpečně uvést na trh v souladu s aktem. Případně může výrobce určit, že je nutné nově zjištěnou zranitelnost odstranit dříve, než bude možné uvést produkt s digitálními prvky na trh. Při tomto určování by výrobci měli zohlednit závažnost, zneužitelnost a potenciální dopad dané zranitelnosti, jakož i rizika, která pro samotný produkt s digitálními prvky vznikají při jeho používání. Mohou také zohlednit rizika spojená s odložením vydání produktu do doby, než bude zranitelnost opravena, například z toho důvodu, že nové vydání řeší i další zneužitelné zranitelnosti nebo je nezbytné pro pokračující provoz kritických systémů. V každém případě platí, že jakmile je produkt s digitálními prvky uveden na trh, výrobce zůstává povinen řešit zranitelnosti účinně a v souladu s požadavky na řešení zranitelností stanovenými v části II přílohy I.

9.2.3 *Účinné a pravidelné testy a přezkumy*

238. Bod 3 části II přílohy I ukládá výrobcům povinnost provádět po celou dobu podpory produktu s digitálními prvky jeho účinné a pravidelné testy a přezkumy. Provádění pravidelných testů nevyžaduje mechanické opakování nezměněné testovací série v pevně stanovených intervalech. To znamená pravidelně přezkoumávat, zda nový vstup, jako jsou nově zjištěné hrozby nebo nově objevené zranitelnosti, nevyžaduje aktualizaci stávajících testů, a podle toho tyto testy provádět.

239. Četnost, hloubka a obsah přezkumu by měly být přiměřené profilu kybernetických bezpečnostních rizik produktu s digitálními prvky, jeho vývoji v čase a stavu prostředí hrozeb. Pokud přezkum zjistí relevantní nový vstup, který má vliv na testovací sadu, je třeba navrhnout a provést na produktu nové nebo upravené testy, aby se zajistilo, že žádné zranitelnosti nezůstanou neřešeny. To může zahrnovat opakované provedení stávajících testů v případech, kdy je to vzhledem ke změně produktu s digitálními prvky vhodné, například v případě regresních testů.

240. Pokud přezkum nezjistí žádný takový vstup, není nutné navrhovat další testy. Souběžně s tím platí i další povinnosti týkající se řešení zranitelností, včetně povinnosti řešit a napravovat zranitelnosti s ohledem na rizika, která představují.

9.3 **Vzájemný vztah s ostatními právními předpisy**

9.3.1 *Nařízení (EU) 2019/2144 a nařízení (EU) č. 168/2013*

241. V čl. 2 odst. 2 písm. c) aktu se stanoví, že se toto nařízení nevztahuje na produkty s digitálními prvky, na které se vztahuje nařízení (EU) 2019/2144. Nařízení (EU) 2019/2144 se vztahuje na „vozidla kategorií M, N a O ve smyslu článku 4 nařízení (EU) 2018/858 a na systémy, konstrukční části a samostatné technické celky pro taková vozidla navržené a vyrobené“.

242. Podobně byly z působnosti aktu na základě nařízení Komise v přenesené pravomoci (EU) 2025/1535 vyňaty i produkty s digitálními prvky, které spadají do oblasti působnosti nařízení (EU) č. 168/2013. Nařízení (EU) č. 168/2013 se vztahuje na vozidla kategorie L a „na systémy, konstrukční části a samostatné technické celky, jakož i díly a zařízení, zkonstruované a vyrobené pro taková vozidla“ (čl. 2 odst. 1).

243. Na vozidla, na která se vztahují tato nařízení, se akt nevztahuje. Dále je třeba vyjasnit rozsah výjimky pro systémy, konstrukční části, samostatné technické celky, díly a zařízení (v tomto oddíle dále jen „komponenty“), jež jsou zkonstruovány a vyrobeny pro taková vozidla a považují se za produkty s digitálními prvky ve smyslu aktu.

244. Má se za to, že na takové komponenty se akt nevztahuje, pokud jsou zkonstruovány a vyrobeny výlučně za účelem začlenění do vozidel, na která se vztahují nařízení (EU) 2019/2144 a č. 168/2013. To platí bez ohledu na to, zda danou komponentu její výrobce prodává přímo výrobci vozidel nebo jinému hospodářskému subjektu v dodavatelském řetězci automobilového průmyslu, pokud je tato komponenta jednoznačně určena a je vhodná pouze pro konečné začlenění do těchto vozidel.

245. Naproti tomu výrobce, který prodává generické komponenty, tj. produkty s digitálními prvky, které lze začlenit do různých typů produktů, a nikoli výlučně do vozidel, na něž se tato nařízení vztahují, aktu podléhá.

246. Posouzení, zda je komponenta uvedena na trh ve smyslu aktu, musí vycházet z objektivních podmínek, za nichž je dodávána na trh. Pokud výrobce nabízí komponentu, která není vhodná výlučně ke konečnému začlenění do těchto vozidel, prostřednictvím distribučních kanálů přístupných zákazníkům mimo dodavatelský řetězec automobilového průmyslu, jako jsou běžné maloobchodní prodejny nebo internetové prodejní kanály přijímající objednávky od široké veřejnosti, spadá tato komponenta do oblasti působnosti aktu bez ohledu na jakákoli prohlášení týkající se jejího zamýšleného použití. Za těchto okolností nelze danou komponentu považovat za komponentu zkonstruovanou a vyrobenou výlučně pro začlenění do vozidel, na která se vztahují nařízení (EU) 2019/2144 a č. 168/2013, a výrobce je povinen dodržovat akt. Naproti tomu využití omezených distribučních kanálů mezi jednotlivými podniky určených pouze pro dodavatelský řetězec v automobilovém průmyslu může naznačovat, že je zkonstruována a vyrobena výhradně pro takové začlenění.

9.3.2 *Platnost certifikátů EU přezkoušení typu (čl. 69 odst. 1)*

247. Ustanovení čl. 69 odst. 1 aktu uvádí, že „[c]ertifikáty EU přezkoušení typu a rozhodnutí o schválení vydané v souvislosti s požadavky na kybernetickou bezpečnost produktů s digitálními prvky, které podléhají jiným harmonizačním právním předpisům Unie než tomuto nařízení, zůstávají v platnosti do 11. června 2028, pokud jejich platnost neskončí před tímto datem nebo pokud není stanoveno jinak v těchto jiných harmonizačních právních předpisech Unie, přičemž v takovém případě zůstávají v platnosti podle uvedených právních předpisů“.

248. Pokračující platnost těchto certifikátů a rozhodnutí o schválení je třeba chápat jako omezenou na kybernetická bezpečnostní rizika a odpovídající požadavky, na které se vztahují příslušné harmonizační právní předpisy Unie, na jejichž základě byly vydány. V případě těchto rizik nejsou výrobci povinni provádět nové posouzení ani znovu prokazovat shodu výhradně pro účely aktu během období platnosti uvedeného v čl. 69 odst. 1 u produktů s digitálními prvky, které hodlají uvést na trh dne 11. prosince 2027 nebo později a do 11. června 2028 ([31]). To platí pro certifikáty a rozhodnutí o schválení vydaná v případech, kdy příslušné harmonizační právní předpisy Unie vyžadují, aby výrobce provedl postup posuzování shody prostřednictvím oznámeného subjektu, jakož i v případech, kdy se výrobce pro tento postup rozhodl dobrovolně.

249. V souladu s tím existence platného certifikátu nebo rozhodnutí o schválení podle jiných harmonizačních právních předpisů Unie nezbavuje výrobce povinnosti provést komplexní posouzení kybernetických bezpečnostních rizik podle aktu (ani jiných povinností z něj vyplývajících). Místo toho jim umožňuje opírat se o stávající certifikace jako o důkaz o splnění požadavků v rámci jejich postupu posuzování shody, a to v rozsahu, v jakém jsou příslušná kybernetická bezpečnostní rizika již pokryta. Pokud má certifikát nebo rozhodnutí o schválení platnost podle jiných harmonizačních právních předpisů Unie i po 11. červnu 2028, může se výrobce pro účely aktu na takový certifikát nebo rozhodnutí odvolávat pouze do 11. června 2028.

250. Pokud posouzení kybernetických bezpečnostních rizik provedené v souladu s čl. 13 odst. 2 zjistí další rizika, na která se nevztahují požadavky na kybernetickou bezpečnost, z nichž vychází stávající certifikát nebo rozhodnutí o schválení, zůstávají výrobci odpovědnými za řešení těchto rizik v souladu s aktem. V takových případech je z hlediska dodržování předpisů nutné, aby byly zjištěné nedostatky posouzeny a zmírněny, a to bez ohledu na to, zda stávající certifikát či rozhodnutí o schválení zůstávají v platnosti.

251. To lze ilustrovat na příkladu, kdy se na produkt s digitálními prvky vztahují požadavky na kybernetickou bezpečnost stanovené v nařízení Komise v přenesené pravomoci (EU) 2022/30, kterým se doplňuje směrnice 2014/53/EU (akt v přenesené pravomoci podle směrnice o rádiových zařízeních), a kdy byl na základě těchto požadavků vydán certifikát EU přezkoušení typu nebo rozhodnutí o schválení. V takovém případě zůstává certifikát nebo rozhodnutí v platnosti v souladu s čl. 69 odst. 1 pro kybernetická bezpečnostní rizika, na která se tento certifikát vztahuje a která souvisejí se základními požadavky na kybernetickou bezpečnost stanovenými ve směrnici 2014/53/EU (směrnice o rádiových zařízeních).

252. V takových případech nejsou výrobci pro účely aktu povinni znovu posuzovat ani znovu prokazovat soulad s ohledem na ta rizika, která již byla těmito certifikáty řešena, a to po dobu, po kterou zůstává příslušný certifikát nebo rozhodnutí o schválení v platnosti, a v žádném případě déle než do 11. června 2028. Patří sem například kybernetická bezpečnostní rizika, která jsou spojena s ochranou sítí, ochranou osobních údajů a soukromí nebo předcházením podvodům (v rozsahu, v jakém jsou tato rizika zahrnuta v daném certifikátu), která souvisejí s požadavky směrnice o rádiových zařízeních na kybernetickou bezpečnost a která se odrážejí v posouzení shody.

253. Pokud však posouzení kybernetických bezpečnostních rizik provedené v souladu s čl. 13 odst. 2 aktu zjistí další kybernetická bezpečnostní rizika, na která se tyto certifikáty nevztahují, zůstávají výrobci odpovědnými za řešení těchto rizik v souladu s aktem. Může se jednat například o rizika související s procesy řešení zranitelností, minimalizací dat a zmenšením plochy pro útok, případně o další aspekty kybernetické bezpečnosti specifické pro daný produkt, které tyto certifikáty neřeší nebo které v žádném případě nespadají pod základní požadavky na kybernetickou bezpečnost stanovené směrnicí o rádiových zařízeních.

254. V souladu s tím existence platného certifikátu EU přezkoušení typu nebo rozhodnutí o schválení podle směrnice o rádiových zařízeních, pokud jde o její základní požadavky týkající se kybernetické bezpečnosti, sama o sobě neprokazuje plnou shodu s aktem. Místo toho umožňuje výrobcům opírat se o tento certifikát nebo rozhodnutí u příslušných rizik jako o důkaz shody, přičemž výrobci musí zajistit, že veškerá zbývající nebo nově zjištěná rizika budou posouzena a zmírněna v souladu s aktem.

([31]) Produkty s digitálními prvky uvedené na trh před 11. prosincem 2027 podléhají právním předpisům Unie použitelným v době jejich uvedení na trh, a pokud splňovaly příslušné požadavky, mohou být prodávány a uváděny do provozu, ledaže by byly dne 11. prosince 2027 nebo později podrobeny podstatným změnám. Pokud jde o pojmy „uvedení na trh“ a „dodání na trh“, viz také oddíl *2.1 Uvádění na trh* tohoto dokumentu a kapitolu 2 Modré příručky.

255. Podobně platí, že pokud se na produkt s digitálními prvky vztahují základní požadavky na bezpečnost a ochranu zdraví v souvislosti s kybernetickou bezpečností stanovené v nařízení (EU) 2023/1230 (nařízení o strojních zařízeních), které je plně použitelné od 20. ledna 2027, a pokud byl na základě těchto požadavků vydán certifikát EU přezkoušení typu nebo rozhodnutí o schválení, zůstává tento certifikát nebo rozhodnutí o schválení v souladu s čl. 69 odst. 1 aktu v platnosti pro kybernetická bezpečnostní rizika, na něž se vztahuje nařízení o strojních zařízeních.

256. Jedná se zejména o aspekty kybernetické bezpečnosti související s ochranou před poškozením a s bezpečností a spolehlivostí ovládacích systémů, jak je stanoveno v oddílech 1.1.9 a 1.2.1 přílohy III nařízení o strojních zařízeních. U těchto rizik nejsou výrobci pro účely aktu povinni znovu posuzovat ani znovu prokazovat soulad po dobu, po kterou zůstává příslušný certifikát nebo rozhodnutí o schválení v platnosti, a v žádném případě déle než do 11. června 2028. To platí v rozsahu, v jakém tato rizika byla zohledněna v rámci posouzení shody podle nařízení o strojních zařízeních.

257. Stejně jako v případě výše zmíněných základních požadavků na kybernetickou bezpečnost podle směrnice o rádiových zařízeních platí, že pokud posouzení kybernetických bezpečnostních rizik provedené v souladu s čl. 13 odst. 2 aktu zjistí další kybernetická bezpečnostní rizika, na která se nevztahuje příslušný certifikát vydaný podle nařízení o strojních zařízeních a která souvisejí s požadavky na kybernetickou bezpečnost uvedeného nařízení, zůstávají výrobci odpovědnými za řešení těchto rizik v souladu s aktem.