2024/2847

20.11.2024

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)

(Text s významem pro EHP)

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

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

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

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

po konzultaci s Výborem regionů,

v souladu s řádným legislativním postupem ([2]),

vzhledem k těmto důvodům:

(1) Kybernetická bezpečnost je pro Unii jednou z klíčových výzev. V nadcházejících letech dojde k exponenciálnímu zvýšení počtu a rozmanitosti připojených zařízení. Kybernetické útoky představují záležitost veřejného zájmu, jelikož mají zásadní dopad nejen na hospodářství Unie, ale i na demokracii, stejně jako na bezpečnost a na zdraví spotřebitelů. Je proto nezbytné zpřísnit přístup Unie ke kybernetické bezpečnosti, zabývat se kybernetickou odolností na úrovni Unie a zlepšit fungování vnitřního trhu stanovením jednotného právního rámce pro základní požadavky na kybernetickou bezpečnost při uvádění produktů s digitálními prvky na trh Unie. Měly by být řešeny dva hlavní problémy, které zvyšují náklady pro uživatele a pro společnost: nízká úroveň kybernetické bezpečnosti produktů s digitálními prvky, která se odráží v rozšířených zranitelnostech a nedostatečném a nekonzistentním poskytování bezpečnostních aktualizací k jejímu řešení, a nedostatečné chápání informací a přístup k nim ze strany uživatelů, což jim znemožňuje vybírat si produkty s odpovídajícími kybernetickými bezpečnostními vlastnostmi nebo je používat bezpečným způsobem.

(2) Cílem tohoto nařízení je stanovit mezní podmínky pro vývoj bezpečných produktů s digitálními prvky tím, že bude zajištěno, aby hardwarové a softwarové produkty byly uváděny na trh s menším počtem zranitelností a aby výrobci brali bezpečnost vážně v průběhu celého životního cyklu produktu. Má rovněž vytvořit podmínky umožňující uživatelům, aby při výběru a používání produktů s digitálními prvky zohledňovali kybernetickou bezpečnost, například zajištěním větší transparentnosti, pokud jde o dobu podpory produktů s digitálními prvky dodávaných na trh.

(3) Příslušné platné právo Unie, zahrnuje několik souborů horizontálních pravidel, která se z různých úhlů zabývají určitými aspekty souvisejícími s kybernetickou bezpečností, včetně opatření ke zlepšení bezpečnosti digitálního dodavatelského řetězce. Stávající právo Unie týkající se kybernetické bezpečnosti, včetně nařízení Evropského parlamentu a Rady (EU) 2019/881 ([3]) a směrnice Evropského parlamentu a Rady (EU) 2022/2555 ([4]), však přímo nezahrnuje povinné požadavky na bezpečnost produktů s digitálními prvky.

([1]) Úř. věst. C 100, 16.3.2023, s. 101.
([2]) Postoj Evropského parlamentu ze dne 12. března 2024 (dosud nezveřejněný v Úředním věstníku) a rozhodnutí Rady ze dne 10. října 2024.
([3]) Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) (Úř. věst. L 151, 7.6.2019, s. 15).
([4]) Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2) (Úř. věst. L 333, 27.12.2022, s. 80).

(4) Ačkoli se stávající právo Unie vztahuje na určité produkty s digitálními prvky, neexistuje žádný horizontální regulační rámec Unie, který by stanovil komplexní požadavky na kybernetickou bezpečnost pro všechny produkty s digitálními prvky. Různé akty a iniciativy, které byly dosud přijaty na úrovni Unie a na vnitrostátní úrovni, řeší zjištěné problémy a rizika související s kybernetickou bezpečností pouze částečně, vytvářejí v rámci vnitřního trhu právní nejednotnost, zvyšují právní nejistotu pro výrobce i pro uživatele těchto produktů a vytváří zbytečnou zátěž pro podniky a organizace, pokud jde o plnění řady požadavků a povinností souvisejících s podobnými druhy produktů. Kybernetická bezpečnost těchto produktů má obzvláště silný přeshraniční rozměr, neboť produkty s digitálními prvky vyrobené v jednom členském státě nebo třetí zemi často používají organizace a spotřebitelé na celém vnitřním trhu. Proto je nezbytné regulovat tuto oblast na úrovni Unie s cílem zajistit harmonizovaný regulační rámec a právní jistotu pro uživatele, organizace a podniky, včetně mikropodniků a malých a středních podniků, jak jsou definovány v příloze doporučení Komise 2003/361/ES ([5]). Regulační prostředí Unie by mělo být harmonizováno zavedením horizontálních požadavků na kybernetickou bezpečnost produktů s digitálními prvky. Kromě toho by měla být v celé Unii zajištěna právní jistota pro hospodářské subjekty a uživatele, jakož i lepší harmonizace vnitřního trhu a proporcionalita pro mikropodniky a malé a střední podniky, přičemž pro hospodářské subjekty, které chtějí na tento trh vstoupit, by se tím vytvořily přijatelnější podmínky.

(5) Pokud jde o mikropodniky a malé a střední podniky, měla by se při určování kategorie, do níž daný podnik spadá, použít ustanovení přílohy doporučení 2003/361/ES v plném rozsahu. Proto by se při kalkulaci počtu zaměstnanců a finančních prahů vymezujících kategorie podniků měla použít rovněž ustanovení článku 6 přílohy doporučení 2003/361/ES týkající se stanovení údajů o podniku s ohledem na konkrétní typy podniků, jako jsou partnerské podniky nebo propojené podniky.

(6) Komise by měla hospodářským subjektům, zejména mikropodnikům a malým a středním podnikům, pomoci při uplatňování tohoto nařízení tím, že vydá příslušné pokyny. Tyto pokyny by se měly mimo jiné týkat oblasti působnosti tohoto nařízení, zejména pokud jde o zpracování dat na dálku a jeho důsledky pro vývojáře svobodného softwaru s otevřeným zdrojovým kódem, o uplatňování kritérií používaných ke stanovení doby podpory u produktů s digitálními prvky, o vzájemnou provázanost tohoto nařízení s jiným právem Unie a o konceptu podstatné změny.

(7) Na úrovni Unie se v různých programových a politických dokumentech, například ve společném sdělení Komise a vysokého představitele Unie pro zahraniční věci a bezpečnostní politiku ze dne 16. prosince 2020 nazvaném „Strategie kybernetické bezpečnosti EU pro digitální dekádu“, v závěrech Rady ze dne 2. prosince 2020 o kybernetické bezpečnosti zařízení připojených k internetu a ze dne 23. května 2022 o rozvoji kybernetické pozice Evropské unie a v usnesení Evropského parlamentu ze dne 10. června 2021 o strategii kybernetické bezpečnosti EU pro digitální dekádu ([6]), vyzývá k zavedení zvláštních požadavků Unie na kybernetickou bezpečnost digitálních produktů nebo zařízení připojených k internetu, přičemž několik třetích zemí zavedlo opatření k řešení této otázky z vlastního podnětu. V závěrečné zprávě Konference o budoucnosti Evropy občané požadovali „větší roli EU v boji proti hrozbám v oblasti kybernetické bezpečnosti“. Aby mohla Unie v oblasti kybernetické bezpečnosti zaujmout vedoucí postavení na mezinárodní úrovni, je důležité vytvořit ambiciózní zastřešující regulační rámec.

(8) Aby se zvýšila celková úroveň kybernetické bezpečnosti všech produktů s digitálními prvky uváděných na vnitřní trh, je nezbytné zavést pro tyto produkty cílené a technologicky neutrální základní požadavky na kybernetickou bezpečnost, které by byly horizontálně použitelné.

(9) Za určitých podmínek mohou všechny produkty s digitálními prvky začleněné do většího elektronického informačního systému nebo k němu připojené sloužit pro škodlivé aktéry jako vektor útoku. V důsledku toho může i hardware a software, který je považován za méně kritický, usnadnit prvotní narušení zařízení nebo sítě, což umožní škodlivým aktérům získat privilegovaný přístup k systému nebo se pohybovat napříč systémy. Výrobci by proto měli zajistit, aby byly všechny produkty s digitálními prvky navrhovány a vyvíjeny v souladu se základními požadavky na kybernetickou bezpečnost stanovenými tímto nařízením. Tato povinnost se týká produktů, které lze fyzicky připojit prostřednictvím hardwarových rozhraní, i produktů, které jsou připojeny logicky, například prostřednictvím síťových zásuvek, vedení, souborů, rozhraní pro programování aplikací nebo jakýchkoli jiných druhů softwarového rozhraní. Vzhledem k tomu, že kybernetické hrozby se mohou před dosažením určitého cíle šířit prostřednictvím různých produktů s digitálními prvky, například zřetězením zneužití více zranitelností, měli by výrobci zajistit kybernetickou bezpečnost i u těch produktů s digitálními prvky, které jsou připojeny k jiným zařízením nebo sítím pouze nepřímo.

([5]) Doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků (Úř. věst. L 124, 20.5.2003, s. 36).

([6]) Úř. věst. C 67, 8.2.2022, s. 81.

(10) Stanovení požadavků na kybernetickou bezpečnost pro uvádění produktů s digitálními prvky na trh je určeno ke zvýšení kybernetické bezpečnosti těchto produktů pro spotřebitele i pro podniky. Tyto požadavky rovněž zajistí, aby byla kybernetická bezpečnost zohledňována v celém dodavatelském řetězci, díky čemuž budou konečné produkty s digitálními prvky a jejich komponenty bezpečnější. Tyto požadavky na uvádění na trh by měly být stanoveny i v případě spotřebních produktů s digitálními prvky určených pro zranitelné spotřebitele, například hraček a systémů pro monitorování dětí. Spotřebitelské produkty s digitálními prvky, které jsou v tomto nařízení klasifikovány jako důležité produkty s digitálními prvky, představují vyšší kybernetické bezpečnostní riziko, neboť plní funkci, která s sebou nese významné riziko nepříznivých účinků co do intenzity a schopnosti poškodit zdraví nebo ohrozit bezpečnost uživatelů těchto produktů, a měly by tak podléhat přísnějšímu postupu posuzování shody. Patří mezi ně takové produkty, jako jsou produkty pro inteligentní domácnost s bezpečnostními funkcemi, včetně inteligentních dveřních zámků, systémy pro monitorování dětí a poplašné systémy, hračky připojené k internetu a nositelná elektronika používaná ve zdravotnictví. Přísnější postupy posuzování shody, jimž se musejí podrobit ostatní produkty s digitálními prvky, které jsou v tomto nařízení klasifikovány jako důležité nebo kritické produkty s digitálními prvky, navíc přispějí k zabránění možnému negativnímu dopadu zneužívání zranitelností na spotřebitele.

(11) Účelem tohoto nařízení je zajistit vysokou úroveň kybernetické bezpečnosti produktů s digitálními prvky a jejich integrovaná řešení pro zpracování dat na dálku. Tato řešení pro zpracování dat na dálku by měla být definována jako zpracování dat na dálku, pro něž je software navržen a vyvinut výrobcem daného produktu s digitálními prvky nebo jeho jménem, a pokud by neexistoval, nebylo by možné, aby tento produkt s digitálními prvky plnil některou ze svých funkcí. Tento přístup zajišťuje, aby tyto 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. Zpracování nebo uchovávání dat na dálku zároveň spadá do oblasti působnosti tohoto nařízení pouze tehdy, je-li to nezbytné k tomu, aby produkt s digitálními prvky plnil své funkce. O takové zpracování nebo uchovávání dat na dálku se jedná i tehdy, vyžaduje-li mobilní aplikace přístup k rozhraní pro programování aplikací nebo k databázi poskytované prostřednictvím služby vyvinuté výrobcem. V takovém případě spadá tato služba do oblasti působnosti tohoto nařízení jako řešení pro zpracování dat na dálku. 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.

(12) Cloudová řešení představují řešení pro zpracování dat na dálku ve smyslu tohoto nařízení, pouze pokud splňují definici stanovenou v tomto nařízení. Do oblasti působnosti tohoto nařízení spadají například cloudové funkce poskytované výrobcem zařízení pro inteligentní domácnost, které uživateli umožňují ovládat zařízení na dálku. Naopak internetové stránky, které nepodporují funkce produktu s digitálními prvky, nebo cloudové služby, za jejichž koncepci a vývoj nenese odpovědnost výrobce produktu s digitálními prvky, do oblasti působnosti tohoto nařízení nespadají. Na služby cloud computingu a modely cloudových služeb, jako je software jako služba (SaaS), platforma jako služba (PaaS) nebo infrastruktura jako služba (IaaS), se použije směrnice (EU) 2022/2555. Do oblasti působnosti uvedené směrnice spadají subjekty poskytující v Unii služby cloud computingu, které lze podle článku 2 přílohy doporučení 2003/361/ES považovat za střední podniky nebo které překračují stropy pro střední podniky stanovené v odstavci 1 uvedeného článku.

(13) V souladu s cílem tohoto nařízení odstranit překážky bránící volnému pohybu produktů s digitálními prvky, by členské státy neměly v záležitostech, na něž se vztahuje toto nařízení, bránit tomu, aby byly na trh dodávány produkty s digitálními prvky, které jsou v souladu s tímto nařízením. V záležitostech harmonizovaných tímto nařízením proto členské státy nemohou ukládat dodatečné požadavky na kybernetickou bezpečnost týkající se dodávaní produktů s digitálními prvky na trh. Každý veřejný nebo soukromý subjekt však může k požadavkům stanoveným v tomto nařízení stanovit dodatečné požadavky pro zadávání zakázek nebo používání produktů s digitálními prvky pro své konkrétní účely, a může se proto rozhodnout používat produkty s digitálními prvky, které splňují přísnější nebo konkrétnější požadavky na kybernetickou bezpečnost než ty, které se vztahují na dodávání na trh podle tohoto nařízení. Aniž jsou dotčeny směrnice Evropského parlamentu a Rady 2014/24/EU ([7]) a 2014/25/EU ([8]), měly by členské státy při zadávání zakázek na produkty s digitálními prvky, které musejí splňovat základní požadavky na kybernetickou bezpečnost stanovené v tomto nařízení, včetně požadavků týkajících se řešení

([7]) Směrnice Evropského parlamentu a Rady 2014/24/EU ze dne 26. února 2014 o zadávání veřejných zakázek a o zrušení směrnice 2004/18/ES (Úř. věst. L 94, 28.3.2014, s. 65).

([8]) Směrnice Evropského parlamentu a Rady 2014/25/EU ze dne 26. února 2014 o zadávání zakázek subjekty působícími v odvětví vodního hospodářství, energetiky, dopravy a poštovních služeb a o zrušení směrnice 2004/17/ES (Úř. věst. L 94, 28.3.2014, s. 243).

zranitelností, zajistit, aby byly tyto požadavky při zadávání zakázek zohledněny a aby byla zohledněna rovněž schopnost výrobců účinně uplatňovat opatření v oblasti kybernetické bezpečnosti a zvládat kybernetické hrozby. Ve směrnici (EU) 2022/2555 jsou dále stanovena opatření k řízení kybernetických bezpečnostních rizik pro základní a důležité subjekty podle článku 3 uvedené směrnice, která by mohla zahrnovat opatření v oblasti bezpečnosti dodavatelského řetězce, jež vyžadují, aby tyto subjekty používaly produkty s digitálními prvky, které splňují přísnější požadavky na kybernetickou bezpečnost, než jsou požadavky stanovené v tomto nařízení. V souladu se směrnicí (EU) 2022/2555 a v souladu s její zásadou minimální harmonizace proto mohou členské státy uložit dodatečné požadavky na kybernetickou bezpečnost pro používání produktů informačních a komunikačních technologií (IKT) základními nebo důležitými subjekty podle uvedené směrnice, aby byla zajištěna vyšší úroveň kybernetické bezpečnosti, pokud jsou tyto požadavky v souladu s povinnostmi členských států stanovenými v právu Unie. Záležitosti, na něž se toto nařízení nevztahuje, mohou zahrnovat jiné než technické faktory týkající se produktů s digitálními prvky a jejich výrobců. Členské státy proto mohou stanovit vnitrostátní opatření, včetně omezení týkajících se produktů s digitálními prvky nebo dodavatelů těchto produktů, která zohledňují jiné než technické faktory. Vnitrostátní opatření týkající se těchto faktorů musejí být v souladu s právem Unie.

(14) Tímto nařízením by neměla být dotčena odpovědnost členských států za zajištění národní bezpečnosti v souladu s právem Unie. Členské státy by měly mít možnost uložit pro produkty s digitálními prvky, které jsou pořizovány nebo používány pro účely národní bezpečnosti nebo obrany, dodatečná opatření, pokud jsou tato opatření v souladu s povinnostmi členských států stanovenými v právu Unie.

(15) Toto nařízení se vztahuje na hospodářské subjekty pouze ve vztahu k produktům s digitálními prvky, které jsou dodány na trh, tedy dodány za účelem distribuce nebo použití na trhu Unie v rámci obchodní činnosti. Dodávání v rámci obchodní činnosti může být charakterizováno nejen stanovením ceny za produkt s digitálními prvky, ale také 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. Přijímání darů bez záměru vytvářet zisk by nemělo být považováno za obchodní činnost.

(16) Pro účely tohoto nařízení by produkty s digitálními prvky poskytované v rámci služby, za niž se účtuje poplatek výhradně za účelem úhrady skutečných nákladů, které přímo souvisejí s provozováním této služby, jako je tomu v případě některých produktů s digitálními prvky poskytovaných subjekty veřejné správy, neměly být samy o sobě považovány za obchodní činnost. Dále by se produkty s digitálními prvky, které vyvíjí nebo upravuje subjekt veřejné správy výhradně pro vlastní potřebu neměly považovat za produkty dodávané na trh ve smyslu tohoto nařízení.

(17) Software a data, která jsou otevřeně sdílena a k nimž nebo k jejichž upraveným verzím mají uživatelé volný přístup a mohou je používat, upravovat a redistribuovat, mohou přispět k výzkumu a inovacím na trhu. Na podporu vývoje a zavádění svobodného softwaru s otevřeným zdrojovým kódem, zejména mikropodniky a malými a středními podniky, včetně začínajících podniků, jednotlivci, neziskovými organizacemi a akademickými organizacemi provádějícími výzkum, by se při použití tohoto nařízení na produkty s digitálními prvky, které jsou považovány za svobodný software s otevřeným zdrojovým kódem dodávaný za účelem distribuce nebo použití v rámci obchodní činnosti, měla zohlednit povaha různých modelů vývoje softwaru distribuovaného a vyvíjeného na základě licence k svobodnému softwaru s otevřeným zdrojovým kódem.

(18) Svobodným softwarem s otevřeným zdrojovým kódem se rozumí software, jehož zdrojový kód je otevřeně sdílen a jehož licence poskytuje veškerá práva na to, aby byl volně přístupný, použitelný, upravitelný a dále distribuovatelný. Svobodný software s otevřeným zdrojovým kódem je vyvíjen, udržován a šířen otevřeně, a to i prostřednictvím online platforem. Ve vztahu k hospodářským subjektům, které spadají do oblasti působnosti tohoto nařízení, by do oblasti působnosti tohoto nařízení měl spadat pouze svobodný software s otevřeným zdrojovým kódem, který je dodáván na trh a tedy dodávám za účelem distribuce nebo použití v rámci obchodní činnosti. Při určování komerční nebo nekomerční povahy této činnosti by proto neměly být brány v úvahu pouze okolnosti, za nichž byl produkt s digitálními prvky vyvinut, nebo způsob financování jeho vývoje. Konkrétně 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. Kromě toho by dodání produktů s digitálními prvky, které jsou považovány za komponenty svobodného softwaru s otevřeným zdrojovým kódem určené k začlenění jinými výrobci do jejich vlastních produktů s digitálními prvky, mělo být považováno za dodání na trh pouze tehdy, pokud danou komponentu její původní výrobce zpeněží. Například pouhá skutečnost, že softwarový produkt s otevřeným zdrojovým kódem s digitálními prvky získá finanční podporu od výrobců nebo že výrobci přispívají k vývoji takového produktu, by sama o sobě neměla znamenat, že se jedná o činnost komerční povahy. Ani pouhé pravidelné vydávání produktu s digitálními prvky by samo o sobě nemělo vést k závěru, že je tento produkt dodáván v rámci obchodní činnosti. Za obchodní činnost by navíc neměl být pro účely tohoto nařízení považován ani vývoj produktů s digitálními prvky považovaných za svobodný software s otevřeným zdrojovým kódem neziskovými organizacemi, za předpokladu, že organizace byla zřízena takovým způsobem, aby bylo zajištěno, že veškeré příjmy po odečtení nákladů budou použity k dosažení neziskových cílů. Toto nařízení 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.

(19) Vzhledem k tomu, 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 tohoto nařízení, má význam pro kybernetickou bezpečnost, by se na právnické osoby, které poskytují udržitelnou podporu pro vývoj takových produktů určených k obchodní činnosti a které hrají hlavní úlohu při zajišťování životaschopnosti těchto produktů (správci softwaru s otevřeným zdrojovým kódem), měl vztahovat zjednodušený a individuálně upravený regulační režim. Mezi správce softwaru s otevřeným zdrojovým kódem patří některé nadace a rovněž subjekty, které vyvíjejí a zveřejňují svobodný software s otevřeným zdrojovým kódem v obchodním kontextu, včetně neziskových subjektů. Regulační režim by měl zohledňovat jejich zvláštní povahu a slučitelnost s druhem uložených povinností. Měl by se vztahovat pouze na produkty s digitálními prvky považované za svobodný software 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. Pro účely regulačního režimu zahrnuje záměr začlenění do zpeněžovaných produktů s digitálními prvky případy, kdy výrobci, kteří začleňují určitou komponentu do svých vlastních produktů s digitálními prvky, buď pravidelně přispívají k rozvoji této komponenty, nebo poskytují pravidelnou finanční pomoc k zajištění kontinuity softwarového produktu. Poskytování dlouhodobé podpory vývoji produktu s digitálními prvky zahrnuje mimo jiné hosting a správu platforem pro spolupráci v oblasti vývoje softwaru, hosting zdrojového kódu nebo softwaru, správu nebo řízení produktů s digitálními prvky, které jsou považovány za svobodný software s otevřeným zdrojovým kódem, a směrování vývoje těchto produktů. Vzhledem k tomu, že v rámci zjednodušeného a individuálně upraveného regulačního režimu nemají subjekty jednající jako správci softwaru s otevřeným zdrojovým kódem stejné povinnosti, jaké jsou v tomto nařízení uloženy subjektům jednajícím jako výrobci, nemělo by jim být povoleno umísťovat označení CE na produkty s digitálními prvky, jejichž vývoj podporují.

(20) Samotný akt hostingu produktů s digitálními prvky v otevřených repozitářích, a to i prostřednictvím správců balíčků nebo v rámci platforem pro spolupráci, sám o sobě nepředstavuje dodávání produktu s digitálními prvky na trh. Poskytovatelé těchto služeb by měli být považováni za distributory pouze tehdy, dodávají-li takový software na trh, tedy dodávají-li ho za účelem jeho distribuce nebo použití na trhu Unie v rámci obchodní činnosti.

(21) S cílem podpořit a usnadnit náležitou péči výrobců, kteří do svých produktů s digitálními prvky začleňují komponenty svobodného softwaru s otevřeným zdrojovým kódem, které nepodléhají základním požadavkům na kybernetickou bezpečnost stanoveným v tomto nařízení, by Komise měla mít možnost zavést dobrovolné programy osvědčování bezpečnosti, a to buď prostřednictvím aktu v přenesené pravomoci doplňujícího toto nařízení, nebo na základě žádosti o evropské schéma certifikace kybernetické bezpečnosti podle článku 48 nařízení (EU) 2019/881, který by zohledňoval specifika modelů vývoje svobodného softwaru s otevřeným zdrojovým kódem. Programy osvědčování bezpečnosti by měly být koncipovány tak, aby iniciovat nebo financovat osvědčení bezpečnosti mohly nejen fyzické nebo právnické osoby, které vyvíjejí produkt s digitálními prvky, jenž je považován za svobodný software s otevřeným zdrojovým kódem, nebo k jeho vývoji přispívají, ale také třetí strany, jako jsou výrobci, kteří tyto produkty začleňují do svých vlastních produktů s digitálními prvky, uživatelé nebo unijní a vnitrostátní orgány veřejné správy.

(22) S ohledem na cíle tohoto nařízení týkající se kybernetické bezpečnosti ve veřejné sféře, a s cílem zlepšit informovanost členských států, pokud jde o závislost Unie na softwarových komponentách, a zejména na komponentách potenciálně svobodného softwaru s otevřeným zdrojovým kódem, by měla mít specializovaná skupina pro správní spolupráci zřízená tímto nařízením možnost rozhodnout o společném provedení posouzení závislosti Unie. Orgány dozoru nad trhem by měly mít možnost požádat výrobce kategorií produktů s digitálními prvky stanovených specializovanou skupinou pro správní spolupráci, aby předložili softwarový kusovník (SBOM), jenž vytvořili podle tohoto nařízení. V zájmu ochrany důvěrnosti softwarových kusovníků by orgány dozoru nad trhem měly specializované skupině pro správní spolupráci předkládat příslušné informace o závislostech v anonymizované a souhrnné podobě.

(23) Účinnost uplatňování tohoto nařízení bude rovněž záviset na dostupnosti odpovídajících dovedností v oblasti kybernetické bezpečnosti. Nedostatek dovedností v oblasti kybernetické bezpečnosti v Unii a potřeba prioritního řešení souvisejících výzev ve veřejném i soukromém sektoru byly na úrovni Unie uznány v různých programových a politických dokumentech, mimo jiné ve sdělení Komise ze dne 18. dubna 2023 o řešení nedostatku talentů v oblasti kybernetické bezpečnosti za účelem posílení konkurenceschopnosti, růstu a odolnosti EU a v závěrech Rady ze dne 22. května 2023 o politice EU pro kybernetickou obranu. V zájmu zajištění účinného uplatňování tohoto nařízení by členské státy měly zajistit, aby orgány dozoru nad trhem a subjekty posuzování shody měly k dispozici dostatečné finanční zdroje pro náležité personální zajištění, a mohly tak plnit své úkoly stanovené v tomto nařízení. Tato opatření by měla zvýšit mobilitu pracovních sil v oblasti kybernetické bezpečnosti a rozšířit s ní související profesní možnosti. Měla by rovněž přispět k větší odolnosti a inkluzivnosti pracovní síly v oblasti kybernetické bezpečnosti, a to i pokud jde o genderové otázky. Členské státy by proto měly přijmout opatření k zajištění toho, aby tyto úkoly plnili náležitě vyškolení odborníci s nezbytnými dovednostmi v oblasti kybernetické bezpečnosti. Podobně by výrobci měli zajistit, aby jejich zaměstnanci měli potřebné dovednosti pro plnění svých povinností stanovených v tomto nařízení. Členské státy a Komise by měly v souladu se svými výsadami a pravomocemi a zvláštními úkoly, které jsou jim svěřeny tímto nařízením, přijmout opatření na podporu výrobců, zejména mikropodniků a malých a středních podniků, včetně začínajících podniků, a to i v oblastech, jako je rozvoj dovedností, aby tito výrobci mohli splnit své povinnosti stanovené v tomto nařízení. Vzhledem k tomu, že směrnice (EU) 2022/2555 vyžaduje, aby členské státy přijaly v rámci své vnitrostátní strategie kybernetické bezpečnosti opatření na podporu a rozvoj odborné přípravy a dovedností v oblasti kybernetické bezpečnosti, mohou členské státy při přijímání těchto strategií navíc zvážit, zda budou rovněž řešit potřeby týkající se dovedností v oblasti kybernetické bezpečnosti vyplývající z tohoto nařízení, včetně těch, které se týkají rekvalifikace a zvyšování kvalifikace.

(24) Bezpečný internet je nezbytný pro fungování kritických infrastruktur a pro společnost jako celek. Směrnice (EU) 2022/2555 má za cíl zajistit vysokou úroveň kybernetické bezpečnosti služeb poskytovaných základními a důležitými subjekty uvedenými v článku 3 uvedené směrnice, včetně poskytovatelů digitální infrastruktury, kteří podporují klíčové funkce otevřeného internetu a zajišťují přístup k internetu a poskytují internetové služby. Je proto důležité, aby produkty s digitálními prvky, které poskytovatelé digitální infrastruktury potřebují k zajištění fungování internetu, byly vyvíjeny bezpečným způsobem a aby splňovaly zavedené normy bezpečnosti internetu. Cílem tohoto nařízení, které se vztahuje na všechny připojitelné hardwarové a softwarové produkty, je rovněž usnadnit dodržování požadavků dodavatelského řetězce ze strany poskytovatelů digitální infrastruktury podle směrnice (EU) 2022/2555 tím, že zajistí, aby produkty s digitálními prvky, které používají při poskytování svých služeb, byly vyvíjeny bezpečným způsobem a aby měli přístup k včasným bezpečnostním aktualizacím těchto produktů.

(25) V nařízení Evropského parlamentu a Rady (EU) 2017/745 ([9]) jsou stanovena pravidla pro zdravotnické prostředky a v nařízení Evropského parlamentu a Rady (EU) 2017/746 ([10]) pravidla pro diagnostické zdravotnické prostředky in vitro. Uvedená nařízení řeší kybernetická bezpečnostní rizika a uplatňují konkrétní přístupy, kterými se toto nařízení rovněž zabývá. Přesněji řečeno, v nařízení (EU) 2017/745 a nařízení (EU) 2017/746 jsou stanoveny základní požadavky na zdravotnické prostředky, které fungují prostřednictvím elektronického systému nebo které jsou samy softwarem. Tato nařízení se vztahují rovněž na určitý nevestavěný software a na přístup zohledňující celý životní cyklus. Uvedené požadavky ukládají výrobcům, aby vyvíjeli a vytvářeli své produkty uplatňováním zásad řízení rizik a stanovením požadavků týkajících se opatření v oblasti bezpečnosti IT, jakož i odpovídajících postupů posuzování shody. Kromě toho jsou od prosince 2019 zavedeny zvláštní pokyny týkající se kybernetické bezpečnosti zdravotnických prostředků, které výrobcům zdravotnických prostředků, včetně diagnostických prostředků in vitro, poskytují informace, jak splnit všechny příslušné základní požadavky na kybernetickou bezpečnost stanovené v příloze I uvedených nařízení. Na produkty s digitálními prvky, na něž se vztahuje jedno z těchto nařízení, by se proto toto nařízení nemělo vztahovat.

(26) Do působnosti tohoto nařízení nespadají produkty s digitálními prvky, které jsou vyvinuty nebo upraveny výhradně pro účely národní bezpečnosti nebo obrany, nebo produkty, které jsou speciálně určeny ke zpracování utajovaných informací. Členským státům se doporučuje, aby pro tyto produkty zajistily alespoň stejnou úroveň ochrany jako pro produkty spadající do oblasti působnosti tohoto nařízení.

([9]) Nařízení Evropského parlamentu a Rady (EU) 2017/745 ze dne 5. dubna 2017 o zdravotnických prostředcích, změně směrnice 2001/83/ES, nařízení (ES) č. 178/2002 a nařízení (ES) č. 1223/2009 a o zrušení směrnic Rady 90/385/EHS a 93/42/EHS (Úř. věst. L 117, 5.5.2017, s. 1).

([10]) Nařízení Evropského parlamentu a Rady (EU) 2017/746 ze dne 5. dubna 2017 o diagnostických zdravotnických prostředcích in vitro a o zrušení směrnice 98/79/ES a rozhodnutí Komise 2010/227/EU (Úř. věst. L 117, 5.5.2017, s. 176).

(27) V nařízení Evropského parlamentu a Rady (EU) 2019/2144 ([11]) jsou stanoveny požadavky na schvalování typů vozidel a jejich systémů a komponent a zavedeny určité požadavky na kybernetickou bezpečnost, včetně požadavků na provoz certifikovaného systému řízení kybernetické bezpečnosti, na aktualizace softwaru týkající se politiky a postupů organizací pro kybernetická bezpečnostní rizika, která souvisejí s celým životním cyklem vozidel, zařízení a služeb v souladu s použitelnými předpisy OSN o technických specifikacích a kybernetické bezpečnosti, zejména s předpisem OSN č. 155 – Jednotná ustanovení pro schvalování vozidel z hlediska kybernetické bezpečnosti a systému řízení kybernetické bezpečnosti ([12]), přičemž stanovují konkrétní postupy posuzování shody. V oblasti letectví je hlavním cílem nařízení Evropského parlamentu a Rady (EU) 2018/1139 ([13]) zavést a udržovat vysokou jednotnou úroveň bezpečnosti civilního letectví v Unii. Vytváří rámec pro základní požadavky na letovou způsobilost leteckých výrobků, dílů a vybavení, včetně softwaru, který zahrnuje povinnosti ochrany před hrozbami v oblasti informační bezpečnosti. Certifikace podle nařízení (EU) 2018/1139 poskytuje záruky na úrovni, kterou sleduje i toto nařízení. Na produkty s digitálními prvky, na něž se vztahuje nařízení (EU) 2019/2144, a na produkty certifikované v souladu s nařízením (EU) 2018/1139 by se proto neměly vztahovat základní požadavky na kybernetickou bezpečnost a postupy posuzování shody stanovené v tomto nařízení.

(28) Toto nařízení stanovuje horizontální pravidla kybernetické bezpečnosti, která nejsou specifická pro určitá odvětví nebo určité produkty s digitálními prvky. Nicméně by mohla být zavedena odvětvová pravidla nebo pravidla Unie specifická pro určité produkty, která by stanovila požadavky týkající se všech nebo některých rizik, na něž se vztahují základní požadavky na kybernetickou bezpečnost stanovené tímto nařízením. V těchto případech může být použití tohoto nařízení na produkty s digitálními prvky, na něž se vztahují jiná pravidla Unie, která stanovují požadavky řešící všechna nebo některá rizika, pro něž platí základní požadavky na kybernetickou bezpečnost stanovené v tomto nařízení, omezeno nebo vyloučeno, pokud je takové omezení nebo vyloučení v souladu s celkovým regulačním rámcem použitelným pro tyto produkty a pokud odvětvová pravidla dosahují alespoň stejné úrovně ochrany, jako je stanovena v tomto nařízení. Komisi by měla být svěřena pravomoc přijímat akty v přenesené pravomoci za účelem doplnění tohoto nařízení tím, že tyto produkty a pravidla určí. V případě stávajícího práva Unie, na nějž by se tato omezení nebo vyloučení měla vztahovat, obsahuje toto nařízení zvláštní ustanovení, která objasňují jeho vztah k uvedenému právu Unie.

(29) Aby se zajistila možnost účinné opravy produktů s digitálními prvky dodaných na trh a prodloužení jejich životnosti, je třeba stanovit výjimku pro náhradní komponenty. Tato výjimka by se měla vztahovat jak na náhradní komponenty, které mají sloužit k opravě zastaralých produktů dodaných na trh přede dnem použitelnosti tohoto nařízení, tak na náhradní komponenty, které již prošly postupy posuzování shody podle tohoto nařízení.

(30) V nařízení Komise v přenesené pravomoci (EU) 2022/30 ([14]) je stanoveno, že se na některá rádiová zařízení vztahuje řada základních požadavků uvedených v čl. 3 odst. 3 písm. d), e) a f) směrnice Evropského parlamentu a Rady 2014/53/EU ([15]), které se týkají nepříznivého vlivu na síť a zneužití zdrojů sítě, osobních údajů a soukromí a podvodů. V prováděcím rozhodnutí Komise C(2022) 5637 ze dne 5. srpna 2022 o žádosti o normalizaci předložené Evropskému výboru pro normalizaci a Evropskému výboru pro normalizaci v elektrotechnice, jsou stanoveny požadavky na vypracování konkrétních norem, které dále upřesňují, jak by měly být tyto základní požadavky řešeny. Základní požadavky na kybernetickou bezpečnost stanovené v tomto nařízení zahrnují všechny prvky základních požadavků uvedených v čl. 3 odst. 3 písm. d), e) a f) směrnice 2014/53/EU. Základní požadavky na

([11]) Nařízení Evropského parlamentu a Rady (EU) 2019/2144 ze dne 27. listopadu 2019 o požadavcích pro schvalování typu motorových vozidel a jejich přípojných vozidel a systémů, konstrukčních částí a samostatných technických celků určených pro tato vozidla z hlediska obecné bezpečnosti a ochrany cestujících ve vozidle a zranitelných účastníků silničního provozu, o změně nařízení Evropského parlamentu a Rady (EU) 2018/858 a o zrušení nařízení Evropského parlamentu a Rady (ES) č. 78/2009, (ES) č. 79/2009 a (ES) č. 661/2009 a nařízení Komise (ES) č. 631/2009, (EU) č. 406/2010, (EU) č. 672/2010, (EU) č. 1003/2010, (EU) č. 1005/2010, (EU) č. 1008/2010, (EU) č. 1009/2010, (EU) č. 19/2011, (EU) č. 109/2011, (EU) č. 458/2011, (EU) č. 65/2012, (EU) č. 130/2012, (EU) č. 347/2012, (EU) č. 351/2012, (EU) č. 1230/2012 a (EU) 2015/166 (Úř. věst. L 325, 16.12.2019, s. 1).

([12]) Úř. věst. L 82, 9.3.2021, s. 30.

([13]) Nařízení Evropského parlamentu a Rady (EU) 2018/1139 ze dne 4. července 2018 o společných pravidlech v oblasti civilního letectví a o zřízení Agentury Evropské unie pro bezpečnost letectví, kterým se mění nařízení (ES) č. 2111/2005, (ES) č. 1008/2008, (EU) č. 996/2010, (EU) č. 376/2014 a směrnice Evropského parlamentu a Rady 2014/30/EU a 2014/53/EU a kterým se zrušuje nařízení Evropského parlamentu a Rady (ES) č. 552/2004 a (ES) č. 216/2008 a nařízení Rady (EHS) č. 3922/91 (Úř. věst. L 212, 22.8.2018, s. 1).

([14]) Nařízení Komise v přenesené pravomoci (EU) 2022/30 ze dne 29. října 2021, kterým se doplňuje směrnice Evropského parlamentu a Rady 2014/53/EU, pokud jde o uplatňování základních požadavků uvedených v čl. 3 odst. 3 písm. d), e) a f) uvedené směrnice (Úř. věst. L 7, 12.1.2022, s. 6).

([15]) Směrnice 2014/53/EU Evropského parlamentu a Rady ze dne 16. dubna 2014 o harmonizaci právních předpisů členských států týkajících se dodávání rádiových zařízení na trh a zrušení směrnice 1999/5/ES (Úř. věst. L 153, 22.5.2014, s. 62).

kybernetickou bezpečnost stanovené v tomto nařízení jsou navíc v souladu s cíli požadavků týkajících se konkrétních norem obsažených v uvedené žádosti o normalizaci. Pokud tedy Komise zruší nebo změní nařízení v přenesené pravomoci (EU) 2022/30 s tím důsledkem, že se přestane uplatňovat na některé produkty, na něž se vztahuje toto nařízení, měla by Komise a evropské normalizační organizace při přípravě a vypracovávání harmonizovaných norem s cílem usnadnit uplatňování tohoto nařízení zohlednit normalizační práci provedenou v souvislosti s prováděcím rozhodnutím C(2022) 5637. Během přechodného období pro uplatňování tohoto nařízení by Komise měla poskytnout pokyny výrobcům, na něž se vztahuje toto nařízení i nařízení v přenesené pravomoci (EU) 2022/30, s cílem usnadnit prokázání souladu s oběma těmito nařízeními.

(31) Směrnice Evropského parlamentu a Rady (EU) 2024/2853 ([16]) doplňuje toto nařízení. Směrnice stanovuje pravidla týkající se odpovědnosti za vadné produkty, aby poškozené osoby mohly požadovat náhradu škody, pokud byla tato škoda způsobena vadnými produkty. Je v ní zavedena zásada, podle níž je výrobce produktu odpovědný za škody způsobené nedostatečnou bezpečností jeho produktu, a to bez ohledu na zavinění (objektivní odpovědnost). Pokud taková nedostatečná bezpečnost spočívá v neexistenci bezpečnostních aktualizací po uvedení produktu na trh a vznikne tím škoda, může být uplatněna odpovědnost výrobce. Povinnosti výrobců, které se týkají poskytování těchto bezpečnostních aktualizací, by měly být stanoveny v tomto nařízení.

(32) Tímto nařízením by nemělo být dotčeno nařízení Evropského parlamentu a Rady (EU) 2016/679 ([17]), včetně ustanovení o zavedení mechanismů pro vydávání osvědčení o ochraně údajů a zavedení pečetí a známek dokládajících ochranu údajů pro účely prokázání souladu s uvedeným nařízením v případě operací zpracování prováděných správci a zpracovateli. Tyto operace by mohly být začleněny do produktu s digitálními prvky. Klíčovými prvky nařízení (EU) 2016/679 jsou záměrná a standardní ochrana osobních údajů a kybernetická bezpečnost obecně. Tím, že chrání spotřebitele a organizace před kybernetickými bezpečnostními riziky, mají základní požadavky na kybernetickou bezpečnost stanovené v tomto nařízení rovněž přispět ke zvýšení ochrany osobních údajů a soukromí jednotlivců. Měla by být zvážena součinnost v oblasti normalizace i certifikace týkající se aspektů kybernetické bezpečnosti prostřednictvím spolupráce mezi Komisí, evropskými normalizačními organizacemi, Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA), Evropským sborem pro ochranu osobních údajů zřízeným nařízením (EU) 2016/679 a vnitrostátními dozorovými úřady pro ochranu údajů. Součinnost mezi tímto nařízením a právem Unie v oblasti ochrany údajů by měla být vytvořena rovněž v oblasti dozoru nad trhem a vymáhání práva. Za tímto účelem by vnitrostátní orgány dozoru nad trhem určené podle tohoto nařízení měly spolupracovat s orgány vykonávajícími dohled nad uplatňováním práva Unie v oblasti ochrany údajů. Později zmíněné by měly rovněž mít přístup k informacím, které jsou důležité pro plnění jejich úkolů.

(33) Pokud jejich produkty spadají do oblasti působnosti tohoto nařízení, měli by poskytovatelé evropských peněženek digitální identity podle čl. 5a odst. 2 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ([18]) splňovat horizontální základní požadavky na kybernetickou bezpečnost stanovené v tomto nařízení i konkrétní bezpečnostní požadavky stanovené v článku 5a nařízení (EU) č. 910/2014. Aby se usnadnilo dodržování požadavků, měli by být poskytovatelé peněženek schopni prokázat soulad evropských peněženek digitální identity s požadavky stanovenými v tomto nařízení a v nařízení (EU) č. 910/2014, a to prostřednictvím certifikace svých produktů v rámci evropského schématu certifikace kybernetické bezpečnosti zřízeného podle nařízení (EU) 2019/881, pro který Komise stanovila prostřednictvím aktů v přenesené pravomoci předpoklad shody s tímto nařízením, pokud se certifikát nebo jeho části vztahují na tyto požadavky.

(34) Během fáze návrhu a vývoje by výrobci při začleňování komponent, které pocházejí od třetích stran, do produktů s digitálními prvky měli věnovat náležitou péči těmto komponentám, a to i pokud jde o komponenty svobodného softwaru s otevřeným zdrojovým kódem, které nebyly dodány na trh, aby zajistili, že produkty budou navrženy, vyvinuty a vyrobeny v souladu se základními požadavky na kybernetickou bezpečnost stanovenými v tomto

([16]) Směrnice Evropského parlamentu a Rady (EU) 2024/2853 ze dne 23. října 2024 o odpovědnosti za vadné výrobky a o zrušení směrnice Rady 85/374/EHS (Úř. věst. L, 2024/2853, 18.11.2024, ELI: http://data.europa.eu/eli/dir/2024/2853/oj).

([17]) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

([18]) Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (Úř. věst. L 257, 28.8.2014, s. 73).

nařízení. Vhodná úroveň náležité péče závisí na povaze a úrovni kybernetického bezpečnostního rizika, které se s danou komponentou pojí, a za tímto účelem by měla zohledňovat jeden nebo více z následujících kroků: případné ověření, zda výrobce komponenty prokázal shodu s tímto nařízením, včetně kontroly, zda je komponenta již opatřena označením CE, ověření, zda je komponenta předmětem pravidelných bezpečnostních aktualizací, což je možné zjistit například z její historie bezpečnostních aktualizací, ověření, zda komponenta nemá žádné zranitelnosti registrované v Evropské databázi zranitelností zřízené podle čl. 12 odst. 2 směrnice (EU) 2022/2555 nebo v jiných veřejně přístupných databázích zranitelností nebo provedení dalších bezpečnostních testů. Povinnosti týkající se řešení zranitelností stanovené v tomto nařízení, které musejí výrobci při uvádění produktu s digitálními prvky na trh a během doby podpory dodržet, se vztahují na produkty s digitálními prvky jako na celek, včetně všech začleněných komponent. Pokud při uplatňování náležité péče výrobce produktu s digitálními prvky zjistí, že má určitá komponenta zranitelnost, a to i pokud jde o komponentu tvořenou svobodným softwarem s otevřeným zdrojovým kódem, měl by informovat osobu nebo subjekt, který komponentu vyrobil nebo provádí její údržbu, měl by se zranitelností zabývat a napravit ji a případně poskytnout dotčené osobě nebo subjektu použitou bezpečnostní opravu.

(35) Je možné, že bezprostředně po uplynutí přechodného období pro použití tohoto nařízení nebude mít výrobce produktu s digitálními prvky, který do produktu začlení jednu nebo více komponent pocházejících od třetích stran, na které se rovněž vztahuje toto nařízení, možnost v rámci své povinnosti náležité péče ověřit, zda výrobci těchto komponent prokázali shodu s tímto nařízením, například ověřením toho, zda jsou komponenty již opatřeny označením CE. Tak tomu může být v případě, že komponenty byly do produktu začleněny před tím, než se toto nařízení začalo uplatňovat na výrobce těchto komponent. V takovém případě by měl výrobce, který tyto komponenty do produktu začlenil, zajistit náležitou péči jinými prostředky.

(36) Aby se produkty s digitálními prvky mohly volně pohybovat na vnitřním trhu, měly by být opatřeny označením CE, které viditelně, čitelně a nesmazatelně vyjadřuje jejich shodu s tímto nařízením. Členské státy by neměly vytvářet bezdůvodné překážky bránící uvádění na trh u produktů s digitálními prvky, které jsou v souladu s požadavky stanovenými v tomto nařízení a jsou opatřeny označením CE. Na veletrzích, výstavách a předváděcích nebo podobných akcích by navíc členské státy neměly bránit prezentaci ani používání produktu s digitálními prvky, který není v souladu s tímto nařízením, včetně jeho prototypů, a to za předpokladu, že je produkt prezentován s viditelným označením, které jasně ukazuje, že není v souladu s tímto nařízením a nemá být dodáván na trh, dokud s ním nebude v souladu.

(37) Aby bylo zajištěno, že výrobci mohou vydat software pro účely testování před tím, než podrobí své produkty s digitálními prvky posouzení shody, neměly by členské státy bránit zpřístupnění nedokončeného softwaru, například alfa verzí, beta verzí nebo kandidátů na vydání (*release candidates*), pokud je nedokončený zpřístupněný pouze po dobu nezbytnou k jeho testování a získání zpětné vazby. Výrobci by měli zajistit, aby byl software zpřístupněný za těchto podmínek vydán pouze po posouzení rizik a aby v co největší míře splňoval bezpečnostní požadavky týkající se vlastností produktů s digitálními prvky stanovené tomto nařízení. Výrobci by rovněž měli v co největší míře uplatňovat požadavky na řešení zranitelností. Výrobci by neměli nutit uživatele k přechodu na verze, které jsou vydávány pouze pro účely testování.

(38) Aby se zajistilo, že produkty s digitálními prvky nepředstavují při uvedení na trh kybernetické bezpečnostní riziko pro osoby ani organizace, měly by být pro tyto produkty stanoveny základní požadavky na kybernetickou bezpečnost. Tyto základní požadavky na kybernetickou bezpečnost, včetně požadavků na řešení zranitelností, se vztahují na každý jednotlivý produkt s digitálními prvky při uvedení na trh bez ohledu na to, zda je produkt s digitálními prvky vyroben jednotlivě nebo sériově. Například u každého druhu produktu by měl každý jednotlivý produkt s digitálními prvky před uvedením na trh obdržet veškeré bezpečnostní opravy nebo aktualizace, které jsou v té době k dispozici k řešení příslušných bezpečnostních problémů. Pokud jsou produkty s digitálními prvky následně upraveny, ať už fyzicky, nebo digitálně, a to způsobem, který výrobce při původním posouzení rizik nepředvídal a který by mohl znamenat, že produkty již nesplňují příslušné základní požadavky na kybernetickou bezpečnost, měla by se taková změna považovat za podstatnou změnu. Kupříkladu za údržbové operace mohou být považovány takové opravy, které neupravují produkt s digitálními prvky již uvedený na trh, takovým způsobem, kterým by mohl být ovlivněn jeho soulad s příslušnými požadavky, nebo že zamýšlený účel, pro který byl produkt posouzen, může být změněn.

(39) Stejně jako v případě fyzických oprav nebo změn by měl být produkt s digitálními prvky považován za podstatně změněný změnou softwaru, pokud tato aktualizace softwaru změnila zamýšlený účel tohoto produktu a pokud tyto změny výrobce při původním posouzení rizik nepředvídal či pokud se změnila povaha nebezpečí nebo se

v důsledku aktualizace softwaru změnila úroveň kybernetického bezpečnostního rizika a pokud aktualizovaná verze produktu byla dodána na trh. Pokud bezpečnostní aktualizace, která má snížit úroveň kybernetického bezpečnostního rizika produktu s digitálními prvky, nemění zamýšlený účel produktu s digitálními prvky, nepovažuje se za podstatnou změnu. Mezi tyto nepodstatné změny obvykle patří situace, kdy bezpečnostní aktualizace zahrnuje pouze drobné úpravy zdrojového kódu. Tak by tomu mohlo být například v případě, kdy bezpečnostní aktualizace řeší známou zranitelnost, včetně pomocí změny funkcí nebo výkonnosti produktu s digitálními prvky, a to výhradně za účelem snížení kybernetického bezpečnostního rizika. Drobné aktualizace funkčnosti, jako je zlepšení vizuálních prvků nebo přidání nových piktogramů nebo jazyků do uživatelského rozhraní, by obecně neměly být považovány za podstatné změny. Naopak pokud aktualizace prvků mění původní určené funkce či druh nebo výkonnost produktu s digitálními prvky a splňují uvedená kritéria, měly by být považovány za podstatnou změnu, neboť přidání nových prvků obvykle vede k většímu prostoru k útoku, čímž se zvyšuje kybernetické bezpečnostní riziko. Tak by tomu mohlo být například v případě, kdy je do aplikace přidán nový vstupní prvek, který vyžaduje, aby výrobce zajistil odpovídající validaci vstupů. Při posuzování, zda je aktualizace prvku považována za podstatnou změnu, není důležité, zda je poskytována jako samostatná aktualizace, nebo v kombinaci s bezpečnostní aktualizací. Komise by měla vydat pokyny ohledně způsobu určení podstatné změny.

(40) S ohledem na to, že vývoj softwaru je založen na opakovaných změnách, by výrobci, kteří uvedli kvůli následným podstatným změnám softwarového produktu nové verze tohoto produktu, měli mít možnost poskytovat bezpečnostní aktualizace během doby podpory pouze pro tu verzi softwarového produktu, kterou na trh uvedli jako poslední. Měli by mít možnost tak učinit pouze tehdy, mají-li uživatelé příslušných předchozích verzí produktu bezplatný přístup k té verzi produktu, která byla na trh uvedena jako poslední, a nevznikají jim dodatečné náklady na úpravu hardwaru ani softwaru, na němž produkt používají. Tak by tomu mohlo být například v případech, kdy aktualizace operačního systému stolního počítače nevyžaduje nový hardware, jako je rychlejší centrální procesor nebo větší paměť. Výrobce by však měl během doby podpory i nadále dodržovat další požadavky na řešení zranitelností, například zavést politiku koordinovaného zveřejňování zranitelností nebo opatření na usnadnění sdělování informací o potenciálních zranitelnostech u všech následných podstatně změněných verzí softwarového produktu uvedeného na trh. Výrobci by měli mít možnost poskytovat drobné bezpečnostní aktualizace nebo aktualizace funkcí, které nepředstavují podstatnou změnu, pouze pro poslední verzi nebo dílčí verzi softwarového produktu, který dosud nebyl podstatně změněn. Pokud však hardwarový produkt, jako je chytrý telefon, není kompatibilní s nejnovější verzí operačního systému, s nímž byl původně dodán, měl by výrobce během doby podpory nadále poskytovat bezpečnostní aktualizace alespoň pro poslední kompatibilní verzi operačního systému.

(41) V souladu s obecně zavedeným konceptem podstatné změny u produktů, na něž se vztahují harmonizační právní předpisy Unie, je vhodné, pokud dojde k podstatné změně, která může ovlivnit soulad produktu s digitálními prvky s tímto nařízením nebo pokud se změní zamýšlený účel daného produktu, aby byl u produktu s digitálními prvky ověřen soulad s předpisy a aby byl případně podroben novému posouzení shody. Pokud výrobce provádí posouzení shody za účasti třetí strany, měla by být v příslušném případě této třetí straně oznámena změna, které by mohla vést k podstatné změně.

(42) Pokud 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 ([19]), 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.

(43) Produkty s digitálními prvky by měly být považovány za důležité, pokud může být negativní dopad zneužití případných zranitelností produktu závažný, mimo jiné v důsledku funkcí souvisejících s kybernetickou bezpečností nebo funkce, která s sebou nese významné riziko nepříznivých účinků, pokud jde o intenzitu těchto účinků a jejich možnost narušit, ovládat nebo poškodit velký počet jiných produktů s digitálními prvky nebo zdraví, zabezpečení nebo bezpečnost jeho uživatelů prostřednictvím přímé manipulace, například funkce centrálního systému, včetně správy sítě, řízení konfigurace, virtualizace nebo zpracování osobních údajů. Konkrétně zranitelnosti produktů s digitálními prvky, které mají funkce související s kybernetickou bezpečností, jako jsou například boot managery, mohou vést k šíření bezpečnostních problémů v celém dodavatelském řetězci. Závažnost dopadu incidentu se může

([19]) Nařízení Evropského parlamentu a Rady (EU) 2024/1781 ze dne 13. června 2024 o vytvoření rámce pro stanovení požadavků na ekodesign udržitelných výrobků, o změně směrnice (EU) 2020/1828 a nařízení (EU) 2023/1542 a o zrušení směrnice 2009/125/ES (Úř. věst. L, 2024/1781, 28.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1781/oj).

rovněž zvýšit, pokud produkt vykonává primárně funkci centrálního systému, včetně správy sítě, řízení konfigurace, virtualizace nebo zpracování osobních údajů.

(44) Některé kategorie produktů s digitálními prvky by měly podléhat přísnějším postupům posuzování shody, přičemž by měl být zachován přiměřený přístup. Za tímto účelem by důležité produkty s digitálními prvky měly být rozděleny do dvou tříd, které by odrážely úroveň kybernetických bezpečnostních rizik spojených s těmito kategoriemi produktů. Incident týkající se důležitých produktů s digitálními prvky, které spadají do třídy II, by mohl mít větší negativní dopad než incident týkající se důležitých produktů s digitálními prvky, které spadají do třídy I, například vzhledem k povaze jejich funkce související s kybernetickou bezpečností nebo vzhledem k výkonu jiné funkce, která s sebou nese významné riziko nepříznivých účinků. Ukazatelem takového většího negativního dopadu produktů s digitálními prvky, které spadají do třídy II, by mohlo být to, že plní funkci související s kybernetickou bezpečností nebo jinou funkci, která s sebou nese významné riziko nepříznivých účinků, jež je vyšší než u produktů uvedených ve třídě I, nebo že splňují obě tato kritéria. Důležité produkty s digitálními prvky, které spadají do třídy II, by proto měly podléhat přísnějšímu postupu posuzování shody.

(45) Důležité produkty s digitálními prvky uvedené v tomto nařízení by se měly považovat za produkty, které mají klíčovou funkci jedné z kategorií důležitých produktů s digitálními prvky, která je stanovena v tomto nařízení. V tomto nařízení jsou například stanoveny kategorie důležitých produktů s digitálními prvky, které jsou definovány svou klíčovou funkcí jako firewally nebo systémy detekce narušení či prevence ve třídě II. V důsledku toho podléhají firewally a systémy detekce narušení či prevence povinnému posouzení shody třetí stranou. Tak tomu není v případě jiných produktů s digitálními prvky, které nejsou klasifikovány jako důležité produkty s digitálními prvky, které mohou začlenit firewally nebo systémy detekce narušení či prevence. Komise by měla přijmout prováděcí akt s cílem upřesnit technický popis kategorií důležitých produktů s digitálními prvky, které spadají do třídy I a třídy II, jak je stanoveno v tomto nařízení.

(46) Kategorie kritických produktů s digitálními prvky stanovené v tomto nařízení mají funkci související s kybernetickou bezpečností a plní funkci, která s sebou nese významné riziko nepříznivých účinků, pokud jde o intenzitu těchto účinků a jejich schopnost narušit, ovládat nebo poškodit velký počet jiných produktů s digitálními prvky prostřednictvím přímé manipulace. Kromě toho jsou tyto kategorie produktů s digitálními prvky považovány za produkty, na nichž jsou základní subjekty uvedené v čl. 3 odst. 1 směrnice (EU) 2022/2555 kriticky závislé. Kategorie kritických produktů s digitálními prvky stanovené v příloze tohoto nařízení již vzhledem ke své kritičnosti široce využívají nejrůznější formy certifikace a vztahuje se na ně rovněž evropský systém certifikace kybernetické bezpečnosti (EUCC) stanovený prováděcím nařízením Komise (EU) 2024/482 ([20]). V zájmu zajištění společné odpovídající ochrany kybernetické bezpečnosti kritických produktů s digitálními prvky v Unii by proto mohlo být vhodné a přiměřené, aby tyto kategorie produktů prostřednictvím aktu v přenesené pravomoci podléhaly povinné evropské certifikaci kybernetické bezpečnosti, pokud je příslušné evropské schéma certifikace kybernetické bezpečnosti zahrnující tyto produkty již zaveden, a aby Komise posoudila, jaký dopad by taková plánovaná povinná certifikace mohla mít na trh. Toto posouzení by mělo zohlednit stranu nabídky i stranu poptávky, včetně toho, zda na straně členských států i uživatelů existuje dostatečná poptávka po dotčených produktech s digitálními prvky, aby mohla být evropská certifikace kybernetické bezpečnosti vyžadována, a měla by zohlednit také účely, pro které mají být produkty s digitálními prvky použity, včetně kritické závislosti základních subjektů uvedených v čl. 3 odst. 1 směrnice (EU) 2022/2555 na těchto produktech. V rámci posouzení by se měl analyzovat rovněž možný dopad povinné certifikace na dostupnost těchto produktů na vnitřním trhu a schopnosti a připravenost členských států, pokud jde o zavedení příslušných evropských schémat certifikace kybernetické bezpečnosti.

(47) V aktech v přenesené pravomoci vyžadujících povinnou evropskou certifikaci kybernetické bezpečnosti by měly být určeny produkty s digitálními prvky, které mají klíčovou funkci jedné z kategorií kritických produktů s digitálními prvky stanovených v tomto nařízení a mají podléhat povinné certifikaci a mít požadovanou úroveň záruk, která by měla být alespoň „významná“. Požadovaná úroveň záruky by měla být úměrná úrovni kybernetického bezpečnostního rizika spojeného s produktem s digitálními prvky. Například pokud má produkt s digitálními prvky klíčovou funkci jedné z kategorií kritických produktů s digitálními prvky stanovených v tomto nařízení a je

([20]) Prováděcí nařízení Komise (EU) 2024/482 ze dne 31. ledna 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) 2019/881, pokud jde o přijetí evropského systému certifikace kybernetické bezpečnosti založeného na společných kritériích (EUCC) (Úř. věst. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

určen k použití v citlivém nebo kritickém prostředí, jako jsou produkty určené pro použití základními subjekty podle čl. 3 odst. 1 směrnice (EU) 2022/2555, může u něj být vyžadována nejvyšší úroveň záruky.

(48) Aby byla v Unii zajištěna společná přiměřená ochrana kybernetické bezpečnosti produktů s digitálními prvky, které mají klíčovou funkci jedné z kategorií kritických produktů s digitálními prvky stanovených v tomto nařízení, měla by být Komisi rovněž svěřena pravomoc přijímat akty v přenesené pravomoci za účelem změny tohoto nařízení doplněním nebo vynětím kategorií kritických produktů s digitálními prvky, u nichž by výrobci mohli mít za účelem prokázání souladu s tímto nařízením povinnost získat evropský certifikát kybernetické bezpečnosti v rámci evropského schématu certifikace kybernetické bezpečnosti podle nařízení (EU) 2019/881. K těmto kategoriím lze doplnit novou kategorii kritických produktů s digitálními prvky, pokud jsou na nich základní subjekty uvedené v čl. 3 odst. 1 směrnice (EU) 2022/2555 kriticky závislé, nebo v případě, že jsou tyto kategorie postiženy incidenty či obsahují zneužívané zranitelnosti, by to mohlo vést k narušení kritických dodavatelských řetězců. Při posuzování toho, zda jde nutné doplnit nebo vyjmout některou z kategorií kritických produktů s digitálními prvky prostřednictvím aktu v přenesené pravomoci by Komise měla mít možnost zohlednit, zda členské státy na vnitrostátní úrovni určily produkty s digitálními prvky, které mají zásadní význam pro odolnost základních subjektů uvedených v čl. 3 odst. 1 směrnice (EU) 2022/2555 a které stále častěji čelí kybernetickým útokům v dodavatelském řetězci, jež mohou mít závažný negativní dopad. Kromě toho by Komise měla mít možnost zohlednit výsledek koordinovaného posouzení bezpečnostních rizik kritických dodavatelských řetězců na úrovni Unie, které se provádí v souladu s článkem 22 směrnice (EU) 2022/2555.

(49) Komise by měla zajistit, aby při přípravě opatření pro uplatňování tohoto nařízení proběhly strukturované a pravidelné konzultace se širokou škálou příslušných zúčastněných stran. Tak by tomu mělo být zejména v případě, kdy Komise posuzuje potřebu případné aktualizace seznamů kategorií důležitých nebo kritických produktů s digitálními prvky, přičemž by měla za účelem analýzy kybernetických bezpečnostních rizik a rovnováhy mezi náklady a přínosy spojenými s označením těchto kategorií produktů za důležité nebo kritické vést konzultace s příslušnými výrobci a zohlednit jejich názory.

(50) Toto nařízení se zabývá kybernetickými bezpečnostními riziky cíleným způsobem. Produkty s digitálními prvky však mohou představovat jiná bezpečnostní rizika, která nesouvisejí vždy s kybernetickou bezpečností, ale mohou být důsledkem narušení bezpečnosti. Tato rizika by měla být i nadále upravena jinými příslušnými harmonizačními právními předpisy Unie, než je toto nařízení. Pokud nelze použít žádné jiné harmonizační právní předpisy Unie než toto nařízení, měla by se rizika řídit nařízením Evropského parlamentu a Rady (EU) 2023/988 ([21]).S ohledem na cílenou povahu tohoto nařízení by se proto odchylně od čl. 2 odst. 1 třetího pododstavce písm. b) nařízení (EU) 2023/988 měly použít na produkty s digitálními prvky kapitola III oddílu 1, kapitoly V a VII a kapitoly IX až XI nařízení (EU) 2023/988, pokud jde o bezpečnostní rizika, na něž se toto nařízení nevztahuje, jestliže tyto produkty nejsou předmětem konkrétních požadavků uložených jinými harmonizačními právními předpisy Unie, než je toto nařízení, ve smyslu čl. 3 bodu 27 nařízení (EU) 2023/988.

(51) Produkty s digitálními prvky klasifikované jako vysoce rizikové systémy umělé inteligence podle článku 6 nařízení Evropského parlamentu a Rady (EU) 2024/ 1689 ([22]), které spadají do oblasti působnosti tohoto nařízení, by měly splňovat základní požadavky na kybernetickou bezpečnost stanovené v tomto nařízení. Pokud tyto vysoce rizikové systémy umělé inteligence splňují základní požadavky na kybernetickou bezpečnost stanovené tímto nařízením, mělo by se mít za to, že splňují požadavky na kybernetickou bezpečnost stanovené v článku 15 nařízení (EU) 2024/1689, pokud se na tyto požadavky vztahuje EU prohlášení o shodě nebo jeho části vydané podle tohoto nařízení. Za tímto účelem by se při posuzování kybernetických bezpečnostních rizik, která souvisejí s produktem s digitálními prvky klasifikovaným jako vysoce rizikový systém umělé inteligence podle nařízení (EU) 2024/1689, která je třeba zohlednit ve fázi plánování, návrhu, vývoje, výroby, dodání a údržby tohoto produktu, jak vyžaduje toto nařízení, měla v souladu s nařízením (EU) 2024/1689 zohlednit rizika pro kybernetickou odolnost systému umělé inteligence, pokud jde o pokusy neoprávněných třetích stran změnit jeho použití, chování nebo výkonnost,

([21]) Nařízení Evropského parlamentu a Rady (EU) 2023/988 ze dne 10. května 2023 o obecné bezpečnosti výrobků, o změně nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 a směrnice Evropského parlamentu a Rady (EU) 2020/1828 a o zrušení směrnice Evropského parlamentu a Rady 2001/95/ES a směrnice Rady 87/357/EHS (Úř. věst. L 135, 23.5.2023, s. 1).

([22]) Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci) (Úř. věst. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

včetně zranitelností specifických pro umělou inteligenci, jako je data poisoning nebo nepřátelské útoky, stejně jako příslušná rizika ohrožující základní práva. Pokud jde o postupy posuzování shody týkající se základních požadavků na kybernetickou bezpečnost produktu s digitálními prvky, který spadá do oblasti působnosti tohoto nařízení a který je klasifikován jako vysoce rizikový systém umělé inteligence, měla by se zpravidla namísto příslušných ustanovení tohoto nařízení použít ustanovení článku 43 nařízení (EU) 2024/1689. Toto pravidlo by však nemělo vést ke snížení potřebné míry záruky u důležitých nebo kritických produktů s digitálními prvky uvedených v tomto nařízení. Odchylně od tohoto pravidla by proto vysoce rizikové systémy umělé inteligence, které spadají do oblasti působnosti nařízení (EU) 2024/1689 a jsou rovněž důležité nebo kritické produkty s digitálními prvky uvedené v tomto nařízení a na něž se vztahuje postup posuzování shody založený na interní kontrole podle přílohy VI nařízení (EU) 2024/1689, měly podléhat postupům posuzování shody uvedeným v tomto nařízení, pokud jde o základní požadavky na kybernetickou bezpečnost stanovené v tomto nařízení. V takovém případě by se na všechny ostatní aspekty, na něž se nařízení (EU) 2024/1689 vztahuje, měla použít příslušná ustanovení o posuzování shody, která jsou založena na interní kontrole stanovené v příloze VI uvedeného nařízení.

(52) V zájmu zlepšení bezpečnosti produktů s digitálními prvky uváděných na vnitřní trh je nezbytné stanovit základní požadavky na kybernetickou bezpečnost, které by platily pro tyto produkty. Těmito základními požadavky na kybernetickou bezpečnost by nemělo být dotčeno koordinované posuzování bezpečnostních rizik kritických dodavatelských řetězců na úrovni Unie stanovené v článku 22 směrnice (EU) 2022/2555, při němž se zohledňují technické i případně i jiné než technické rizikové faktory, například nepatřičný vliv třetí země na dodavatele. Dále by jimi neměla být dotčena výsada členských států stanovit dodatečné požadavky, které by zohledňovaly jiné než technické faktory za účelem zajištění vysoké úrovně odolnosti, včetně požadavků stanovených v doporučení Komise (EU) 2019/534 ([23]), v posouzení rizik kybernetické bezpečnosti sítí 5G koordinovaném na úrovni EU a v souboru opatření EU pro kybernetickou bezpečnost sítí 5G, na němž se dohodla skupina pro spolupráci zřízená podle článku 14 směrnice (EU) 2022/2555.

(53) Výrobci produktů spadajících do oblasti působnosti nařízení Evropského parlamentu a Rady (EU) 2023/1230 ([24]), které jsou rovněž produkty s digitálními prvky definovanými v tomto nařízení, by měli splňovat základní požadavky na kybernetickou bezpečnost stanovené v tomto nařízení i základní požadavky na ochranu zdraví a bezpečnost stanovené v nařízení (EU) 2023/1230. Základní požadavky na kybernetickou bezpečnost stanovené v tomto nařízení a některé základní požadavky stanovené v nařízení (EU) 2023/1230 mohou řešit podobná kybernetická bezpečnostní rizika. Soulad se základními požadavky na kybernetickou bezpečnost stanovenými v tomto nařízení by proto mohl usnadnit dodržování základních požadavků, které se vztahují rovněž na určitá kybernetická bezpečnostní rizika, stanovených v nařízení (EU) 2023/1230, a to zejména těch, které se týkají ochrany před poškozením a bezpečnosti a spolehlivosti ovládacích systémů podle oddílu 1.1.9 a 1.2.1 přílohy III uvedeného nařízení. Tento soulad musí výrobce prokázat například použitím harmonizovaných norem nebo jiných technických specifikací, které se vztahují na příslušné základní požadavky na kybernetickou bezpečnost, jsou-li k dispozici, a to na základě posouzení rizik, které se těchto kybernetických bezpečnostních rizik týká. Výrobce by měl dodržet také příslušné postupy posuzování shody stanovené v tomto nařízení a v nařízení (EU) 2023/1230. Komise a evropské normalizační organizace by v rámci přípravných prací na podporu uplatňování tohoto nařízení a nařízení (EU) 2023/1230 a souvisejících normalizačních procesů měly podporovat důslednost, pokud jde o způsob posuzování kybernetických bezpečnostních rizik a způsob, jakým se mají na tato rizika vztahovat harmonizované normy, pokud jde o příslušné základní požadavky. Komise a evropské normalizační organizace by zejména měly zohlednit toto nařízení při přípravě a vypracovávání harmonizovaných norem s cílem usnadnit uplatňování nařízení (EU) 2023/1230, především pokud jde o aspekty kybernetické bezpečnosti týkající se ochrany před poškozením a bezpečnosti a spolehlivosti ovládacích systémů podle oddílu 1.1.9 a 1.2.1 přílohy III uvedeného nařízení. Komise by měla poskytnout pokyny na podporu výrobců, na něž se vztahuje toto nařízení a také nařízení (EU) 2023/1230, zejména s cílem usnadnit prokázání souladu s příslušnými základními požadavky stanovenými v tomto nařízení a v nařízení (EU) 2023/1230.

(54) Aby bylo zajištěno, že produkty s digitálními prvky jsou bezpečné v době jejich uvedení na trh i po celou dobu, po kterou se předpokládá jejich používání, je nezbytné stanovit základní požadavky na kybernetickou bezpečnost na řešení zranitelností a základní požadavky na kybernetickou bezpečnost týkající se vlastností produktů s digitálními prvky. Výrobci by měli splňovat všechny základní požadavky na kybernetickou bezpečnost týkající se řešení

([23]) Doporučení Komise (EU) 2019/534 ze dne 26. března 2019 Kybernetická bezpečnost sítí 5G (Úř. věst. L 88, 29.3.2019, s. 42).
([24]) Nařízení Evropského parlamentu a Rady (EU) 2023/1230 ze dne 14. června 2023 o strojních zařízeních a o zrušení směrnice Evropského parlamentu a Rady 2006/42/ES a směrnice Rady 73/361/EHS (Úř. věst. L 165, 29.6.2023, s. 1).

zranitelností po celou dobu podpory, měli by však určit, které další základní požadavky na kybernetickou bezpečnost týkající se vlastností produktu jsou pro dotčený druh produktu s digitálními prvky relevantní. Za tímto účelem by výrobci měli provést posouzení kybernetických bezpečnostních rizik spojených s produktem s digitálními prvky s cílem určit příslušná rizika a příslušné základní požadavky na kybernetickou bezpečnost, aby mohli zpřístupnit své produkty s digitálními prvky bez známých zneužitelných zranitelností, které by mohly mít dopad na bezpečnost těchto produktů, a náležitě uplatňovat vhodné harmonizované normy, společné specifikace či evropské nebo mezinárodní normy.

(55) Pokud se na produkt s digitálními prvky nevztahují určité základní požadavky na kybernetickou bezpečnost, měl by výrobce zahrnout do posouzení kybernetických bezpečnostních rizik uvedeného v technické dokumentaci jasné odůvodnění. Tak by tomu mohlo být v případě, kdy je základní požadavek na kybernetickou bezpečnost neslučitelný s povahou produktu s digitálními prvky. Například zamýšlený účel produktu s digitálními prvky může vyžadovat, aby se výrobce řídil obecně uznávanými normami interoperability, i když jeho bezpečnostní prvky již nejsou považovány za nejmodernější. Podobně další právo Unie vyžaduje, aby výrobci uplatňovali zvláštní požadavky na interoperabilitu. Pokud se základní požadavek na kybernetickou bezpečnost produktu s digitálními prvky nevztahuje, ale výrobce zjistil ve vztahu k tomuto základnímu požadavku na kybernetickou bezpečnost nějaká kybernetická bezpečnostní rizika, měl by přijmout opatření k řešení těchto rizik jinými prostředky, například tak, že omezí zamýšlený účel produktu na důvěryhodné prostředí nebo o těchto rizicích informuje uživatele.

(56) Jedním z nejdůležitějších opatření, která by měli uživatelé přijmout na ochranu svých produktů s digitálními prvky před kybernetickými útoky, je co nejdříve si nainstalovat nejnovější dostupné bezpečnostní aktualizace. Výrobci by proto měli navrhovat své produkty tak, aby zajistili, aby produkty s digitálními prvky zahrnovaly funkce, které by umožnily automatické oznamování, distribuci, stahování a instalaci bezpečnostních aktualizací, zejména v případě spotřebitelských produktů, a měly by za tímto účelem zavést příslušné postupy. Měli by rovněž nabízet možnost přijmout stažení a instalaci bezpečnostních aktualizací jako poslední krok. Uživatelé by měli mít nadále možnost automatické aktualizace deaktivovat, a to prostřednictvím jasného a snadno použitelného mechanismu, který by byl doplněn o jasné pokyny, jak mohou uživatelé automatické aktualizace zakázat. Požadavky týkající se automatických aktualizací stanovené v příloze tohoto nařízení se nevztahují na produkty s digitálními prvky, které jsou primárně určeny k tomu, aby byly začleněny do jiných produktů jako jejich komponenty. Nevztahují se ani na produkty s digitálními prvky, u nichž uživatelé důvodně neočekávají automatické aktualizace, včetně produktů s digitálními prvky, které mají být použity v profesionálních sítích IKT, a zejména v kritickém a průmyslovém prostředí, kde by automatická aktualizace mohla narušit provoz. Bez ohledu na to, zda je produkt s digitálními prvky navržen tak, aby přijímal automatické aktualizace, či nikoli, měl by jeho výrobce uživatele informovat o zranitelnostech a bezodkladně zpřístupnit bezpečnostní aktualizace. Pokud má produkt s digitálními prvky uživatelské rozhraní nebo podobné technické prostředky umožňující přímou interakci s jeho uživateli, měl by výrobce tyto prvky použít k informování uživatelů o tom, že jejich produkt s digitálními prvky dosáhl konce doby podpory. Oznámení by se mělo omezit na informace nezbytné k jeho pochopení, a nemělo by mít negativní dopad na zkušenost uživatele s produktem s digitálními prvky.

(57) Aby se zvýšila transparentnost postupů řešení zranitelností a zajistilo, že uživatelé nebudou povinni instalovat nové aktualizace funkcí pouze proto, aby získali nejnovější bezpečnostní aktualizace, měli by výrobci zajistit, je-li to technicky možné, aby nové bezpečnostní aktualizace byly poskytovány odděleně od aktualizací funkcí.

(58) Ve společném sdělení Komise a vysokého představitele Unie pro zahraniční věci a bezpečnostní politiku ze dne 20. června 2023 nazvaném „Strategie evropské hospodářské bezpečnosti“ se uvádí, že Unie musí maximalizovat přínosy své hospodářské otevřenosti a zároveň minimalizovat rizika vyplývající z hospodářské závislosti na vysoce rizikových prodejcích, a to prostřednictvím společného strategického rámce pro hospodářskou bezpečnost Unie. Závislost na vysoce rizikových dodavatelích produktů s digitálními prvky může představovat strategické riziko, kterým je třeba se zabývat na úrovni Unie, zejména pokud jsou tyto produkty s digitálními prvky určeny k použití základními subjekty uvedenými v čl. 3 odst. 1 směrnice (EU) 2022/2555. Tato rizika mohou být spojena mimo jiné s jurisdikcí rozhodnou pro daného výrobce, s povahou jeho podnikového vlastnictví a s řídícími vazbami na vládu třetí země, pokud tato vazba existuje, zejména pokud se daná třetí země podílí na hospodářské špionáži nebo nezodpovědném chování státu v kyberprostoru a její právní předpisy umožňují svévolný přístup k veškerým operacím společnosti či údajům, včetně obchodně citlivých údajů, a mohou ukládat povinnosti pro účely zpravodajství bez demokratického systému brzd a protivah, mechanismů dohledu, spravedlivého řízení nebo práva na odvolání k nezávislému soudu. Při určování významu kybernetického bezpečnostního rizika ve smyslu tohoto nařízení by Komise a orgány dozoru nad trhem měly v souladu se svými povinnostmi stanovenými v tomto nařízení

zohlednit také jiné než technické rizikové faktory, zejména ty, které byly stanoveny na základě koordinovaného posouzení bezpečnostních rizik kritických dodavatelských řetězců na úrovni Unie provedeného v souladu s článkem 22 směrnice (EU) 2022/2555.

(59) Za účelem zajištění bezpečnosti produktů s digitálními prvky po jejich uvedení na trh by výrobci měli stanovit dobu podpory, které by měla zohledňovat očekávanou dobu používání produktu s digitálními prvky. Při stanovování doby podpory by měl výrobce přihlížet zejména k přiměřeným očekáváním uživatelů, povaze produktu a k příslušnému právu Unie, které určuje životnost produktů s digitálními prvky. Výrobci by měli mít rovněž možnost zohlednit další relevantní faktory. Kritéria by měla být uplatňována takovým způsobem, aby byla zajištěna proporcionalita při stanovování doby podpory. Výrobce by měl na žádost poskytnout orgánům dozoru nad trhem informace, ke kterým přihlížel při stanovování doby podpory u produktu s digitálními prvky.

(60) Doba podpory, po kterou výrobce zajišťuje účinné řešení zranitelností, by neměla být kratší než pět let, pokud není životnost produktu s digitálními prvky kratší než pět let; v takovém případě by měl výrobce zajistit řešení zranitelností po dobu jeho životnosti. Pokud je očekávaná doba používání produktu s digitálními prvky delší než pět let, jako je tomu často v případě hardwarových komponent, jako jsou základní desky nebo mikroprocesory, síťových zařízení, jako jsou směrovače, modemy nebo přepínače, a u softwaru jako jsou operační systémy nebo nástroje pro úpravu videa, měli by výrobci zajistit delší dobu podpory. Po výrazně delší dobu se často používají zejména produkty s digitálními prvky určené k použití v průmyslovém prostředí, jako jsou průmyslové řídicí systémy. Výrobce by měl mít možnost stanovit dobu podpory kratší než pět let pouze tehdy, odůvodňuje-li to povaha daného produktu s digitálními prvky a pokud se očekává, že se tento produkt bude používat po dobu kratší než pět let, přičemž v takovém případě by doba podpory měla odpovídat očekávané době použití. Například životnost aplikace pro dohledávání kontaktů určená k použití během pandemie by mohla být omezena na dobu trvání pandemie. Některé softwarové aplikace mohou být navíc ze své podstaty zpřístupněny pouze na základě předplatného, zejména pokud se aplikace po uplynutí doby předplatného stane pro uživatele nedostupnou, a proto se již nepoužívá.

(61) Pokud produkty s digitálními prvky dosáhnou konce doby podpory, měli by výrobci zvážit uvolnění zdrojového kódu těchto produktů s digitálními prvky buď jiným podnikům, které se zaváží, že budou dále poskytovat služby spojené s řešením zranitelností, nebo veřejnosti, aby se zajistilo, že zranitelnosti budou moci být řešeny i po skončení doby podpory. V případě, že výrobci zpřístupní zdrojový kód jiným podnikům, měli by mít možnost chránit vlastnictví produktu s digitálními prvky a zabránit veřejnému šíření zdrojového kódu, například prostřednictvím smluvních ujednání.

(62) Aby se zajistilo, že výrobci v celé Unii budou pro srovnatelné produkty s digitálními prvky stanovovat podobné doby podpory, měla by specializovaná skupina pro správní spolupráci zveřejňovat statistiky o průměrné době podpory stanovené výrobci pro různé kategorie produktů s digitálními prvky a vydávat pokyny uvádějící vhodné doby podpory pro tyto kategorie. Komise měla mít v zájmu zajištění harmonizovaného přístupu na celém vnitřním trhu navíc možnost přijímat akty v přenesené pravomoci za účelem stanovení minimální doby podpory pro konkrétní kategorie produktů, pokud z údajů poskytnutých orgány dozoru nad trhem vyplývá, že doba podpory stanovená výrobci buď není systematicky v souladu s kritérii pro stanovení doby podpory uvedenými v tomto nařízení, nebo že výrobci v různých členských státech bezdůvodně stanovují různé doby podpory.

(63) Výrobci by měli zřídit jednotné kontaktní místo, které uživatelům umožní snadno s nimi komunikovat, a to i za účelem nahlašování zranitelností produktů s digitálním prvkem a přijímání informací o nich. Měli by zajistit snadný přístup uživatelů k jednotnému kontaktnímu místu, jasně uvést jeho dostupnost a tyto informace pravidelně aktualizovat. Pokud se výrobci rozhodnou nabízet automatizované nástroje, například chatovací box, měli by rovněž uvést telefonní číslo nebo jiné digitální kontaktní údaje, jako je e-mailová adresa či kontaktní formulář. Jednotné kontaktní místo by nemělo záviset výhradně na automatizovaných nástrojích.

(64) Výrobci by měli své produkty s digitálními prvky dodávat na trh se standardně bezpečnou konfigurací a poskytovat uživatelům bezplatné bezpečnostní aktualizace. Výrobci by měli mít možnost odchýlit se od těchto základních požadavků na kybernetickou bezpečnost pouze ve vztahu k individuálně uzpůsobeným výrobkům, které jsou určeny pro konkrétního podnikatelského uživatele za konkrétním účelem a u nichž se výrobce s uživatelem výslovně dohodl na jiných smluvních podmínkách.

(65) Výrobci by měli prostřednictvím jednotné platformy pro podávání zpráv oznámit aktivně zneužívané zranitelnosti produktů s digitálními prvky a závažné incidenty, které mají dopad na bezpečnost těchto produktů, současně jak týmu pro reakce na počítačové bezpečnostní incidenty (CSIRT) určenému jako koordinátor, tak i agentuře ENISA. Tato oznámení by měla být podávána prostřednictvím koncového bodu elektronického oznamování týmu CSIRT určeného jako koordinátor a měla by být současně přístupná agentuře ENISA.

(66) Výrobci by měli oznamovat aktivně zneužívané zranitelnosti s cílem zajistit, aby týmy CSIRT určené jako koordinátoři a agentura ENISA měly o těchto zranitelnostech náležitý přehled a aby jim byly poskytovány informace nezbytné k plnění jejich úkolů stanovených ve směrnici (EU) 2022/2555 a ke zvýšení celkové úrovně kybernetické bezpečnosti základních a důležitých subjektů uvedených v článku 3 uvedené směrnice, a aby se zajistilo účinné fungování orgánů dozoru nad trhem. Vzhledem k tomu, že většina produktů s digitálními prvky je nabízena na celém vnitřním trhu, jakákoli zneužívaná zranitelnost produktu s digitálními prvky by měla být považována za hrozbu pro fungování vnitřního trhu. Agentura ENISA by měla po dohodě s výrobcem zveřejnit opravené zranitelnosti v evropské databázi zranitelností zřízené podle čl. 12 odst. 2 směrnice (EU) 2022/2555. Evropská databáze zranitelností výrobcům pomůže při odhalování známých zneužitelných zranitelností jejich produktů, aby se zajistilo, že na trh budou dodávány bezpečné produkty.

(67) Výrobci by rovněž měli týmu CSIRT určenému jako koordinátor a agentuře ENISA oznámit každý závažný incident, který má dopad na bezpečnost produktu s digitálními prvky. S cílem zajistit, aby uživatelé mohli rychle reagovat na závažné incidenty, které mají dopad na bezpečnost jejich produktů s digitálními prvky, by výrobci měli rovněž informovat uživatele o každém takovém incidentu a případně o veškerých nápravných opatřeních, která mohou uživatelé zavést za účelem zmírnění dopadu incidentu, například zveřejněním příslušných informací na svých internetových stránkách nebo v případech, kdy je výrobce schopen kontaktovat uživatele a je-li to odůvodněno kybernetickými bezpečnostními riziky, tím, že se obrátí přímo na uživatele.

(68) Aktivně zneužívané zranitelnosti se týkají případů, kdy výrobce zjistí, že došlo k narušení bezpečnosti, které se dotýká jeho uživatelů nebo jiné fyzické či právnické osoby a které způsobil škodlivý aktér, jenž využil chybu v jednom z produktů s digitálními prvky dodaných výrobcem na trh. Příkladem těchto zranitelností by mohly být slabiny ve funkci identifikace a autentizace u produktu. Povinné oznamování by se nemělo vztahovat na zranitelnosti, které jsou zjištěny bez škodlivého záměru za účelem testování, vyšetřování, opravy nebo zveřejnění v dobré víře s cílem podpořit zabezpečení nebo bezpečnost vlastníka systému a jeho uživatelů. Na druhé straně, závažné incidenty, které mají dopad na bezpečnost produktu s digitálními prvky, se týkají situací, kdy se incident související s kybernetickou bezpečností týká postupů výrobce v oblasti vývoje, výroby nebo údržby takovým způsobem, že by mohl vést k vyššímu kybernetickému bezpečnostnímu riziku pro uživatele nebo jiné osoby. Mezi tyto závažné incidenty by mohla patřit situace, kdy se útočníkovi podařilo do kanálu, jehož prostřednictvím výrobce vydává bezpečnostní aktualizace pro uživatele, úspěšně zavést škodlivý kód.

(69) Aby se zajistilo rychlé rozesílání oznámení všem příslušným týmům CSIRT určeným jako koordinátoři a aby výrobci mohli v každé fázi postupu oznamování podávat jediné oznámení, měla by agentura ENISA zřídit jednotnou platformu pro podávání zpráv s vnitrostátními koncovými body elektronického oznamování. Každodenní provoz této jednotné platformy pro podávání zpráv by měla řídit a udržovat agentura ENISA. Týmy CSIRT určené jako koordinátoři by měly o oznámených zranitelnostech nebo incidentech informovat své příslušné orgány dozoru nad trhem. Jednotná platforma pro podávání zpráv by měla být navržena tak, aby zajišťovala důvěrnost oznámení, zejména pokud jde o zranitelnosti, u nichž ještě není k dispozici bezpečnostní aktualizace. Kromě toho by agentura ENISA měla zavést postupy pro bezpečné a důvěrné nakládání s informacemi. Na základě shromážděných informací by agentura ENISA měla každé dva roky vypracovat technickou zprávu o nových trendech týkajících se kybernetických bezpečnostních rizik u produktů s digitálními prvky a předložit ji skupině pro spolupráci zřízené podle článku 14 směrnice (EU) 2022/2555.

(70) Za výjimečných okolností, a zejména na žádost výrobce by tým CSIRT určený jako koordinátor, který obdržel prvotní oznámení, měl mít možnost rozhodnout o tom, že na nezbytně nutnou dobu odloží jeho zaslání ostatním příslušným týmům CSIRT určeným jako koordinátoři prostřednictvím jednotné platformy pro podávání zpráv, pokud to lze odůvodnit s ohledem na kybernetickou bezpečnost. Tým CSIRT určený jako koordinátor by měl agenturu ENISA neprodleně informovat o rozhodnutí o odkladu a jeho důvodech, jakož i o tom, kdy má v úmyslu předat příslušné informace dále. Komise by měla prostřednictvím aktu v přenesené pravomoci specifikovat podmínky, za nichž by bylo možné uplatnit důvody související s kybernetickou bezpečností, přičemž by při přípravě návrhu aktu v přenesené pravomoci měla spolupracovat se sítí týmů CSIRT zřízenou podle článku 15 směrnice (EU) 2022/2555 (síť CSIRT) a agenturou ENISA. Mezi příklady důvodů souvisejících s kybernetickou bezpečností patří probíhající postup koordinovaného zveřejňování zranitelností nebo situace, kdy se očekává, že výrobce v brzké době zajistí zmírňující opatření, a kdy kybernetická bezpečnostní rizika spojená s okamžitým poskytnutím příslušných informací prostřednictvím jednotné platformy pro podávání zpráv převažují nad jeho přínosy. Agentura ENISA by

na základě informací, které od týmu CSIRT určeného jako koordinátor obdržela ohledně rozhodnutí odložit poskytnutí příslušných informací z důvodů zajištění kybernetické bezpečnosti, pokud o to tento tým požádá, měla mít možnost podpořit jej na základě poskytnutých důvodů při odkladu rozesílání oznámení na. Kromě toho by za zvláště výjimečných okolností neměla agentura ENISA získat veškeré podrobné informace o oznámení aktivně zneužívané zranitelnosti současně. Tak by tomu bylo v případě, kdy výrobce ve svém oznámení uvede, že oznámená zranitelnost je aktivně zneužívána škodlivým aktérem a že podle dostupných informací není zneužívána v žádném jiném členském státě než v členském státě týmu CSIRT určeného jako koordinátor, jemuž výrobce zranitelnost oznámil, pokud by jakékoli okamžité další předávání informací o oznámené zranitelnosti pravděpodobně vedlo k poskytnutí takových informací, jejichž zveřejnění by bylo v rozporu se zásadními zájmy tohoto členského státu, nebo pokud z dalšího poskytování informací o oznámené zranitelnosti vyplývá vysoké bezprostřední kybernetické bezpečnostní riziko. V takových případech obdrží agentura ENISA současně pouze přístup k informacím o tom, že výrobce učinil oznámení, k obecným informacím o daném produktu s digitálními prvky, k informacím o obecné povaze zneužití a k informacím o tom, že výrobce uplatnil bezpečnostní důvody, a proto jí byl odepřen přístup k úplnému obsahu oznámení. Úplné oznámení by pak mělo být zpřístupněno agentuře ENISA a dalším příslušným týmům CSIRT určeným jako koordinátoři, jakmile tým CSIRT určený jako koordinátor, který obdržel prvotní oznámení, sezná, že tyto bezpečnostní důvody, které zohledňují zvláště výjimečné okolnosti stanovené v tomto nařízení, pominuly. Pokud se agentura ENISA na základě dostupných informací domnívá, že existuje systémové riziko ovlivňující bezpečnost na vnitřním trhu, měla by týmu CSIRT, který oznámení obdržel, doporučit, aby ostatním týmům CSIRT určeným jako koordinátoři i samotné agentuře ENISA poskytl úplné oznámení.

(71) Pokud výrobci oznámí aktivně zneužívanou zranitelnost nebo závažný incident, který má dopad na bezpečnost produktu s digitálními prvky, měli by uvést, jak citlivé jsou podle nich oznámené informace. Tým CSIRT určený jako koordinátor, který obdržel prvotní oznámení, by měl tyto informace zohlednit při posuzování, zda se při oznámení uplatní výjimečné okolnosti, které jsou důvodem ke zpoždění při předávání informací o oznámení ostatním příslušným týmům CSIRT určeným jako koordinátoři na odůvodněném základě souvisejícím s kybernetickou bezpečností. Tyto informace by měl zohlednit rovněž při posuzování, zda se v případě oznámení aktivně zneužívané zranitelnosti uplatní obzvláště výjimečné okolnosti, které odůvodní, že není úplné oznámení současně poskytnuto agentuře ENISA. Týmy CSIRT určené jako koordinátoři by měly mít možnost tuto informaci zohlednit při určování vhodných opatření ke zmírnění rizik vyplývajících z těchto zranitelností a incidentů.

(72) Za účelem zjednodušení oznamování informací požadovaných podle tohoto nařízení a s ohledem na další doplňkové požadavky na podávání zpráv stanovené v právu Unie, jako je nařízení (EU) 2016/679, nařízení Evropského parlamentu a Rady (EU) 2022/2554 ([25]), směrnice Evropského parlamentu a Rady 2002/58/ES ([26]) a směrnice (EU) 2022/2555 a za účelem snížení administrativní zátěže subjektů se členským státům se doporučuje, aby zvážily vytvoření jednotných kontaktních míst pro oznamování těchto informací na národní úrovni. Používáním těchto vnitrostátních jednotných kontaktních míst pro nahlašování bezpečnostních incidentů podle nařízení (EU) 2016/679 a směrnice 2002/58/ES by nemělo být dotčeno uplatňování ustanovení nařízení (EU) 2016/679 a směrnice 2002/58/ES, zejména těch ustanovení, která se týkají nezávislosti orgánů v nich uvedených. Při zřizování jednotné platformy pro podávání zpráv uvedené v tomto nařízení by agentura ENISA měla zohlednit možnost začlenit vnitrostátní koncové body elektronického oznamování uvedené v tomto nařízení do vnitrostátních jednotných kontaktních míst, kde by mohlo být možné podávat i další oznámení požadovaná podle práva Unie.

(73) Při zřizování jednotné platformy pro podávání zpráv uvedené v tomto nařízení a s cílem využít zkušeností z minulosti by agentura ENISA měla vést konzultace s dalšími orgány nebo subjekty Unie, které spravují platformy nebo databáze podléhající přísným bezpečnostním požadavkům, jako je Agentura Evropské unie pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva (eu-LISA). Agentura ENISA by měla také analyzovat potenciální doplňkovost s evropskou databází zranitelností zřízenou podle čl. 12 odst. 2 směrnice (EU) 2022/2555.

(74) Výrobci i jiné fyzické a právnické osoby by měli mít možnost dobrovolně oznámit týmu CSIRT určenému jako koordinátor nebo agentuře ENISA každou zranitelnost produktu s digitálními prvky, kybernetické hrozby, které by

([25]) Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011 (Úř. věst. L 333, 27.12.2022, s. 1).

([26]) Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Úř. věst. L 201, 31.7.2002, s. 37).

mohly ovlivnit rizikový profil produktu s digitálními prvky, každý incident, který má dopad na bezpečnost produktu s digitálními prvky, i významné události, které téměř vedly k takovému incidentu.

(75) Členské státy měly usilovat o to, aby se v souladu s vnitrostátním právem v co největší míře zabývaly výzvami, jimž čelí výzkumní pracovníci zabývající se problematikou zranitelnosti, a to i pokud jde o jejich možnou trestní odpovědnost. Vzhledem k tomu, že fyzické a právnické osoby, které se zabývají výzkumem zranitelností, by v některých členských státech mohly podléhat trestní a občanskoprávní odpovědnosti, doporučuje se členským státům, aby přijaly pokyny týkající se nemožnosti stíhat výzkumné pracovníky zabývající se bezpečností informací a vyloučení vzniku občanskoprávní odpovědnosti v souvislosti s jejich činností.

(76) Výrobci produktů s digitálními prvky by měli zavést politiky koordinovaného zveřejňování zranitelností s cílem usnadnit jednotlivcům nebo subjektům oznamování zranitelností, a to buď přímo výrobci, nebo nepřímo, a požádají-li o to, anonymně, prostřednictvím týmů CSIRT určených jako koordinátoři pro účely koordinovaného zveřejňování zranitelností v souladu s čl. 12 odst. 1 směrnice (EU) 2022/2555. Politika výrobců v oblasti koordinovaného zveřejňování zranitelností by měla specifikovat strukturovaný proces, jehož prostřednictvím jsou zranitelná místa hlášena výrobcům takovým způsobem, který výrobci umožní diagnostikovat a odstranit tyto zranitelnosti dříve, než budou podrobné informace o nich sděleny třetím stranám nebo veřejnosti. Výrobci by navíc měli zvážit zveřejnění své bezpečnostní politiky ve strojově čitelném formátu. Vzhledem k tomu, že informace o zneužitelných zranitelnostech široce používaných produktů s digitálními prvky lze na černém trhu prodávat za vysoké ceny, měli by mít výrobci těchto produktů možnost využívat v rámci své politiky koordinovaného zveřejňování zranitelností programy motivující k oznamování zranitelností, které zajistí, že jednotlivci nebo subjekty získají za svou snahu uznání a odměnu. Jedná se o takzvaný „program odměn za nalezení chyb“ (*bug bounty programmes*).

(77) Aby se usnadnila analýza zranitelností, měli by výrobci zjistit a zdokumentovat komponenty obsažené v produktech s digitálními prvky, mimo jiné vypracováním softwarového kusovníku. Softwarový kusovník může poskytnout těm, kdo software vyrábějí, nakupují a provozují, informace, které jim umožní lépe pochopit dodavatelský řetězec, což má řadu výhod, zejména to pomáhá výrobcům a uživatelům při vyhledávání známých nově se objevujících zranitelností a kybernetických bezpečnostních rizik. Pro výrobce je obzvláště důležité zajistit, aby jejich produkty s digitálními prvky neobsahovaly zranitelné komponenty vyvinuté třetími stranami. Výrobci by neměli mít povinnost softwarový kusovník zveřejnit.

(78) V nových složitých obchodních modelech spojených s online prodejem může podnik působící online poskytovat různé služby. V závislosti na povaze služeb, které poskytuje v souvislosti s daným produktem s digitálními prvky, může tentýž subjekt spadat do různých kategorií obchodních modelů nebo hospodářských subjektů. Pokud daný subjekt poskytuje v souvislosti s produktem s digitálními prvky výlučně zprostředkovatelské služby online a je pouze poskytovatelem online tržiště ve smyslu definice uvedené v čl. 3 bodě 14 nařízení (EU) 2023/988, nepovažuje se za některý z druhů hospodářských subjektů ve smyslu definice uvedené v tomto nařízení. Pokud je tentýž subjekt poskytovatelem online tržiště a působí v případě prodeje produktů s digitálními prvky rovněž jako hospodářský subjekt ve smyslu tohoto nařízení, měly by se na něj vztahovat povinnosti stanovené v tomto nařízení pro tento typ hospodářských subjektů. Pokud například poskytovatel online tržiště rovněž produkt s digitálními prvky distribuuje, pak by byl v souvislosti s prodejem tohoto výrobku považován za distributora. Podobně pokud by dotčený subjekt prodával produkty s digitálními prvky pod svou vlastní značkou, považoval by se za výrobce, a proto by musel splňovat požadavky uplatňující se na výrobce. Některé subjekty mohou být rovněž považovány za poskytovatele služeb kompletního vyřízení objednávek ve smyslu čl. 3 bodu 11 nařízení Evropského parlamentu a Rady (EU) 2019/1020 ([27]), pokud takové služby nabízejí. Takové případy je třeba posuzovat individuálně. Vzhledem k tomu, že online tržiště mají zásadní význam z hlediska elektronického obchodování, měla by usilovat o spolupráci s orgány dozoru nad trhem členských států, aby pomohla zajistit soulad produktů s digitálními prvky zakoupených na online tržištích s požadavky na kybernetickou bezpečnost stanovenými v tomto nařízení.

(79) Aby se usnadnilo posuzování shody s požadavky stanovenými v tomto nařízení, měl by se uplatňovat předpoklad shody u produktů s digitálními prvky, které splňují harmonizované normy převádějící základní požadavky na kybernetickou bezpečnost stanovené v tomto nařízení do podrobných technických specifikací a které jsou přijaty

([27]) 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 (Úř. věst. L 169, 25.6.2019, s. 1).

v souladu s nařízením Evropského parlamentu a Rady (EU) č. 1025/2012 ([28]). V uvedeném nařízení je stanoven postup pro námitky proti harmonizovaným normám, pokud tyto normy nesplňují požadavky stanovené v tomto nařízení v plné míře. Proces normalizace by měl zajišťovat vyvážené zastoupení zájmů a účinnou účast zúčastněných stran z občanské společnosti, včetně spotřebitelských organizací. Aby se usnadnilo vypracování harmonizovaných norem a uplatňování tohoto nařízení, jakož i jeho dodržování ze strany společností, zejména mikropodniků a malých a středních podniků a podniků působících na celém světě, měly by být zohledněny rovněž mezinárodní normy, které jsou v souladu s takovou úrovní ochrany kybernetické bezpečnosti, na kterou cílí základní požadavky na kybernetickou bezpečnost stanovené v tomto nařízení.

(80) Pro účinné uplatňování tohoto nařízení bude obzvláště důležité včasné vypracování harmonizovaných norem během přechodného období pro uplatňování tohoto nařízení a zajištění jejich dostupnosti před datem použitelnosti tohoto nařízení. To se týká zejména důležitých produktů s digitálními prvky, které spadají do třídy I. Dostupnost harmonizovaných norem umožní výrobcům těchto produktů použít k provedení posouzení shody postup interní kontroly, což umožní zabránit překážkám a průtahům v činnosti subjektů posuzování shody.

(81) Nařízení (EU) 2019/881 stanoví dobrovolný evropský rámec pro certifikaci kybernetické bezpečnosti pro produkty IKT, procesy IKT a služby IKT. Evropská schémata certifikace kybernetické bezpečnosti poskytují společný rámec důvěry pro uživatele, kteří používají produkty s digitálními prvky, jež spadají do působnosti tohoto nařízení. Toto nařízení by proto mělo vytvářet součinnost s nařízením (EU) 2019/881. S cílem usnadnit posuzování shody s požadavky stanovenými v tomto nařízení se předpokládá, že produkty s digitálními prvky, které jsou certifikovány nebo pro něž bylo vydáno prohlášení o shodě v rámci evropského schématu kybernetické bezpečnosti podle nařízení (EU) 2019/881, které Komise určila v prováděcím aktu, jsou v souladu se základními požadavky na kybernetickou bezpečnost stanovenými v tomto nařízení, pokud se na tyto požadavky vztahuje evropský certifikát kybernetické bezpečnosti nebo prohlášení o shodě či jeho části. Potřeba nových evropských schémat certifikace kybernetické bezpečnosti pro produkty s digitálními prvky by měla být posuzována s ohledem na toto nařízení, a to i při přípravě průběžného pracovního programu Unie v souladu s nařízením (EU) 2019/881. Pokud je třeba zavést nové schéma zahrnující produkty s digitálními prvky, například proto, aby se usnadnilo plnění ustanovení tohoto nařízení, může Komise v souladu s článkem 48 nařízení (EU) 2019/881 požádat agenturu ENISA, aby připravila návrhy takových schémat. Tato budoucí evropská schémata certifikace kybernetické bezpečnosti týkající se produktů s digitálními prvky by měla zohledňovat základní požadavky na kybernetickou bezpečnost a postupy posuzování shody stanovené v tomto nařízení a usnadňovat s ním soulad. U evropských schémat certifikace kybernetické bezpečnosti, která vstoupí v platnost před vstupem tohoto nařízení v platnost, mohou být zapotřebí další specifikace podrobných aspektů toho, jak lze uplatnit předpoklad shody. Komise by měla být zmocněna k tomu, aby prostřednictvím aktů v přenesené pravomoci upřesnila, za jakých podmínek je možné použít evropská schémata certifikace v oblasti kybernetické bezpečnosti k prokázání shody se základními požadavky na kybernetickou bezpečnost stanovenými v tomto nařízení. Aby se zabránilo nepřiměřené administrativní zátěži, neměla by existovat žádná povinnost výrobců nechat si provést posouzení shody třetí stranou, jak je pro příslušné požadavky stanoveno v tomto nařízení, pokud byl evropský certifikát kybernetické bezpečnosti vydán v rámci těchto evropských schémat certifikace kybernetické bezpečnosti alespoň na úrovni „významná“.

(82) Poté, co prováděcí nařízení (EU) 2024/482, jež se týká produktů, které spadají do působnosti tohoto nařízení, například hardwarových bezpečnostních modulů a mikroprocesorů, vstoupí v platnost, by měla mít Komise možnost prostřednictvím aktu v přenesené pravomoci upřesnit, jak EUCC zakládá předpoklad shody se základními požadavky na kybernetickou bezpečnost stanovenými v tomto nařízení nebo jejich části. V tomto aktu v přenesené pravomoci může být dále upřesněno, jakým způsobem certifikát vydaný v rámci EUCC ruší povinnost výrobců nechat si provést posouzení třetí stranou, jak je požadováno podle tohoto nařízení pro příslušné požadavky.

(83) Stávající normalizační rámec EU, který je založen na zásadách nového přístupu stanovených v usnesení Rady ze dne 7. května 1985 o novém přístupu k technické harmonizaci a normám a na nařízení (EU) č. 1025/2012, představuje standardní rámec pro vypracování norem, které zakládají předpoklad shody s příslušnými základními požadavky na kybernetickou bezpečnost stanovenými v tomto nařízení. Evropské normy by se měly řídit trhem, měly by zohledňovat veřejný zájem a politické cíle jasně uvedené v žádosti Komise adresované jedné nebo více evropským normalizačním organizacím, aby ve stanovené lhůtě vypracovaly harmonizované normy, a měly by být založeny na konsensu. Pokud však příslušné odkazy na harmonizované normy neexistují, měla by být Komisi svěřena pravomoc

([28]) Nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 ze dne 25. října 2012 o evropské normalizaci, změně směrnic Rady 89/686/EHS a 93/15/EHS a směrnic Evropského parlamentu a Rady 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES a 2009/105/ES, a kterým se ruší rozhodnutí Rady 87/95/EHS a rozhodnutí Evropského parlamentu a Rady č. 1673/2006/ES (Úř. věst. L 316, 14.11.2012, s. 12).

přijímat prováděcí akty, kterými se stanoví společné specifikace pro základní požadavky na kybernetickou bezpečnost obsažené v tomto nařízení, za předpokladu, že přitom bude řádně respektovat úlohu a funkce evropských normalizačních organizací, přičemž půjde o výjimečné náhradní řešení s cílem usnadnit výrobci plnit povinnost spojenou s dodržování těchto základních požadavků na kybernetickou bezpečnost, je-li proces normalizace zablokován nebo dojde-li při vypracovávání vhodných harmonizovaných norem k prodlevám. Je-li toto zpoždění způsobeno technickou složitostí dané normy, měla by to Komise zvážit předtím, než začne uvažovat o stanovení společných specifikací.

(84) Aby Komise mohla co nejúčinněji stanovit společné specifikace, které se vztahují na základní požadavky na kybernetickou bezpečnost uvedené v tomto nařízení, měla by do tohoto procesu zapojit příslušné zúčastněné strany.

(85) „Přiměřenou lhůtou“ se v souvislosti se zveřejněním odkazu na harmonizované normy v *Úředním věstníku Evropské unie* v souladu s nařízením (EU) č. 1025/2012 rozumí období, během něhož se očekává zveřejnění odkazu na normu, její opravu nebo změnu v *Úředním věstníku Evropské unie* a které by nemělo překročit jeden rok po uplynutí lhůty pro vypracování evropské normy stanovené v souladu s nařízením (EU) č. 1025/2012.

(86) Aby se usnadnilo posuzování shody se základními požadavky na kybernetickou bezpečnost stanovenými v tomto nařízení, měl by u produktů s digitálními prvky, které jsou ve shodě se společnými specifikacemi přijatými Komisí podle tohoto nařízení za účelem vyjádření podrobných technických specifikací těchto požadavků, existovat předpoklad shody.

(87) Uplatňování harmonizovaných norem, společných specifikací nebo evropských schémat certifikace kybernetické bezpečnosti přijatých podle nařízení (EU) 2019/881, které zakládají předpoklad shody ve vztahu k základním požadavkům na kybernetickou bezpečnost vztahujícím se na produkty s digitálními prvky, usnadní výrobcům posuzování shody. Pokud se výrobce rozhodne, že tyto prostředky pro určité požadavky nepoužije, musí ve své technické dokumentaci uvést, jakým jiným způsobem bylo shody dosaženo. Kromě toho by uplatňování harmonizovaných norem, společných specifikací nebo evropských schémat certifikace kybernetické bezpečnosti přijatých podle nařízení (EU) 2019/881, které zakládají předpoklad shody ze strany výrobců, usnadnilo kontrolu souladu produktů s digitálními prvky orgány dozoru nad trhem. Proto se výrobcům produktů s digitálními prvky doporučuje, aby tyto harmonizované normy, společné specifikace nebo evropská schémata certifikace kybernetické bezpečnosti uplatňovali.

(88) Výrobci by měli vypracovat EU prohlášení o shodě s cílem poskytnout informace požadované podle tohoto nařízení o shodě produktů s digitálními prvky se základními požadavky na kybernetickou bezpečnost stanovenými v tomto nařízení a případně v dalších příslušných harmonizačních právních předpisech Unie, které se na produkt s digitálními prvky vztahují. Od výrobců může být rovněž požadováno, aby vypracovali EU prohlášení o shodě na základě jiných právních aktů Unie. Aby se pro účely dozoru nad trhem zajistil účinný přístup k informacím, mělo by být vypracováno jediné EU prohlášení o shodě týkající se shody se všemi příslušnými právními akty Unie. Za účelem snížení administrativní zátěže hospodářských subjektů by toto jediné EU prohlášení o shodě mohlo mít podobu složky tvořené příslušnými jednotlivými prohlášeními o shodě.

(89) Označení CE, které vyjadřuje shodu výrobku, je viditelným výsledkem celého postupu zahrnujícího posuzování shody v širším smyslu. Obecné zásady upravující označení CE jsou stanoveny v nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ([29]). V tomto nařízení by měla být stanovena pravidla týkající se umisťování označení CE na produkty s digitálními prvky. Označení CE by mělo být jediným označením, které zaručuje, že produkt s digitálními prvky splňuje požadavky stanovené v tomto nařízení.

(90) Aby mohly hospodářské subjekty prokázat shodu se základními požadavky na kybernetickou bezpečnost stanovenými v tomto nařízení a aby orgány dozoru nad trhem mohly zajistit, že produkty s digitálními prvky dodávané na trh tyto požadavky splňují, je nezbytné stanovit postupy posuzování shody. V rozhodnutí Evropského

([29]) Nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a kterým se zrušuje nařízení (EHS) č. 339/93 (Úř. věst. L 218, 13.8.2008, s. 30).

parlamentu a Rady č. 768/2008/ES ([30]) jsou stanoveny moduly pro postupy posuzování shody podle míry souvisejícího rizika a požadované úrovně bezpečnosti. S cílem zajistit soudržnost mezi odvětvími a zabránit variantám ad hoc by měly být na těchto modulech založeny postupy posuzování shody vhodné pro ověření shody produktů s digitálními prvky se základními požadavky na kybernetickou bezpečnost stanovenými v tomto nařízení. V rámci postupů posuzování shody by se měly přezkoumat a ověřit požadavky týkající se produktu i postupu, které se vztahují na celý životní cyklus produktů s digitálními prvky, včetně plánování, návrhu, vývoje nebo výroby, testování a údržby produktu s digitálními prvky.

(91) Posuzování shody produktů s digitálními prvky, které nejsou v tomto nařízení uvedeny na seznamu důležitých nebo kritických produktů s digitálními prvky, může v souladu s tímto nařízením na vlastní odpovědnost provádět výrobce postupem interní kontroly založeným na modulu A rozhodnutí č. 768/2008/ES. To platí i pro případy, kdy se výrobce rozhodne zcela nebo zčásti nepoužít příslušnou harmonizovanou normu, společnou specifikaci nebo evropské schéma certifikace kybernetické bezpečnosti. Výrobce si ponechá možnost zvolit přísnější postup posuzování shody za účasti třetí strany. V rámci posuzování shody postupem interní kontroly výrobce na svou výhradní odpovědnost zajišťuje a prohlašuje, že produkt s digitálními prvky a postupy výrobce splňují příslušné základní požadavky na kybernetickou bezpečnost stanovené v tomto nařízení. Spadá-li důležitý produkt s digitálními prvky do třídy I, vyžaduje se dodatečná záruka za účelem prokázání shody se základními požadavky na kybernetickou bezpečnost stanovenými v tomto nařízení. Pokud chce výrobce provést posouzení shody na vlastní odpovědnost (modul A), měl by uplatňovat harmonizované normy, společné specifikace nebo evropská schémata certifikace kybernetické bezpečnosti přijatá podle nařízení (EU) 2019/881, které byly identifikované Komisí v prováděcím aktu. Pokud výrobce tyto harmonizované normy, společné specifikace nebo evropská schémata certifikace kybernetické bezpečnosti nepoužije, mělo by u něj proběhnout posouzení shody za účasti třetí strany (na základě modulů B a C nebo H). S ohledem na administrativní zátěž výrobců a na skutečnost, že kybernetická bezpečnost hraje důležitou úlohu ve fázi návrhu a vývoje hmotných i nehmotných produktů s digitálními prvky, byly jako nejvhodnější pro přiměřené a účinné posouzení souladu důležitých produktů s digitálními prvky vybrány postupy posuzování shody založené na modulech B a C nebo na modulu H rozhodnutí č. 768/2008/ES. Výrobce, který provádí posouzení shody za účasti třetí strany, si může zvolit postup, který je nejvhodnější z hlediska jeho procesu návrhu a výroby. Vzhledem k ještě většímu kybernetickému bezpečnostnímu riziku spojenému s používáním důležitých produktů s digitálními prvky, které spadají do třídy II, by se posuzování shody mělo vždy provádět za účasti třetí strany, a to i v případě, že produkt zcela nebo částečně splňuje harmonizované normy, společné specifikace nebo evropská schémata certifikace kybernetické bezpečnosti. Výrobci důležitých produktů s digitálními prvky, které jsou považovány za svobodný software s otevřeným zdrojovým kódem, by měli mít možnost řídit se postupem interní kontroly založeným na modulu A za předpokladu, že technickou dokumentaci zpřístupní veřejnosti.

(92) Zatímco vytváření hmotných produktů s digitálními prvky obvykle vyžaduje, aby výrobci vynaložili značné úsilí během fáze návrhu, vývoje a výroby, vytváření produktů s digitálními prvky ve formě softwaru se zaměřuje téměř výhradně na návrh a vývoj, zatímco výrobní fáze hraje jen vedlejší roli. V řadě případů však musejí být softwarové produkty ještě před uvedením na trh zkompilovány, vytvořeny, zabaleny, zpřístupněny ke stažení nebo zkopírovány na fyzické nosiče. Tyto činnosti by měly být při použití příslušných modulů posuzování shody s cílem ověřit soulad produktu se základními požadavky na kybernetickou bezpečnost stanovenými v tomto nařízení ve fázi návrhu, vývoje a výroby považovány za činnosti odpovídající výrobě.

(93) Pokud jde o mikropodniky a malé podniky, je v zájmu zajištění proporcionality vhodné snížit administrativní náklady, aniž by to ovlivnilo úroveň kybernetické bezpečnosti produktů s digitálními prvky, které spadají do oblasti působnosti tohoto nařízení, nebo rovné podmínky mezi výrobci. Je proto vhodné, aby Komise vytvořila zjednodušený formulář technické dokumentace zaměřený na potřeby mikropodniků a malých podniků. Zjednodušený formulář technické dokumentace přijatý Komisí by měl zahrnovat všechny příslušné prvky týkající se technické dokumentace stanovené v tomto nařízení a upřesňovat, jak může mikropodnik nebo malý podnik stručně poskytnout požadované prvky, jako je popis návrhu, vývoje a výroby produktu s digitálními prvky. Formulář by tak přispěl ke zmírnění administrativní zátěže spojené s dodržováním předpisů tím, že by dotčeným podnikům poskytl právní jistotu ohledně toho, jak rozsáhlé a nakolik podrobné informace mají poskytnout. Mikropodniky a malé podniky by měly mít možnost zvolit si poskytování příslušných prvků technické dokumentace v rozšířené podobě a nepoužít zjednodušený formulář technické dokumentace, který mají k dispozici.

([30]) 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 (Úř. věst. L 218, 13.8.2008, s. 82).

(94) V zájmu podpory a ochrany inovací je důležité brát zvláštní ohled na zájmy výrobců, kteří jsou mikropodniky nebo malými nebo středními podniky, zejména mikropodniků a malých podniků, včetně začínajících podniků. Za tímto účelem by členské státy mohly vyvinout iniciativy zaměřené na výrobce, kteří jsou mikropodniky nebo malými podniky, včetně iniciativ v oblasti školení, zvyšování informovanosti, poskytování informací, testování a činnosti při posuzování shody třetími stranami a v oblasti zřizování sandboxů. Náklady na překlad související s povinnou dokumentací, jako je technická dokumentace a informace a pokyny pro uživatele požadované podle tohoto nařízení, a na komunikaci s orgány mohou pro výrobce, zejména ty menší velikosti, představovat značné náklady. Členské státy by proto měly mít možnost zvážit, aby jedním z jazyků, který určí a přijmou pro příslušnou dokumentaci výrobců a pro komunikaci s výrobci, byl jazyk, kterému obecně rozumí co nejvyšší počet uživatelů.

(95) V zájmu zajištění hladkého uplatňování tohoto nařízení by členské státy měly usilovat o zajištění toho, aby byl před datem použitelnosti tohoto nařízení k dispozici dostatečný počet oznámených subjektů k provádění posouzení shody třetí stranou. Komise by se měla snažit členským státům a dalším příslušným stranám v tomto úsilí pomoci, aby se předešlo překážkám a problémům bránícím vstupu výrobců na trh. Cílená školící činnost vedená členskými státy, případně i s podporou Komise, může přispět k dostupnosti kvalifikovaných odborníků, mimo jiné za účelem podpory činnosti oznámených subjektů podle tohoto nařízení. Kromě toho by s ohledem na náklady, které mohou být s posuzováním shody třetí stranou spojeny, měly být zváženy iniciativy v oblasti financování na úrovni Unie a členských států s cílem snížit tyto náklady pro mikropodniky a malé podniky.

(96) Aby byla zajištěna proporcionalita, měly by subjekty posuzování shody při stanovování poplatků za postupy posuzování shody zohledňovat zvláštní zájmy a potřeby mikropodniků a malých a středních podniků, včetně začínajících podniků. Zejména by subjekty posuzování shody měly uplatňovat příslušný přezkumný postup a zkoušky stanovené v tomto nařízení pouze v případě potřeby a v souladu s přístupem založeným na posouzení rizik.

(97) Cílem regulačních sandboxů by měla být podpora inovací a konkurenceschopnosti podniků vytvořením kontrolovaného testovacího prostředí před uvedením produktů s digitálními prvky na trh. Regulační sandboxy by měly přispět ke zvýšení právní jistoty pro všechny subjekty, které spadají do oblasti působnosti tohoto nařízení, a usnadnit a urychlit přístup produktů s digitálními prvky na trh Unie, zejména pokud je dodávají mikropodniky a malé podniky, včetně začínajících podniků.

(98) Za účelem provedení posouzení shody produktů s digitálními prvky třetí stranou by subjekty posuzování shody měly být oznámeny vnitrostátními oznamujícími orgány Komisi a ostatním členským státům, pokud splňují určitý soubor požadavků, zejména požadavků na nezávislost, způsobilost a neexistenci střetu zájmů.

(99) Za účelem zajištění jednotné úrovně kvality při posuzování shody produktů s digitálními prvky je rovněž nezbytné stanovit požadavky pro oznamující orgány a ostatní subjekty zapojené do posuzování, oznamování a kontroly oznámených subjektů. Systém stanovený v tomto nařízení by měl být doplněn akreditačním systémem stanoveným v nařízení (ES) č. 765/2008. Vzhledem k tomu, že akreditace je základním prostředkem ověřování způsobilosti subjektů posuzování shody, měla by být používána rovněž pro účely oznamování.

(100) Subjekty posuzování shody, které byly akreditovány a oznámeny podle práva Unie stanovujícího požadavky podobné těm, jež jsou obsaženy v tomto nařízení, jako je subjekt posuzování shody oznámený v rámci evropského schématu certifikace kybernetické bezpečnosti přijatého podle nařízení (EU) 2019/881 nebo oznámený podle nařízení v přenesené pravomoci (EU) 2022/30, by měly být nově posouzeny a oznámeny podle tohoto nařízení. Příslušné orgány však mohou vymezit součinnost, pokud jde o překrývající se požadavky, aby se předešlo zbytečné finanční a administrativní zátěži a zajistil hladký a včasný postup oznamování.

(101) Transparentní akreditaci stanovenou v nařízení (ES) č. 765/2008, zajišťující nezbytnou míru důvěry v certifikáty shody, by měly vnitrostátní veřejné orgány v Unii považovat za přednostní způsob prokázání odborné způsobilosti subjektů posuzování shody. Vnitrostátní orgány se však mohou domnívat, že mají vhodné prostředky k tomu, aby toto hodnocení prováděly samy. V takovém případě by s cílem zajistit náležitou úroveň věrohodnosti hodnocení prováděného jinými vnitrostátními orgány měly Komisi a ostatním členským státům poskytnout nezbytné doklady o tom, že hodnocené subjekty posuzování shody splňují příslušné regulační požadavky.

(102) Subjekty posuzování shody často zadávají část svých činností souvisejících s posuzováním shody subdodavateli nebo dceřiné společnosti. V zájmu zachování úrovně ochrany požadované pro produkt s digitálními prvky, který má být uveden na trh, je nezbytné, aby subdodavatelé a dceřiné společnosti provádějící posuzování shody splňovali při provádění úkolů posuzování shody stejné požadavky jako oznámené subjekty.

(103) Oznámení subjektu posuzování shody by měl oznamující orgán zaslat Komisi a ostatním členským státům prostřednictvím informačního systému oznámených a jmenovaných organizací podle nového přístupu (NANDO). Informační systém NANDO je elektronický nástroj pro oznamování vyvinutý a spravovaný Komisí, v němž lze nalézt seznam všech oznámených subjektů.

(104) Vzhledem k tomu, že oznámené subjekty mohou své služby nabízet na území celé Unie, je vhodné dát ostatním členským státům a Komisi možnost vznést námitky týkající se oznámeného subjektu. Je proto důležité stanovit dobu, během níž bude možné vyjasnit veškeré pochyby nebo výhrady týkající se způsobilosti subjektů posuzování shody předtím, než začnou fungovat jako oznámené subjekty.

(105) Z důvodu konkurenceschopnosti je zásadně důležité, aby oznámené subjekty používaly postupy posuzování shody, aniž by zbytečně zatěžovaly hospodářské subjekty. Ze stejného důvodu a v zájmu zajištění rovného zacházení s hospodářskými subjekty je třeba zajistit jednotné technické provádění postupů posuzování shody. Toho by mělo být nejlépe dosaženo vhodnou koordinací a spoluprací mezi oznámenými subjekty.

(106) Dozor nad trhem je základním nástrojem při zajišťování řádného a jednotného uplatňování práva Unie. Proto je vhodné vytvořit právní rámec, ve kterém může dozor nad trhem vhodným způsobem probíhat. Na produkty s digitálními prvky, které spadají do oblasti působnosti tohoto nařízení, se vztahují pravidla pro dozor nad trhem Unie a kontrolu výrobků vstupujících na trh Unie stanovená v nařízení (EU) 2019/1020.

(107) V souladu s nařízením (EU) 2019/1020 vykonává orgán dozoru nad trhem dozor nad trhem na území toho členského státu, který jej určí. Toto nařízení by nemělo členským státům bránit, aby si samy zvolily příslušné orgány, které budou tyto úkoly plnit. Každý členský stát by měl na svém území určit jeden nebo více orgánů dozoru nad trhem. Členské státy by měly mít možnost určit některý stávající nebo nový orgán, který bude působit jako orgán dozoru nad trhem, včetně příslušných orgánů určených nebo zřízených podle článku 8 směrnice (EU) 2022/2555, vnitrostátních orgánů certifikace kybernetické bezpečnosti určených podle článku 58 nařízení (EU) 2019/881 nebo orgánů dozoru nad trhem určených pro účely směrnice 2014/53/EU. Hospodářské subjekty by měly plně spolupracovat s orgány dozoru nad trhem a dalšími příslušnými orgány. Každý členský stát by měl oznámit Komisi a ostatním členským státům své orgány dozoru nad trhem a působnost každého z nich, přičemž by měl zajistit nezbytné zdroje a dovednosti pro plnění úkolů dozoru nad trhem souvisejících s tímto nařízením. Podle čl. 10 odst. 2 a 3 nařízení (EU) 2019/1020 by měl každý členský stát jmenovat ústřední styčný úřad, který by měl mimo jiné odpovídat za zastupování koordinovaného postoje orgánů dozoru nad trhem a za pomoc při spolupráci mezi orgány dozoru nad trhem v různých členských státech.

(108) Pro jednotné uplatňování tohoto nařízení by měla být zřízena podle čl. 30 odst. 2 nařízení (EU) 2019/1020 specializovaná skupina pro správní spolupráci zabývající se kybernetickou odolností produktů s digitálními prvky. Tato skupina by se měla skládat ze zástupců určených orgánů dozoru nad trhem a případně i ze zástupců ústředních styčných úřadů. Komise by měla podporovat a podněcovat spolupráci mezi orgány dozoru nad trhem prostřednictvím sítě Unie pro soulad výrobků s předpisy, zřízené podle článku 29 nařízení (EU) 2019/1020 a složené ze zástupců každého členského státu, včetně zástupce každého ústředního styčného úřadu podle článku 10 uvedeného nařízení a nepovinného vnitrostátního odborníka, předsedů skupiny pro správní spolupráci a zástupců Komise. Komise by se měla účastnit zasedání sítě Unie pro soulad výrobků s předpisy, jejích podskupin a specializované skupiny pro správní spolupráci. Měla by skupině pro správní spolupráci rovněž poskytovat pomoc prostřednictvím výkonného sekretariátu, který poskytuje technickou a logistickou podporu. Specializovaná skupina pro správní spolupráci může přizvat k účasti rovněž nezávislé odborníky a spolupracovat s dalšími skupinami pro správní spolupráci, jako je skupina zřízená podle směrnice 2014/53/EU.

(109) Orgány dozoru nad trhem by prostřednictvím specializované skupiny pro správní spolupráci zřízené podle tohoto nařízení měly úzce spolupracovat a měly by být schopny vypracovat pokyny pro usnadnění dozoru nad trhem na vnitrostátní úrovni, například vypracováním osvědčených postupů a ukazatelů pro účinnou kontrolu souladu produktů s digitálními prvky s tímto nařízením.

(110) V zájmu zajištění včasných, přiměřených a účinných opatření ve vztahu k produktům s digitálními prvky, které představují významné kybernetické bezpečnostní riziko, by měl být stanoven ochranný postup Unie, v jehož rámci jsou zúčastněné strany informovány o opatřeních, která mají být v souvislosti s těmito produkty přijata. Tento postup by měl orgánům dozoru nad trhem umožnit, aby ve spolupráci s příslušnými hospodářskými subjekty jednaly v případě potřeby dříve. Pokud se členské státy a Komise shodují na důvodnosti opatření přijatého členským státem, neměl by být vyžadován žádný další zásah Komise, kromě případů, kdy lze nesoulad přisuzovat nedostatkům v harmonizované normě.

(111) V některých případech však může produkt s digitálními prvky, který je v souladu s tímto nařízením, přesto představovat významné kybernetické bezpečnostní riziko nebo představovat riziko pro zdraví nebo bezpečnost osob, pro dodržování povinností podle unijního nebo vnitrostátního práva, jejichž cílem je ochrana základních práv, pro dostupnost, autenticitu, integritu nebo důvěrnost služeb nabízených prostřednictvím elektronického informačního systému základními subjekty podle čl. 3 odst. 1 směrnice (EU) 2022/2555 nebo pro jiné aspekty ochrany veřejného zájmu. Je proto nezbytné stanovit pravidla, která zajistí zmírnění těchto rizik. V důsledku toho by orgány dozoru nad trhem měly přijmout opatření požadující po hospodářském subjektu, aby zajistil, že produkt již toto riziko nepředstavuje, nebo aby jej v závislosti na riziku stáhl z oběhu nebo z trhu. Jakmile orgán dozoru nad trhem takto omezí nebo zakáže volný pohyb produktu s digitálními prvky, měl by členský stát neprodleně oznámit Komisi a ostatním členským státům prozatímní opatření s uvedením důvodů a vysvětlení tohoto rozhodnutí. Pokud orgán dozoru nad trhem tato opatření proti produktům s digitálními prvky představujícím riziko přijme, měla by Komise neprodleně zahájit konzultace s členskými státy a příslušným hospodářským subjektem nebo subjekty a měla by vnitrostátní opatření vyhodnotit. Na základě výsledků tohoto hodnocení by měla Komise rozhodnout, zda je vnitrostátní opatření důvodné, či nikoli. Rozhodnutí Komise by mělo být určeno všem členským státům a Komise jej neprodleně sdělí členským státům a příslušnému hospodářskému subjektu nebo subjektům. Pokud je opatření považováno za důvodné, měla by mít Komise rovněž možnost zvážit přijetí návrhů na revizi příslušného práva Unie.

(112) U produktů s digitálními prvky, které představují významné kybernetické bezpečnostní riziko, a pokud existuje důvod se domnívat, že nejsou v souladu s tímto nařízením, nebo u produktů, které jsou v souladu s tímto nařízením, avšak představují jiná důležitá rizika, například rizika pro zdraví nebo bezpečnost osob, pro dodržování povinností podle unijního nebo vnitrostátního práva určeného k ochraně základních práv nebo pro dostupnost, autenticitu, integritu či důvěrnost služeb nabízených prostřednictvím elektronického informačního systému základními subjekty podle čl. 3 odst. 1 směrnice (EU) 2022/2555, by Komise měla mít možnost požádat agenturu ENISA o provedení hodnocení. Na základě tohoto hodnocení by Komise měla mít možnost prostřednictvím prováděcích aktů přijmout nápravná nebo omezující opatření na úrovni Unie, včetně požadavku na stažení příslušných produktů s digitálními prvky z trhu nebo z oběhu, a to v přiměřené lhůtě úměrné povaze rizika. Komise by měla mít možnost tento zásah použít pouze za výjimečných okolností, které jsou důvodem k okamžitému zásahu za účelem zachování řádného fungování vnitřního trhu, a pouze v případě, že orgány dozoru nad trhem nepřijaly účinná opatření k nápravě situace. Těmito výjimečnými okolnostmi mohou být mimořádné situace, kdy výrobce například ve velkém měřítku zpřístupňuje produkt s digitálními prvky nesplňující požadavky ve více členských státech a tento produkt se používá i v klíčových odvětvích ze strany subjektů, které spadají do oblasti působnosti směrnice (EU) 2022/2555, přičemž obsahuje známé zranitelnosti, které zneužívají škodliví aktéři a pro něž výrobce neposkytuje dostupné opravy. Komise by měla mít možnost v těchto mimořádných situacích zasáhnout pouze po dobu trvání mimořádných okolností a v případě, že přetrvává nesoulad s tímto nařízením nebo že přetrvávají uvedená významná rizika.

(113) Pokud existují náznaky nesouladu s tímto nařízením v několika členských státech, měly by mít orgány dozoru nad trhem možnost provádět společnou činnost s jinými orgány za účelem ověření souladu a zjištění kybernetických bezpečnostních rizik produktů s digitálními prvky.

(114) Souběžné koordinované kontrolní akce (společné kontrolní akce) jsou konkrétní donucovací opatření orgánů dozoru nad trhem, která mohou dále zvýšit bezpečnost produktů. Společné kontrolní akce by měly být prováděny zejména v případech, kdy tržní trendy, stížnosti spotřebitelů nebo jiné náznaky ukazují, že některé kategorie produktů s digitálními prvky často představují kybernetická bezpečnostní rizika. Kromě toho by orgány dozoru nad trhem měly při určování kategorií produktů, na které se mají vztahovat tyto společné kontrolní akce, zohlednit i okolnosti týkající se jiných než technických rizikových faktorů. Za tímto účelem by orgány dozoru nad trhem měly mít možnost zohlednit výsledky koordinovaného posuzování bezpečnostních rizik kritických dodavatelských řetězců na úrovni Unie prováděného v souladu s článkem 22 směrnice (EU) 2022/2555, včetně okolností týkajících se jiných než technických rizikových faktorů. Agentura ENISA by měla orgánům dozoru nad trhem předkládat návrhy na kategorie produktů s digitálními prvky, u nichž by mohly být tyto společné kontrolní akce zorganizovány, mimo jiné na základě obdržených oznámení o zranitelnosti produktů a o incidentech.

(115) Agentura ENISA by s ohledem na své odborné znalosti a mandát měla být schopna podporovat proces uplatňování tohoto nařízení. Agentura ENISA by zejména měla mít možnost navrhovat společné činnosti, které mají provádět orgány dozoru nad trhem na základě údajů nebo informací o možném nesouladu produktů s digitálními prvky s tímto nařízením v některých členských státech, nebo určit kategorie produktů, pro něž by měly být organizovány společné kontrolní akce. Za výjimečných okolností by agentura ENISA měla mít na žádost Komise možnost provádět hodnocení konkrétních produktů s digitálními prvky, které představují významné kybernetické bezpečnostní riziko, je-li pro zachování řádného fungování vnitřního trhu nutný okamžitý zásah.

(116) Toto nařízení svěřuje agentuře ENISA určité úkoly, které vyžadují odpovídající zdroje z hlediska odborných znalostí i z hlediska lidských zdrojů, aby je mohla agentura ENISA účinně plnit. Při přípravě návrhu souhrnného rozpočtu Unie navrhne Komise v souladu s postupem stanoveným v článku 29 nařízení (EU) 2019/881 nezbytné rozpočtové zdroje pro plán pracovních míst agentury ENISA. Během tohoto procesu Komise zváží celkové zdroje agentury ENISA, aby mohla plnit své úkoly, včetně úkolů svěřených agentuře ENISA podle tohoto nařízení.

(117) Aby bylo zajištěno, že regulační rámec může být v případě potřeby upraven, měla by být na Komisi přenesena pravomoc přijímat akty v souladu s článkem 290 Smlouvy o fungování Evropské unie (dále jen „Smlouva o fungování EU"), pokud jde o aktualizace a přílohu tohoto nařízení obsahující seznam kritických produktů s digitálními prvky. Na Komisi by měla být přenesena pravomoc přijímat akty v souladu s uvedeným článkem, v nichž by stanovila, na které produkty s digitálními prvky se vztahují jiná pravidla Unie, jež dosahují stejné úrovně ochrany jako toto nařízení, a upřesnila, zda by bylo nezbytné je omezit nebo vyloučit z oblasti působnosti tohoto nařízení, jakož i případně rozsah tohoto omezení. Na Komisi by také měla být přenesena pravomoc přijímat akty v souladu s uvedeným článkem, pokud jde o případné pověření certifikací v rámci evropského schématu certifikace kybernetické bezpečnosti pro kritické produkty s digitálními prvky stanovené v příloze tohoto nařízení, jakož i o aktualizaci seznamu kritických produktů s digitálními prvky na základě kritérií kritičnosti stanovených v tomto nařízení a o upřesnění evropských schémat certifikace kybernetické bezpečnosti přijatých podle nařízení (EU) 2019/881, které lze použít k prokázání souladu se základními požadavky na kybernetickou bezpečnost nebo jejich částmi, jak je stanoveno v příloze tohoto nařízení. Na Komisi by měla být přenesena rovněž pravomoc přijímat akty v přenesené pravomoci ke stanovení minimální doby podpory pro konkrétní kategorie produktů, u nichž údaje z dozoru nad trhem naznačují, že tato doba je nedostatečná, a také ke stanovení podmínek pro uplatnění důvodů souvisejících s kybernetickou bezpečností, pokud jde o odklad zasílání oznámení o aktivně zneužívaných zranitelnostech. Kromě toho by na Komisi měla být přenesena pravomoc přijímat akty za účelem zavedení dobrovolných programů osvědčování bezpečnosti pro posuzování shody produktů s digitálními prvky, které lze považovat za svobodný software s otevřeným zdrojovým kódem, se všemi nebo některými základními požadavky na kybernetickou bezpečnost či jinými povinnostmi stanovenými v tomto nařízení, jakož i za účelem stanovení minimálního obsahu EU prohlášení o shodě a doplnění prvků, které mají být obsaženy v technické dokumentaci. Je obzvláště důležité, aby Komise v rámci přípravné činnosti vedla odpovídající konzultace, a to i na odborné úrovni, a aby tyto konzultace probíhaly v souladu se zásadami stanovenými v interinstitucionální dohodě ze dne 13. dubna 2016 o zdokonalení tvorby právních předpisů ([31]). Pro zajištění rovné účasti na vypracovávání aktů v přenesené pravomoci obdrží Evropský parlament a Rada veškeré dokumenty současně s odborníky z členských států a jejich odborníci mají automaticky přístup na setkání skupin odborníků Komise, jež se věnují přípravě aktů v přenesené pravomoci. Pravomoc přijímat akty v přenesené pravomoci podle tohoto nařízení by měla být Komisi svěřena na dobu pěti let od 10. prosince 2024. Komise by měla vypracovat zprávu o přenesení pravomoci nejpozději devět měsíců před koncem tohoto pětiletého období. Přenesení pravomoci se automaticky prodlužuje o stejně dlouhá období, pokud Evropský parlament ani Rada nevysloví proti tomuto prodloužení námitku nejpozději tři měsíce před koncem každého z těchto období.

(118) Za účelem zajištění jednotných podmínek uplatňování tohoto nařízení by měly být Komisi svěřeny prováděcí pravomoci, aby určila technický popis kategorií důležitých produktů s digitálními prvky stanovených v příloze tohoto nařízení a formát a prvky softwarového kusovníku, blíže upřesnila formát a postup oznamování aktivně zneužívaných zranitelností a závažných incidentů s dopadem na bezpečnost produktů s digitálními prvky ze strany výrobců, stanovila společné specifikace týkající se technických požadavků, které poskytují prostředky k prokázání shody se základními požadavky na kybernetickou bezpečnost stanovenými v příloze tohoto nařízení, stanovila technické specifikace pro označení, piktogramy nebo jakékoli jiné značky týkající se bezpečnosti produktů s digitálními prvky, jejich doby podpory a mechanismů na podporu jejich používání, zvýšila informovanost veřejnosti o bezpečnosti produktů s digitálními prvky, upřesnila zjednodušený formulář dokumentace zaměřený na potřeby mikropodniků a malých podniků a rozhodla o nápravných nebo omezujících opatřeních na úrovni Unie za

([31]) Úř. věst. L 123, 12.5.2016, s. 1.

výjimečných okolností, které odůvodňují okamžitý zásah za účelem zachování řádného fungování vnitřního trhu. Tyto pravomoci by měly být vykonávány v souladu s nařízením Evropského parlamentu a Rady (EU) č. 182/2011 ([32]).

(119) V zájmu zajištění důvěryhodné a konstruktivní spolupráce orgánů dozoru nad trhem na úrovni Unie a členských států by měly všechny strany zapojené do uplatňování tohoto nařízení respektovat důvěrnost informací a údajů získaných při plnění svých úkolů.

(120) S cílem zajistit účinné vymáhání povinností stanovených v tomto nařízení by každý orgán dozoru nad trhem měl mít pravomoc ukládat správní pokuty nebo požadovat uložení správních pokut. Proto by měly být stanoveny maximální úrovně správních pokut za nedodržení povinností stanovených v tomto nařízení, které mají být určeny ve vnitrostátních právních předpisech. Při rozhodování o výši správní pokuty v každém jednotlivém případě by měly být zohledněny veškeré relevantní okolnosti konkrétní situace a přinejmenším ty, které jsou výslovně stanoveny v tomto nařízení, včetně skutečnosti, zda je výrobcem mikropodnik, malý nebo střední podnik, včetně začínajících podniků, a zda tytéž nebo jiné orgány dozoru nad trhem již neuložily témuž hospodářskému subjektu správní pokutu za podobné porušení. Tyto okolnosti by mohly být buď přitěžující v situacích, kdy porušení ze strany téhož hospodářského subjektu trvá na území jiných členských států, než je stát, v němž již byla správní pokuta uložena, nebo polehčující čím bude zajištěno, aby jakákoli jiná správní pokuta zvažovaná jiným orgánem dozoru nad trhem pro tentýž hospodářský subjekt nebo stejný druh protiprávního jednání již zohledňovala, spolu s dalšími relevantními zvláštními okolnostmi, pokutu a její výši uloženou v jiných členských státech. Ve všech těchto případech by kumulativní správní pokuta, kterou by mohly uložit orgány dozoru nad trhem několika členských států témuž hospodářskému subjektu za stejný druh porušení, měla zajišťovat dodržení zásady proporcionality. Vzhledem k tomu, že se správní pokuty nevztahují na mikropodniky nebo malé podniky za nedodržení 24 hodinové lhůty pro včasné varování o aktivně zneužívaných zranitelnostech nebo závažných incidentech, které mají dopad na bezpečnost produktu s digitálními prvky, ani na správce softwaru s otevřeným zdrojovým kódem za jakékoli porušení tohoto nařízení, a s výhradou zásady, že sankce by měly být účinné, přiměřené a odrazující, neměly by členské státy těmto subjektům ukládat jiné druhy sankcí peněžní povahy.

(121) Jsou-li správní pokuty uloženy osobě, která není podnikem, měl by příslušný úřad při rozhodování o odpovídající výši pokuty zohlednit obecnou úroveň příjmů v daném členském státě a ekonomickou situaci dané osoby. Mělo by být ponecháno na členských státech, aby určily, zda a v jaké míře by měly podléhat správním pokutám orgány veřejné správy.

(122) Členské státy by měly s přihlédnutím k vnitrostátním okolnostem posoudit možnost použití příjmů ze sankcí stanovených v tomto nařízení nebo jejich finančního ekvivalentu na podporu opatření v oblasti kybernetické bezpečnosti a zvýšení úrovně kybernetické bezpečnosti v Unii, mimo jiné zvýšením počtu kvalifikovaných odborníků v oblasti kybernetické bezpečnosti, posílením budování kapacit mikropodniků a malých a středních podniků a zlepšením informovanosti veřejnosti o kybernetických hrozbách.

(123) Ve vztazích s třetími zeměmi usiluje Unie o podporu mezinárodního obchodu s regulovanými produkty. V zájmu usnadnění obchodu lze uplatnit širokou škálu opatření, včetně několika právních nástrojů, například dvoustranných (mezivládních) dohod o vzájemném uznávání posuzování shody a označování regulovaných produktů. Dohody o vzájemném uznávání se uzavírají mezi Unií a třetími zeměmi, které jsou na srovnatelné úrovni technického rozvoje a mají slučitelný přístup k posuzování shody. Tyto dohody jsou založeny na vzájemném uznávání certifikátů, označení shody a protokolů o zkouškách vystavených subjekty posuzování shody jedné ze stran v souladu s právními předpisy druhé strany. V současné době platí dohody o vzájemném uznávání s několika třetími zeměmi. Tyto dohody se uzavírají v řadě konkrétních odvětví, která se mohou u jednotlivých třetích zemích lišit. S cílem dále usnadnit obchod a s vědomím, že dodavatelské řetězce produktů s digitálními prvky jsou celosvětové, mohou být dohody o vzájemném uznávání týkající se posuzování shody pro produkty, na něž se vztahuje toto nařízení, uzavřeny Unií v souladu s článkem 218 Smlouvy o fungování EU. V zájmu posílení kybernetické odolnosti v celosvětovém měřítku je rovněž důležitá spolupráce s partnerskými třetími zeměmi, neboť to v dlouhodobém horizontu přispěje k posílení rámce kybernetické bezpečnosti v rámci Unie i mimo ni.

([32]) Nařízení Evropského parlamentu a Rady (EU) č. 182/2011 ze dne 16. února 2011, kterým se stanoví pravidla a obecné zásady způsobu, jakým členské státy kontrolují Komisi při výkonu prováděcích pravomocí (Úř. věst. L 55, 28.2.2011, s. 13. ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(124) Spotřebitelé by měli být oprávněni vymáhat svá práva v souvislosti s povinnostmi, které byly podle tohoto nařízení uloženy hospodářským subjektům, prostřednictvím zástupných žalob v souladu se směrnicí Evropského parlamentu a Rady (EU) 2020/1828 ([33]). Za tímto účelem by mělo být v tomto nařízení stanoveno, že se směrnice (EU) 2020/1828 použije na zástupné žaloby týkající se porušení tohoto nařízení, které poškozuje nebo může poškodit kolektivní zájmy spotřebitelů. Proto je zapotřebí změnit odpovídajícím způsobem přílohu I uvedené směrnice. Členské státy by měly zajistit zohlednění uvedených změn v prováděcích opatřeních přijatých podle uvedené směrnice, i když přijetí vnitrostátních prováděcích opatření v tomto ohledu není podmínkou pro použitelnost uvedené směrnice na zmíněné zástupné žaloby. Pokud jde o zástupné žaloby týkající se porušení ustanovení tohoto nařízení hospodářskými subjekty, které poškozuje nebo může poškodit kolektivní zájmy spotřebitelů, měla by být uvedená směrnice použitelná od 11. prosince 2027.

(125) Komise by měla provádět pravidelné hodnocení a přezkum tohoto nařízení za konzultace s příslušnými zúčastněnými stranami, zejména pokud jde o nutnost změn s ohledem na měnící se společenské, politické, technické nebo tržní podmínky. Toto nařízení usnadní subjektům, které spadají do oblasti působnosti nařízení (EU) 2022/2554 a směrnice (EU) 2022/2555 a které používají produkty s digitálními prvky, plnění povinností v oblasti bezpečnosti dodavatelského řetězce. Komise by měla v rámci pravidelného přezkumu vyhodnotit kombinované účinky rámce Unie pro kybernetickou bezpečnost.

(126) Hospodářským subjektům by měl být poskytnut dostatečný čas na přizpůsobení se požadavkům stanoveným v tomto nařízení. Toto nařízení by se mělo použít od 11. prosince 2027, s výjimkou povinností podávat zprávy o aktivně zneužívaných zranitelnostech a závažných incidentech s dopadem na bezpečnost produktů s digitálními prvky, které by se měly použít od 11. září 2026, a ustanovení o oznamování subjektů posuzování shody, která by se měla použít od 11. června 2026.

(127) Je důležité poskytovat při uplatňování tohoto nařízení podporu mikropodnikům a malým a středním podnikům, včetně začínajících podniků, a minimalizovat rizika pro jeho uplatňování vyplývající z nedostatku znalostí a odborných poznatků na trhu a také usnadnit výrobcům plnění jejich povinností stanovených v tomto nařízení. Program Digitální Evropa a další příslušné programy Unie poskytují finanční a technickou podporu, která těmto podnikům umožňuje přispívat k růstu hospodářství Unie a k posílení společné úrovně kybernetické bezpečnosti v Unii. Evropské centrum kompetencí pro kybernetickou bezpečnost a národní koordinační centra, jakož i evropská centra pro digitální inovace zřízená Komisí a členskými státy na úrovni Unie nebo členských států by mohla podporovat rovněž podniky a organizace veřejného sektoru a mohla by přispět k uplatňování tohoto nařízení. V rámci svých příslušných úkolů a oblasti působnosti by mohla poskytovat technickou a vědeckou podporu mikropodnikům a malým a středním podnikům, například v oblasti testování a posuzování shody třetí stranou. Mohla by rovněž podpořit zavádění nástrojů usnadňujících uplatňování tohoto nařízení.

(128) Kromě toho by členské státy měly zvážit přijetí doplňkových opatření zaměřených na poskytování pokynů a podpory mikropodnikům a malým a středním podnikům, jako je zřízení regulačních sandboxů a vyhrazených komunikačních kanálů. V zájmu zvýšení úrovně kybernetické bezpečnosti v Unii mohou členské státy rovněž zvážit poskytnutí podpory na rozvoj kapacit a dovedností souvisejících s kybernetickou bezpečností produktů s digitálními prvky, na zlepšení kybernetické odolnosti hospodářských subjektů, zejména mikropodniků a malých a středních podniků, a na zvyšování informovanosti veřejnosti o kybernetické bezpečnosti produktů s digitálními prvky.

(129) Jelikož cíle tohoto nařízení nemůže být dosaženo uspokojivě členskými státy, ale spíše jej, z důvodu účinků opatření, může být lépe dosaženo na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy o Evropské unii. V souladu se zásadou proporcionality stanovenou v uvedeném článku nepřekračuje toto nařízení rámec toho, co je nezbytné k dosažení tohoto cíle.

(130) Evropský inspektor ochrany údajů byl konzultován v souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([34]) a dne 9. listopadu 2022 vydal své stanovisko ([35]),

([33]) Směrnice Evropského parlamentu a Rady (EU) 2020/1828 ze dne 25. listopadu 2020 o zástupných žalobách na ochranu kolektivních zájmů spotřebitelů a o zrušení směrnice 2009/22/ES (Úř. věst. L 409, 4.12.2020, s. 1).

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

([35]) Úř. věst. C 452, 29.11.2022, s. 23.

PŘIJALY TOTO NAŘÍZENÍ:

KAPITOLA I

OBECNÁ USTANOVENÍ

Článek 1

Předmět

Tímto nařízením se stanovují:

a) pravidla pro dodání produktů s digitálními prvky na trh s cílem zajistit kybernetickou bezpečnost těchto produktů,

b) základní požadavky na kybernetickou bezpečnost týkající se navrhování, vývoje a výroby produktů s digitálními prvky a povinnosti hospodářských subjektů v souvislosti s těmito produkty s ohledem na kybernetickou bezpečnost,

c) základní požadavky na kybernetickou bezpečnost týkající se procesů řešení zranitelnosti zavedené výrobci s cílem zajistit kybernetickou bezpečnost produktů s digitálními prvky během předpokládané doby používání produktu a povinnosti hospodářských subjektů v souvislosti s těmito procesy,

d) pravidla pro dozor nad trhem, včetně monitoringu, a prosazování pravidel a požadavků uvedených v tomto článku.

Článek 2

Oblast působnosti

1. Toto nařízení se 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.

2. Toto nařízení se nevztahuje na produkty s digitálními prvky, na něž se vztahují tyto právní akty Unie:

a) nařízení (EU) 2017/745,

b) nařízení (EU) 2017/746,

c) nařízení (EU) 2019/2144.

3. Toto nařízení se nevztahuje na výrobky s digitálními prvky, které byly certifikovány v souladu s nařízením (EU) 2018/1139.

4. Toto nařízení se nevztahuje na výstroj spadající do oblasti působnosti směrnice Evropského parlamentu a Rady 2014/90/EU ([36]).

5. Použití tohoto nařízení na produkty s digitálními prvky, na něž se vztahují jiná pravidla Unie stanovující požadavky, které se týkají všech nebo některých rizik, pro které platí základní požadavky na kybernetickou bezpečnost stanovené v příloze I, může být omezeno nebo vyloučeno, pokud:

a) je toto omezení nebo vyloučení v souladu s celkovým regulačním rámcem, který se na tyto produkty vztahuje, a

b) odvětvová pravidla dosahují stejné nebo vyšší úrovně ochrany, než jakou stanovuje toto nařízení.

Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 61 za účelem doplnění tohoto nařízení upřesněním, zda je toto omezení nebo vyloučení nezbytné, a specifikací dotčených produktů a pravidel a případně i rozsahu omezení.

([36]) Směrnice Evropského parlamentu a Rady 2014/90/EU ze dne 23. července 2014 o lodní výstroji a o zrušení směrnice Rady 96/98/ES (Úř. věst L 257, 28.8.2014, s. 146).

6. Toto nařízení se nevztahuje na náhradní díly, které jsou dodávány na trh za účelem nahrazení totožných komponent v produktech s digitálními prvky a které jsou vyrobeny podle stejných specifikací jako komponent, které mají nahradit.

7. Toto nařízení se nevztahuje na produkty s digitálními prvky vyvinuté nebo upravené výlučně pro účely národní bezpečnosti nebo obrany, ani na produkty speciálně určené ke zpracování utajovaných informací.

8. Povinnosti stanovené v tomto nařízení nezahrnují poskytování informací, jejichž zpřístupnění by bylo v rozporu se zásadními zájmy členských států v oblasti národní bezpečnosti, veřejné bezpečnosti nebo obrany.

Článek 3

Definice

Pro účely tohoto nařízení se rozumí:

1) „produktem s digitálními prvky“ softwarový nebo hardwarový produkt a jeho řešení pro zpracování dat na dálku, včetně softwarových nebo hardwarových komponent, které jsou uváděny na trh samostatně;

2) „zpracováním dat na dálku“ 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;

3) „kybernetickou bezpečností“ kybernetická bezpečnost ve smyslu čl. 2 bodu 1 nařízení (EU) 2019/881;

4) „softwarem“ část elektronického informačního systému, která sestává z počítačového kódu;

5) „hardwarem“ fyzický elektronický informační systém nebo jeho části schopné zpracovávat, uchovávat nebo přenášet digitální data;

6) „komponenta“ software nebo hardware určený pro začlenění do elektronického informačního systému;

7) „elektronickým informačním systémem“ systém, včetně elektrických nebo elektronických zařízení, který je schopen zpracovávat, uchovávat nebo přenášet digitální data;

8) „logickým připojením“ virtuální forma datového připojení zajišťovaná prostřednictvím softwarového rozhraní;

9) „fyzickým připojením“ spojení mezi elektronickými informačními systémy nebo komponentami zajišťované fyzickými prostředky, včetně elektrických, optických nebo mechanických rozhraní, vodičů nebo rádiových vln;

10) „nepřímým připojením“ připojení k zařízení nebo síti, které neprobíhá přímo, ale spíše jako součást větší soustavy, kterou lze k tomuto zařízení nebo síti přímo připojit;

11) „koncovým bodem“ jakékoli zařízení, které je připojeno k síti a slouží jako vstupní bod do této sítě;

12) „hospodářským subjektem“ výrobce, zplnomocněný zástupce, dovozce, distributor nebo jiná fyzická nebo právnická osoba, na kterou se vztahují povinnosti v souvislosti s výrobou produktů s digitálními prvky nebo s jejich dodáváním na trh v souladu s tímto nařízením;

13) „výrobcem“ fyzická nebo právnická osoba, která vyvíjí nebo vyrábí produkty s digitálními prvky, nebo která nechala produkty s digitálními prvky navrhnout, vyvinout nebo vyrobit a nabízí je pod svým jménem nebo ochrannou známkou, ať už za úplatu, jiné zpeněžení nebo bezplatně;

14) „správcem softwaru s otevřeným zdrojovým kódem“ právnická osoba jiná než výrobce, jejímž účelem nebo cílem je systematicky a dlouhodobě podporovat vývoj konkrétních produktů s digitálními prvky považovaných za svobodný software s otevřeným zdrojovým kódem a určených pro obchodní činnost, a která zajišťuje životaschopnost těchto produktů;

15) „zplnomocněným zástupcem“ fyzická nebo právnická osoba usazená v Unii, která byla výrobcem písemně pověřena, aby při plnění konkrétních úkolů jednala jeho jménem;

16) „dovozcem“ fyzická nebo právnická osoba usazená v Unii, která uvádí na trh produkt s digitálními prvky označený jménem nebo ochrannou známkou fyzické nebo právnické osoby usazené mimo Unii;

17) „distributorem“ fyzická nebo právnická osoba v dodavatelském řetězci jiná než výrobce nebo dovozce, která dodává produkt s digitálními prvky na trh Unie, aniž by ovlivňovala jeho vlastnosti;

18) „spotřebitelem“ fyzická osoba, která jedná za účelem, který není v rámci její obchodní činnosti, podnikání, řemesla nebo povolání;

19) „mikropodniky“, „malými podniky“ a „středními podniky“ mikropodniky, malé podniky a střední podniky ve smyslu definice uvedené v příloze k doporučení 2003/361/ES;

20) „dobou podpory“ období, během něhož musí výrobce zajistit, aby se zranitelnosti produktu s digitálními prvky řešily účinně a v souladu se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I části II;

21) „uvedením na trh“ první dodání produktu s digitálními prvky na trh Unie;

22) „dodáním na trh“ dodání produktu s digitálními prvky k distribuci nebo použití na trhu Unie v rámci obchodní činnosti, ať už za úplatu, nebo bezplatně;

23) „zamýšleným účelem“ použití produktu s digitálními prvky určené výrobcem, včetně konkrétního kontextu a podmínek použití, které jsou uvedeny v informacích dodaných výrobcem v návodu k použití, v propagačních nebo prodejních materiálech a prohlášeních, jakož i v technické dokumentaci;

24) „rozumně předvídatelným použitím“ použití, které není nutně zamýšleným účelem uvedeným výrobcem v návodu k použití, propagačních nebo prodejních materiálech a prohlášeních, jakož i v technické dokumentaci, ale které pravděpodobně vyplývá z důvodně předvídatelného lidského chování nebo technických operací nebo interakcí;

25) „rozumně předvídatelným nesprávným použitím“ použití produktu s digitálními prvky způsobem, který není v souladu s jeho zamýšleným účelem, avšak může vyplývat z důvodně předvídatelného lidského chování nebo z interakce s jinými systémy;

26) „oznamujícím orgánem“ vnitrostátní orgán odpovědný za stanovení a provádění postupů nezbytných pro posuzování, jmenování a oznamování subjektů posuzování shody a za jejich monitorování;

27) „posouzením shody“ postup ověřující, zda byly splněny základní požadavky na kybernetickou bezpečnost stanovené v příloze I;

28) „subjektem posuzování shody“ subjekt posuzování shody ve smyslu čl. 2 bodu 13 nařízení (ES) č. 765/2008;

29) „oznámeným subjektem“ subjekt posuzování shody určený v souladu s článkem 43 a dalšími příslušnými harmonizačními právními předpisy Unie;

30) „podstatnou změnou“ změna produktu s digitálními prvky po jeho uvedení na trh, která ovlivňuje soulad produktu s digitálními prvky se základními požadavky na kybernetickou bezpečnost stanovenými v části I přílohy I, nebo která vede ke změně zamýšleného účelu, pro nějž bylo provedeno posouzení produktu s digitálními prvky;

31) „označením CE“ označení, kterým výrobce vyjadřuje, že produkt s digitálními prvky a postupy zavedené výrobcem jsou ve shodě se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I a s dalšími použitelnými harmonizačními právními předpisy Unie, které upravují umístění tohoto označení;

32) „harmonizačními právními předpisy Unie“ právní předpisy Unie uvedené v příloze I nařízení (EU) 2019/1020 a jakékoli jiné právní předpisy Unie harmonizující podmínky pro nabízení výrobků, na něž se vztahuje uvedené nařízení, na trh;

33) „orgánem dozoru nad trhem“ orgán dozoru nad trhem ve smyslu čl. 3 bodu 4 nařízení (EU) 2019/1020;

34) „mezinárodní normou“ mezinárodní norma ve smyslu čl. 2 bodu 1 písm. a) nařízení (EU) č. 1025/2012;

35) „evropskou normou“ evropská norma ve smyslu čl. 2 odst. 1 písm. b) nařízení (EU) č. 1025/2012;

36) „harmonizovanou normou“ harmonizovaná norma ve smyslu čl. 2 bodu 1 písm. c) nařízení (EU) č. 1025/2012;

37) „kybernetickým bezpečnostním rizikem“ možnost ztráty nebo narušení v důsledku incidentu, přičemž toto riziko má být vyjádřeno jako kombinace rozsahu takové ztráty nebo takového narušení a pravděpodobnosti výskytu incidentu;

38) „významným kybernetickým bezpečnostním rizikem“ kybernetické bezpečnostní riziko, o němž lze na základě jeho technických charakteristik předpokládat, že u něj existuje vysoká pravděpodobnost incidentu, který by mohl vést k závažnému negativnímu dopadu, mimo jiné způsobením značné hmotné nebo nehmotné ztráty nebo narušení;

39) „softwarovým kusovníkem“ (SBOM) formální záznam obsahující podrobné informace o komponentách obsažených v softwarových prvcích produktu s digitálními prvky a o vztazích těchto komponent k dodavatelskému řetězci;

40) „zranitelností“ slabina, snížená odolnost nebo chyba produktu s digitálními prvky, kterou lze zneužít v rámci kybernetické hrozby;

41) „zneužitelnou zranitelností“ zranitelnost, která může být za praktických provozních podmínek účinně zneužita nepřátelským subjektem;

42) „aktivně zneužívanou zranitelností“ zranitelnost, u níž existují spolehlivé důkazy o tom, že ji škodlivý aktér v systému zneužil bez svolení vlastníka systému;

43) „incidentem“ incident ve smyslu čl. 6 bodu 6 směrnice (EU) 2022/2555;

44) „incidentem s dopadem na bezpečnost produktu s digitálními prvky“ incident, který negativně ovlivňuje nebo může negativně ovlivnit schopnost produktu s digitálními prvky chránit dostupnost, autenticitu, integritu nebo důvěrnost dat nebo funkcí;

45) „významnou událostí“ významná událost ve smyslu čl. 6 bodu 5 směrnice (EU) 2022/2555;

46) „kybernetickou hrozbou“ kybernetická hrozba ve smyslu čl. 2 bodu 8 nařízení (EU) 2019/881;

47) „osobními údaji“ osobní údaje ve smyslu čl. 4 bodu 1 nařízení (EU) 2016/679;

48) „svobodným softwarem s otevřeným zdrojovým kódem“ 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;

49) „stažením z oběhu“ stažení z oběhu ve smyslu čl. 3 bodu 22 nařízení (EU) 2019/1020;

50) „stažením z trhu“ stažení z trhu ve smyslu čl. 3 bodu 23 nařízení (EU) 2019/1020;

51) „týmem CSIRT určeným jako koordinátor“ tým CSIRT, který byl určen koordinátorem podle čl. 12 odst. 1 směrnice (EU) 2022/2555.

Článek 4

Volný pohyb

1. Členské státy nesmějí v záležitostech, na něž se vztahuje toto nařízení, bránit tomu, aby byly na trh dodávány produkty s digitálními prvky, které jsou v souladu s tímto nařízením.

2. Na veletrzích, výstavách, předváděcích nebo podobných akcích nesmějí členské státy bránit prezentaci ani používání produktu s digitálními prvky, který není v souladu s tímto nařízením, včetně jeho prototypů, za předpokladu, že je produkt prezentován s viditelným označením, které jasně ukazuje, že produkt není v souladu s tímto nařízením a nemá být dodáván na trh, dokud s ním nebude v souladu.

3. Členské státy nebrání dodávání nedokončeného softwaru, který není v souladu s tímto nařízením, na trh, za předpokladu, že software bude zpřístupněn pouze po omezenou dobu nezbytnou pro účely testování s viditelným označením jasně uvádějícím, že není v souladu s tímto nařízením a nebude dodáván na trh k jiným účelům než k testování.

4. Odstavec 3 se nevztahuje na bezpečnostní komponenty, které jsou uvedeny v jiných harmonizačních právních předpisech Unie než v tomto nařízení.

Článek 5

Zadávání zakázek na produkty s digitálními prvky nebo používání těchto produktů

1. Toto nařízení nebrání členským státům v tom, aby při zadávání zakázek na produkty s digitálními prvky nebo při jejich používání pro konkrétní účely, mimo jiné v případech, kdy jsou tyto produkty pořizovány či používány pro účely národní bezpečnosti nebo obrany, vyžadovaly, aby se na tyto produkty vztahovaly dodatečné požadavky na kybernetickou bezpečnost, a to za předpokladu, že takové požadavky jsou v souladu s povinnostmi členských států stanovenými v právu Unie a jsou nezbytné a přiměřené z hlediska dosažení těchto účelů.

2. Aniž jsou dotčeny směrnice 2014/24/EU a 2014/25/EU, v případech, kdy jsou pořizovány produkty s digitálními prvky, které spadají do oblasti působnosti tohoto nařízení, členské státy zajistí, aby byl při zadávání příslušných zakázek zohledněn soulad se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I tohoto nařízení, včetně schopnosti výrobců účinně řešit zranitelnosti.

Článek 6

Požadavky na produkty s digitálními prvky

Produkty s digitálními prvky se na trh dodávají pouze tehdy, pokud:

a) splňují základní požadavky na kybernetickou bezpečnost stanovené v části I přílohy I, za předpokladu, že jsou řádně instalovány, udržovány, používány k zamýšlenému účelu nebo za podmínek, které lze rozumně předvídat, a případně vybaveny nezbytnými bezpečnostními aktualizacemi, a

b) postupy zavedené výrobcem jsou v souladu se základními požadavky na kybernetickou bezpečnost stanovenými v části II přílohy I.

Článek 7

Důležité produkty s digitálními prvky

1. Produkty s digitálními prvky, jejichž klíčová funkce spadá do produktové kategorie stanovené v příloze III, se považují za důležité produkty s digitálními prvky a podléhají postupům posuzování shody uvedeným v čl. 32 odst. 2 a 3. Začlenění produktu s digitálními prvky, který má klíčovou funkci spadající do produktové kategorie stanovené v příloze III, samo o sobě neznamená, že produkt, do něhož je začleněn produkt s klíčovou funkci spadající do produktové kategorie stanovené v příloze III, podléhá postupům posuzování shody uvedeným v čl. 32 odst. 2 a 3.

2. Kategorie produktů s digitálními prvky uvedené v odstavci 1 tohoto článku, rozdělené do třídy I a II, jak jsou stanoveny v příloze III, splňují alespoň jedno z těchto kritérií:

a) produkt s digitálními prvky plní primárně funkce, které mají zásadní význam z hlediska kybernetické bezpečnosti jiných produktů, sítí nebo služeb, včetně zabezpečení ověřování a přístupu, prevence a detekce narušení, bezpečnosti koncových bodů nebo ochrany sítě,

b) produkt s digitálními prvky plní funkci, která s sebou nese značné riziko nepříznivých účinků, pokud jde o intenzitu a možnost narušit, ovládat nebo poškodit velký počet jiných produktů nebo zdraví, zabezpečení či bezpečnost jeho uživatelů prostřednictvím přímé manipulace, například funkci centrálního systému, včetně správy sítě, řízení konfigurace, virtualizace nebo zpracování osobních údajů.

3. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 61 za účelem změny přílohy III zařazením nové kategorie do každé třídy kategorií produktů s digitálními prvky na příslušném seznamu, upřesněním její definice, přesunutím kategorie produktů do jiné třídy nebo vynětím stávající kategorie z tohoto seznamu. Při posuzování potřeby změnit seznam uvedený v příloze III Komise zohlední funkcionalitu nebo funkci související s kybernetickou bezpečností a úroveň kybernetického bezpečnostního rizika, které s sebou nesou produkty s digitálními prvky, jak je stanoveno v kritériích uvedených v odstavci 2 tohoto článku.

V aktech v přenesené pravomoci uvedených v prvním pododstavci tohoto odstavce je případně stanoveno minimální přechodné období v délce 12 měsíců, zejména pokud je do třídy I nebo II doplněna nová kategorie důležitých produktů s digitálními prvky nebo pokud je přesunuta z třídy I do třídy II, jak jsou stanoveny v příloze III, před tím, než se začnou uplatňovat příslušné postupy posuzování shody uvedené v čl. 32 odst. 2 a 3, jestliže není ze závažných naléhavých důvodů opodstatněno stanovení kratšího přechodného období.

4. Do 11. prosince 2025 přijme Komise prováděcí akt, kterým upřesní technický popis kategorií produktů s digitálními prvky třídy I a II jak jsou stanoveny v příloze III a technický popis kategorií produktů s digitálními prvky jak jsou stanoveny v příloze IV. Tento prováděcí akt se přijme přezkumným postupem podle čl. 62 odst. 2.

Článek 8

Kritické produkty s digitálními prvky

1. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 61 za účelem doplnění tohoto nařízení tím, že určí, které produkty s digitálními prvky, jež mají klíčovou funkci produktové kategorie stanovené v příloze IV tohoto nařízení, musejí získat v rámci evropského schématu certifikace kybernetické bezpečnosti přijatého podle nařízení (EU) 2019/881 evropský certifikát kybernetické bezpečnosti alespoň na úrovni záruky „významná“, aby prokázaly shodu se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I tohoto nařízení nebo jejich částmi, pokud bylo v souladu s nařízením (EU) 2019/881 přijato evropské schéma certifikace kybernetické bezpečnosti zahrnující tyto kategorie produktů s digitálními prvky a je k dispozici výrobcům. Tyto akty v přenesené pravomoci stanoví požadovanou úroveň záruky, která je úměrná úrovni kybernetického bezpečnostního rizika spojeného s produkty s digitálními prvky, a zohlední jejich zamýšlený účel, včetně kritické závislosti základních subjektů uvedených v čl. 3 odst. 1 směrnice (EU) 2022/2555 na daných produktech s digitálními prvky.

Před přijetím těchto aktů v přenesené pravomoci posoudí Komise potenciální dopad plánovaných opatření na trh a uspořádá konzultace s příslušnými zúčastněnými stranami, mimo jiné s Evropskou skupinou pro certifikaci kybernetické bezpečnosti zřízenou nařízením (EU) 2019/881. Při tomto posuzování zohlední připravenost a kapacitu členských států pro uplatňování příslušných evropských schémat certifikace kybernetické bezpečnosti. Pokud nebyl přijat žádný akt v přenesené pravomoci uvedený v prvním pododstavci tohoto odstavce, vztahují se na produkty s digitálními prvky, které mají klíčovou funkci produktové kategorie, jak jsou stanoveny v příloze IV, postupy posuzování shody uvedené v čl. 32 odst. 3.

V aktech v přenesené pravomoci uvedených v prvním pododstavci je stanoveno minimální přechodné šestiměsíční období, není-li ze závažných naléhavých důvodů opodstatněno stanovení kratšího přechodného období.

2. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 61 za účelem změny přílohy IV doplněním nebo vynětím kategorií kritických produktů s digitálními prvky. Při určování těchto kategorií kritických produktů s digitálními prvky a požadované úrovně záruky v souladu s odstavcem 1 tohoto článku Komise zohlední kritéria uvedená v čl. 7 odst. 2 a rovněž to, do jaké míry platí alespoň jedno z těchto kritérií:

a) existuje kritická závislost základních subjektů uvedených v článku 3 směrnice (EU) 2022/2555 na kategorii produktů s digitálními prvky,

b) incidenty a zneužívané zranitelnosti týkající se kategorie produktů s digitálními prvky mohou vést k vážnému narušení kritických dodavatelských řetězců na celém vnitřním trhu.

Před přijetím těchto aktů v přenesené pravomoci provede Komise posouzení typu uvedené v odstavci 1.

V aktech v přenesené pravomoci uvedených v prvním pododstavci je stanoveno minimální přechodné šestiměsíční období, není-li ze závažných naléhavých důvodů opodstatněno stanovení kratšího přechodného období.

Článek 9

Konzultace se zúčastněnými stranami

1. Při přípravě opatření pro uplatňování tohoto nařízení Komise vede konzultace s příslušnými zúčastněnými stranami, jako jsou příslušné orgány členských států, podniky ze soukromého sektoru, včetně mikropodniků a malých a středních podniků, komunita zabývající se softwarem s otevřeným zdrojovým kódem, sdružení spotřebitelů, akademická obec a příslušné agentury a subjekty Unie a také odborné skupiny zřízené na úrovni Unie, a zohledňuje jejich názory. Komise případně konzultuje strukturovaným způsobem zejména s těmito zúčastněnými stranami a vyžádá si jejich názory:

a) při vypracovávání doporučujících pokynů podle článku 26,

b) při přípravě technických popisů kategorií produktů stanovených v příloze III v souladu s čl. 7 odst. 4, při posuzování nutnosti případné aktualizace seznamu kategorií produktů v souladu s čl. 7 odst. 3 a čl. 8 odst. 2 nebo při posuzování potenciálního dopadu na trh podle čl. 8 odst. 1, aniž je dotčen článek 61;

c) při provádění přípravných prací za účelem hodnocení a přezkumu tohoto nařízení.

2. Komise pořádá pravidelné konzultační a informační schůzky, a to nejméně jednou ročně, s cílem získat názory zúčastněných stran uvedených v odstavci 1 na uplatňování tohoto nařízení.

Článek 10

Prohloubení dovedností v oblasti kyberneticky odolného digitálního prostředí

Členské státy, pro účely tohoto nařízení a s cílem reagovat na potřeby odborníků při podpoře uplatňování tohoto nařízení, ve vhodných případech za podpory Komise, Evropského centra kompetencí pro kybernetickou bezpečnost a agentury ENISA a za plného respektování odpovědnosti členských států v oblasti vzdělávání, prosazují opatření a strategie zaměřené na:

a) rozvoj dovedností v oblasti kybernetické bezpečnosti a vytváření organizačních a technických nástrojů s cílem zajistit dostatečnou dostupnost kvalifikovaných odborníků na podporu činnosti orgánů dozoru nad trhem a subjektů posuzování shody,

b) prohloubení spolupráce mezi soukromým sektorem, hospodářskými subjekty, mimo jiné prostřednictvím rekvalifikace a prohlubování dovedností zaměstnanců výrobců, a mezi spotřebiteli, poskytovateli odborné přípravy a veřejnou správou, čímž rozšíří možnosti mladých lidí získat přístup k pracovním místům v odvětví kybernetické bezpečnosti.

Článek 11

Obecná bezpečnost produktů

Odchylně od čl. 2 odst. 1 třetího pododstavce písm. b) nařízení (EU) 2023/988 se na produkty s digitálními prvky s ohledem na aspekty a rizika nebo kategorie rizik neupravené tímto nařízením použije oddíl 1 kapitoly III, kapitola V a VII a kapitola IX až XI uvedeného nařízení, pokud se na tyto produkty nevztahují zvláštní požadavky na bezpečnost stanovené v jiných „harmonizačních právních předpisech Unie“ ve smyslu čl. 3 bodu 27 nařízení (EU) 2023/988.

Článek 12

Vysoce rizikové systémy umělé inteligence

1. Aniž jsou dotčeny požadavky na přesnost a spolehlivost stanovené v článku 15 nařízení (EU) 2024/1689, považují se produkty s digitálními prvky, které spadají do oblasti působnosti tohoto nařízení a jsou klasifikovány jako vysoce rizikové systémy umělé inteligence podle článku 6 uvedeného nařízení, za produkty, které jsou v souladu s požadavky na kybernetickou bezpečnost stanovenými v článku 15 uvedeného nařízení, pokud:

a) splňují základní požadavky na kybernetickou bezpečnost stanovené v příloze I části I,

b) postupy zavedené výrobcem splňují základní požadavky na kybernetickou bezpečnost stanovené v příloze I části II a

c) dosažení takové úrovně ochrany kybernetické bezpečnosti, kterou vyžaduje článek 15 nařízení (EU) 2024/1689, je potvrzeno v EU prohlášení o shodě vydaném podle tohoto nařízení.

2. U produktů s digitálními prvky a požadavků na kybernetickou bezpečnost podle odstavce 1 tohoto článku se použije příslušný postup posuzování shody stanovený v článku 43 nařízení (EU) 2024/1689. Pro účely tohoto posouzení jsou oznámené subjekty, které jsou příslušné ke kontrole shody vysoce rizikových systémů umělé inteligence podle nařízení (EU) 2024/1689, příslušné rovněž ke kontrole shody vysoce rizikových systémů umělé inteligence, které spadají do oblasti působnosti tohoto nařízení, s požadavky stanovenými v příloze I tohoto nařízení, pokud byl soulad těchto oznámených subjektů s požadavky stanovenými v článku 39 tohoto nařízení posouzen v rámci postupu oznamování podle nařízení (EU) 2024/1689.

3. Odchylně od odstavce 2 tohoto článku, se na důležité produkty s digitálními prvky uvedené v příloze III tohoto nařízení, na něž se vztahují postupy posuzování shody podle čl. 32 odst. 2 písm. a) a b) a čl. 32 odst. 3 tohoto nařízení, a na kritické produkty s digitálními prvky, jak jsou uvedeny v příloze IV tohoto nařízení, které musejí získat evropský certifikát kybernetické bezpečnosti podle čl. 8 odst. 1 tohoto nařízení, nebo na něž se v opačném případě vztahují postupy posuzování shody uvedené v čl. 32 odst. 3 tohoto nařízení, a které jsou klasifikovány jako vysoce rizikové systémy umělé inteligence podle článku 6 nařízení (EU) 2024/1689 a na něž se vztahuje postup posuzování shody založený na interní kontrole, jak je uvedeno v příloze VI nařízení (EU) 2024/1689, vztahují postupy posuzování shody stanovené v tomto nařízení, pokud jde o základní požadavky na kybernetickou bezpečnost stanovené v tomto nařízení.

4. Výrobci produktů s digitálními prvky uvedených v odst. 1 tohoto článku se mohou účastnit regulačních sandboxů pro umělou inteligenci, která jsou uvedena v článku 57 nařízení (EU) 2024/1689.

KAPITOLA II

POVINNOSTI HOSPODÁŘSKÝCH SUBJEKTŮ A USTANOVENÍ SOUVISEJÍCÍ SE SVOBODNÝM SOFTWAREM S OTEVŘENÝM ZDROJOVÝM Kódem

Článek 13

Povinnosti výrobců

1. Při uvádění produktu s digitálními prvky na trh výrobci zajistí, aby byl produkt navržen, vyvinut a vyroben v souladu se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I části I.

2. Pro účely splnění povinnosti stanovené v odstavci 1 provedou výrobci posouzení kybernetických bezpečnostních rizik spojených s produktem s digitálními prvky a výsledek tohoto posouzení zohlední během fáze plánování, navrhování, vývoje, výroby, dodání a údržby produktu s digitálními prvky s cílem minimalizovat kybernetická bezpečnostní rizika, předcházet incidentům a co nejvíce omezit jejich dopady, a to i v souvislosti se zdravím a bezpečností uživatelů.

3. Posouzení kybernetických bezpečnostních rizik se během doby podpory stanoveného v souladu s odstavcem 8 tohoto článku zdokumentuje a podle potřeby aktualizuje. Toto posouzení kybernetických bezpečnostních rizik zahrnuje alespoň analýzu kybernetických bezpečnostních rizik založenou na zamýšleném účelu a rozumně předvídatelném použití produktu s digitálními prvky a také na podmínkách jeho použití, jako je provozní prostředí nebo aktiva, která mají být ochráněna, s přihlédnutím k očekávané době používání produktu. Při posuzování kybernetických bezpečnostních rizik se zjistí, zda a pokud ano, jakým způsobem se bezpečnostní požadavky stanovené v příloze I části I bodě 2 vztahují na příslušný produkt s digitálními prvky a jak jsou tyto požadavky na základě posuzování kybernetických bezpečnostních rizik uplatňovány. Uvede se rovněž, jak má výrobce uplatňovat přílohu I část I bod 1 a požadavky na řešení zranitelností stanovené v příloze I části II.

4. Při uvádění produktu s digitálními prvky na trh zahrne výrobce posouzení kybernetických bezpečnostních rizik uvedené v odstavci 3 tohoto článku do technické dokumentace, jak vyžadují ustanovení článku 31 a přílohy VII. U produktů s digitálními prvky podle článku 12, který se řídí i jinými právními akty Unie, může být posouzení kybernetických bezpečnostních rizik součástí posouzení rizik vyžadovaného těmito právními akty Unie. Pokud se na produkt s digitálními prvky nevztahují určité základní požadavky na kybernetickou bezpečnost, výrobce do této technické dokumentace zahrne jasné odůvodnění.

5. Pro účely splnění povinnosti stanovené v odstavci 1 musejí výrobci při začleňování komponent pocházejících od třetích stran postupovat s náležitou péčí, aby tyto komponenty nenarušovaly kybernetickou bezpečnost produktu s digitálními prvky, včetně případů začleňování komponent svobodného softwaru s otevřeným zdrojovým kódem, které nebyly dodány na trh v rámci obchodní činnosti.

6. Po zjištění zranitelnosti v určité komponenty, včetně komponenty s otevřeným zdrojovým kódem, která je začleněna do produktu s digitálními prvky, oznámí výrobci zranitelnost osobě nebo subjektu, který komponentu vyrábí nebo provádí její údržbu, a tuto zranitelnost řeší a sjednají nápravu v souladu s požadavky na řešení zranitelností uvedenými v příloze I části II. Pokud výrobci vyvinuli změnu softwaru nebo hardwaru s cílem řešit zranitelnost této komponenty, poskytnou příslušný kód nebo dokumentaci osobě nebo subjektu, který komponentu vyrábí nebo provádí její údržbu, a to případně ve strojově čitelném formátu.

7. Výrobci systematicky dokumentují relevantní aspekty kybernetické bezpečnosti týkající se produktů s digitálními prvky, a to způsobem, který je přiměřený povaze a kybernetickým bezpečnostním rizikům, včetně zranitelností, o nichž se dozvědí, a veškerých relevantních informací poskytnutých třetími stranami, a případně aktualizují posouzení kybernetického bezpečnostního rizika produktů.

8. Při uvádění produktu s digitálními prvky na trh a během doby podpory výrobci zajistí, aby se zranitelnostmi tohoto produktu, včetně zranitelností jeho komponent, bylo nakládáno účinně a v souladu se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I části II.

Výrobci stanoví dobu podpory tak, aby odrážela dobu, po kterou se očekává používání produktu, zejména s přihlédnutím k přiměřeným očekáváním uživatelů, k povaze produktu, včetně jeho zamýšleného účelu, a k příslušnému právu Unie, které určuje životnost produktů s digitálními prvky. Při stanovování doby podpory mohou výrobci rovněž zohlednit 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 specializovaná skupina pro správní spolupráci zřízená podle čl. 52 odst. 15 a Komise. Záležitosti, které je třeba vzít v úvahu při stanovován doby podpory, se zohledňují tak, aby byla zajištěna proporcionalita.

Aniž je dotčen druhý pododstavec, trvá doba podpory nejméně pět let. Pokud se očekává, že produkt s digitálními prvky bude používán méně než pět let, odpovídá doba podpory očekávané době použití.

S přihlédnutím k doporučením specializované skupiny pro správní spolupráci podle čl. 52 odst. 16 může Komise přijmout akty v přenesené pravomoci v souladu s článkem 61 za účelem doplnění tohoto nařízení upřesněním minimální doby podpory pro konkrétní kategorie produktů, u nichž údaje v oblasti dozoru nad trhem naznačují, že jejich doby podpory nejsou dostatečné.

Výrobci uvedou informace, které byly zohledněny při stanovování doby podpory produktu s digitálními prvky, v technické dokumentaci, jak je stanovena v příloze VII.

Výrobci mají vhodnou politiku a postupy, včetně politiky koordinovaného zveřejňování zranitelností podle přílohy I části II bodu 5, pro zpracování a nápravu možných zranitelností v produktu s digitálními prvky hlášených z interních nebo externích zdrojů.

9. Výrobci zajistí, aby každá bezpečnostní aktualizace uvedená v příloze I části II bodě 8, která byla zpřístupněna uživatelům během doby podpory, byla po vydání dále k dispozici po dobu nejméně deseti let, nebo po zbytek doby podpory, podle toho, které z těchto časových období je delší.

10. Pokud výrobce uvedl na trh další podstatně změněné verze softwarového produktu, může soulad se základním požadavkem na kybernetickou bezpečnost stanoveným v příloze I části II bodě 2 zajistit pouze pro verzi, kterou uvedl na trh jako poslední, za předpokladu, že uživatelé verzí, jež byly uvedeny na trh dříve, mají bezplatný přístup k verzi, která byla uvedena na trh jako poslední, a že jim nevznikají dodatečné náklady na úpravu hardwarového a softwarového prostředí, v němž používají původní verzi tohoto výrobku.

11. Výrobci mohou vést veřejné softwarové archivy, které rozšiřují přístup uživatelů k předchozím verzím. V takových případech jsou uživatelé snadno přístupným způsobem jasně informováni o rizicích spojených s používáním nepodporovaného softwaru.

12. Před uvedením produktu s digitálními prvky na trh vypracují výrobci technickou dokumentaci podle článku 31.

Výrobci provedou nebo nechají provést zvolené postupy posuzování shody podle článku 32.

Pokud byl v rámci postupu posuzování shody prokázán soulad produktu s digitálními prvky se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I části I a soulad postupů zavedených výrobcem se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I části II, vypracují výrobci EU prohlášení o shodě v souladu s článkem 28 a umístí označení CE v souladu s článkem 30.

13. Výrobci technickou dokumentaci a EU prohlášení o shodě uchovávají pro potřebu orgánů dozoru nad trhem po dobu nejméně deseti let od uvedení produktu s digitálními prvky na trh nebo po dobu trvání doby podpory, podle toho, které z těchto časových období je delší.

14. Výrobci zajistí, aby byly zavedeny postupy, díky nimž produkty s digitálními prvky, které jsou součástí sériové výroby, zůstanou ve shodě s tímto nařízením. Výrobci náležitě přihlédnou ke změnám ve vývoji a výrobním postupu nebo v návrhu či vlastnostech produktu s digitálními prvky a změnám harmonizovaných norem, evropských schémat certifikace kybernetické bezpečnosti nebo společných specifikací uvedených v článku 27, na jejichž základě se prohlašuje nebo ověřuje shoda produktu s digitálními prvky.

15. Výrobci zajistí, aby bylo na jejich produktech s digitálními prvky uvedeno číslo typu, šarže nebo série či jiný prvek umožňující jejich identifikaci, nebo pokud to není možné, aby byla tato informace uvedena na obalu nebo v dokumentu přiloženém k produktu s digitálními prvky.

16. Výrobci na produktu s digitálními prvky, na jeho obalu nebo v dokumentu přiloženém k tomuto produktu uvedou své jméno, zapsaný obchodní název nebo zapsanou ochrannou známku výrobce a poštovní adresu, e-mailovou adresu nebo jiné digitální kontaktní údaje, a případně internetovou stránku, na níž lze výrobce kontaktovat. Tyto údaje jsou obsaženy rovněž v informacích a pokynech pro uživatele stanovených v příloze II. Kontaktní údaje se uvádějí v jazyce snadno srozumitelném uživatelům a orgánům dozoru nad trhem.

17. Pro účely tohoto nařízení určí výrobci jednotné kontaktní místo, které uživatelům umožní s nimi přímo a rychle komunikovat, mimo jiné s cílem usnadnit oznamování zranitelností produktu s digitálními prvky.

Výrobci zajistí, aby bylo jednotné kontaktní místo pro uživatele snadno identifikovatelné. Jednotné kontaktní místo uvedou také v informacích a pokynech pro uživatele stanovených v příloze II.

Jednotné kontaktní místo uživatelům umožní zvolit si upřednostňované komunikační prostředky a neomezí tyto prostředky na automatizované nástroje.

18. Výrobci zajistí, aby k produktům s digitálními prvky byly v papírové nebo elektronické podobě přiloženy informace a pokyny pro uživatele stanovené v příloze II. Tyto informace a pokyny jsou poskytnuty v jazyce snadno srozumitelném uživatelům a orgánům dozoru nad trhem. Jsou jasné, srozumitelné, snadno pochopitelné a čitelné. Umožňují bezpečnou instalaci, provoz a používání produktů s digitálními prvky. Výrobci tyto informace a pokyny pro uživatele stanovené v příloze II uchovávají pro potřebu uživatelů a orgánů dozoru nad trhem po dobu nejméně deseti let od uvedení produktu s digitálními prvky na trh nebo po dobu trvání doby podpory, podle toho, které z těchto časových období je delší. Pokud jsou tyto informace a pokyny poskytovány online, výrobci zajistí, aby byly přístupné, uživatelsky přívětivé a dostupné online po dobu nejméně deseti let od uvedení produktu s digitálními prvky na trh nebo po dobu trvání doby podpory, podle toho, které z těchto časových období je delší.

19. Výrobci zajistí, aby byl v době nákupu jasně a srozumitelně uveden alespoň měsíc a rok skončení doby podpory stanovené v odstavci 8, snadno přístupným způsobem, a to na produktu s digitálními prvky, případně na jeho obalu nebo digitálními prostředky.

Je-li to s ohledem na povahu produktu s digitálními prvky technicky proveditelné, zobrazí výrobci uživatelům oznámení, kterým je informují o tom, že jejich produktu s digitálními prvky končí doba podpory.

20. Výrobci k produktu s digitálními prvky přiloží buď kopii EU prohlášení o shodě, nebo zjednodušené EU prohlášení o shodě. Je-li poskytnuto zjednodušené EU prohlášení o shodě, musí obsahovat přesnou internetovou adresu, kde je přístupné celé EU prohlášení o shodě.

21. Od uvedení na trh a po dobu podpory výrobci, kteří vědí nebo mají důvod se domnívat, že produkt s digitálními prvky nebo postupy zavedené výrobcem nejsou ve shodě se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I, přijmou okamžitě nápravná opatření nezbytná k dosažení shody produktu s digitálními prvky nebo postupů výrobce nebo případně ke stažení produktu z trhu či z oběhu.

22. Výrobci poskytnou orgánu dozoru nad trhem na základě jeho odůvodněné žádosti v jazyce, kterému tento orgán snadno rozumí, všechny informace a dokumentaci v papírové nebo elektronické podobě nezbytnou k prokázání shody produktu s digitálními prvky a postupů zavedených výrobcem se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I. Na žádost tohoto orgánu s ním výrobci spolupracují na veškerých opatřeních přijatých k odstranění kybernetických bezpečnostních rizik představovaných produktem s digitálními prvky, který uvedli na trh.

23. Výrobce, který ukončí svou činnost, a v důsledku toho není schopen dodržovat toto nařízení, informuje před tím, než ukončení činnosti nabude účinku, příslušné orgány dozoru nad trhem a v co největší míře také uživatele příslušných produktů s digitálními prvky uvedené na trh o nadcházejícím ukončení činnosti.

24. Komise může prostřednictvím prováděcích aktů zohledňujících evropské nebo mezinárodní normy a osvědčené postupy stanovit formát a prvky softwarového kusovníku uvedeného v příloze I části II bodě 1. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 62 odst. 2.

25. Za účelem posouzení závislosti členských států a Unie jako celku na softwarových komponentách, a zejména na komponentách, které jsou považovány za svobodný software s otevřeným zdrojovým kódem, se může specializovaná skupina pro správní spolupráci rozhodnout provést celounijní posouzení závislosti u konkrétních kategorií produktů s digitálními prvky. Za tímto účelem mohou orgány dozoru nad trhem požádat výrobce těchto kategorií produktů s digitálními prvky, aby poskytli příslušné softwarové kusovníky uvedené v příloze I části II bodě 1. Na základě těchto informací mohou orgány dozoru nad trhem poskytnout specializované skupině pro správní spolupráci anonymizované souhrnné informace o závislosti na softwaru. Specializovaná skupina pro správní spolupráci předloží zprávu o výsledcích posouzení závislosti skupině pro spolupráci zřízené podle článku 14 směrnice (EU) 2022/2555.

Článek 14

Povinnosti výrobců podávat zprávy

1. Výrobce každou aktivně zneužívanou zranitelnost obsaženou v produktu s digitálními prvky, o níž se dozví, oznámí současně týmu CSIRT určenému jako koordinátor a agentuře ENISA v souladu s odstavcem 7 tohoto článku. Výrobce tuto aktivně zneužívanou zranitelnost oznámí prostřednictvím jednotné platformy pro podávání zpráv zřízené podle článku 16.

2. Pro účely oznamování ve smyslu odstavce 1 výrobce předloží:

a) včasné varování o aktivně zneužívané zranitelnosti, a to bez zbytečného odkladu a v každém případě do 24 hodin od okamžiku, kdy se o ní dozví, případně s uvedením členských států, na jejichž území je podle vědomostí výrobce jeho produkt s digitálními prvky zpřístupněn,

b) pokud již nebyly poskytnuty příslušné informace, oznámení o zranitelnosti, a to bez zbytečného odkladu a v každém případě do 72 hodin od okamžiku, kdy se o aktivně zneužívané zranitelnosti dozví, které obsahuje dostupné obecné informace o dotčeném produktu s digitálními prvky, o obecné povaze zneužívání a dotčené zranitelnosti, o veškerých přijatých nápravných nebo zmírňujících opatřeních a o nápravných nebo zmírňujících opatřeních, která mohou přijmout uživatelé, a v němž je případně rovněž uvedeno, nakolik výrobce považuje oznámené informace za citlivé,

c) pokud ještě nebyly příslušné informace poskytnuty, závěrečnou zprávu nejpozději do 14 dnů od okamžiku, kdy začalo být k dispozici nápravné nebo zmírňující opatření, která obsahuje alespoň tyto informace:

   i) popis zranitelnosti, včetně její závažnosti a dopadu,

   ii) případné informace o každém škodlivém aktéru, který zranitelnost zneužil nebo zneužívá,

   iii) podrobné informace o bezpečnostních aktualizacích nebo jiných nápravných opatřeních, které jsou k dispozici k odstranění zranitelnosti.

3. Výrobce každý závažný incident, který má dopad na bezpečnost produktu s digitálními prvky, o němž se dozví, oznámí v souladu s odstavcem 7 tohoto článku současně týmu CSIRT určenému jako koordinátor a agentuře ENISA. Výrobce tento incident oznámí prostřednictvím jednotné platformy pro podávání zpráv zřízené podle článku 16.

4. Pro účely oznamování ve smyslu odstavce 3 předloží výrobce:

a) včasné varování o závažném incidentu, který má dopad na bezpečnost produktu s digitálními prvky, a to bez zbytečného odkladu a v každém případě do 24 hodin od okamžiku, kdy se o něm dozví, včetně alespoň informace, zda existuje podezření, že byl incident způsoben nezákonným nebo škodlivým jednáním, případně také s uvedením členských států, na jejichž území je podle vědomostí výrobce jeho produkt s digitálními prvky zpřístupněn,

b) pokud již nebyly poskytnuty příslušné informace, oznámení o incidentu, a to bez zbytečného odkladu a v každém případě do 72 hodin od okamžiku, kdy se o incidentu dozví, které obsahuje dostupné obecné informace o povaze incidentu, o počátečním posouzení incidentu, o veškerých přijatých nápravných nebo zmírňujících opatřeních a o nápravných nebo zmírňujících opatřeních, která mohou přijmout uživatelé, a v němž je případně uvedeno, nakolik výrobce považuje oznámené informace za citlivé,

c) pokud již nebyly poskytnuty příslušné informace, závěrečnou zprávu nejpozději do jednoho měsíce od okamžiku, kdy bylo vydáno oznámení o incidentu podle písmene b), která obsahuje alespoň tyto informace:

i) podrobný popis incidentu včetně jeho závažnosti a dopadu,

ii) druh hrozby nebo základní příčinu, která incident pravděpodobně spustila,

iii) učiněná a probíhající zmírňující opatření.

5. Pro účely odstavce 3 se incident, který má dopad na bezpečnost produktu s digitálními prvky, považuje za závažný, pokud:

a) negativně ovlivňuje nebo může negativně ovlivnit schopnost produktu s digitálními prvky chránit dostupnost, autenticitu, integritu nebo důvěrnost citlivých či důležitých dat nebo funkcí; nebo

b) vedl či může vést k zavedení nebo spuštění škodlivého kódu v produktu s digitálními prvky nebo v síti a informačních systémech uživatele tohoto produktu.

6. V případě potřeby může tým CSIRT určený jako koordinátor, který obdržel oznámení jako první, výrobce požádat, aby mu poskytli průběžnou zprávu o relevantním vývoji týkajícím se aktivně zneužívané zranitelnosti nebo závažného incidentu, které mají dopad na bezpečnost produktu s digitálními prvky.

7. Oznámení uvedená v odstavcích 1 a 3 tohoto článku se podávají prostřednictvím jednotné platformy pro podávání zpráv uvedené v článku 16 za použití jednoho z koncových bodů elektronického oznamování uvedených v čl. 16 odst. 1. Oznámení se podává prostřednictvím koncového bodu elektronického oznamování týmu CSIRT určeného jako koordinátor toho členského státu, v němž mají výrobci hlavní provozovnu v Unii, a je současně přístupné agentuře ENISA.

Pro účely tohoto nařízení se má za to, že hlavní provozovnu má výrobce v Unii v tom členském státě, v němž jsou nejčastěji přijímána rozhodnutí týkající se kybernetické bezpečnosti jeho produktů s digitálními prvky. Nelze-li takový členský stát určit, má se za to, že dotčený výrobce má hlavní provozovnu v tom členském státě, v němž má provozovnu s nejvyšším počtem zaměstnanců v Unii.

Pokud výrobce v Unii nemá hlavní provozovnu, podává oznámení uvedená v odstavcích 1 a 3 prostřednictvím koncového bodu elektronického oznamování týmu CSIRT určenému jako koordinátor v členském státě, který je stanoven na základě informací, jež má výrobce k dispozici, a v tomto pořadí:

a) v členském státě, v němž je usazen zplnomocněný zástupce jednající jménem výrobce pro nejvyšší počet produktů s digitálními prvky tohoto výrobce,

b) v členském státě, v němž je usazen dovozce uvádějící na trh nejvyšší počet produktů s digitálními prvky tohoto výrobce,

c) v členském státě, v němž je usazen distributor, který dodává na trh nejvyšší počet produktů s digitálními prvky tohoto výrobce,

d) v členském státě, v němž se nachází nejvyšší počet uživatelů produktů s digitálními prvky tohoto výrobce.

V souvislosti s třetím pododstavcem písm. d) může výrobce podávat oznámení týkající se jakékoli následné aktivně zneužívané zranitelnosti nebo závažného incidentu, které mají dopad na bezpečnost produktu s digitálními prvky, témuž týmu CSIRT určenému jako koordinátor, jemuž podal prvotní oznámení.

8. Poté, co se dozví o aktivně zneužívané zranitelnosti nebo závažném incidentu, které mají dopad na bezpečnost produktu s digitálními prvky, výrobce informuje zasažené uživatele produktu s digitálními prvky, a případně všechny uživatele, o této zranitelnosti nebo incidentu; v případě potřeby informuje také o veškerých opatřeních na zmírnění rizik a nápravných opatřeních, která mohou uživatelé zavést ke zmírnění dopadu této zranitelnosti nebo incidentu, a to pokud možno ve strukturovaném, strojově čitelném a snadno automaticky zpracovatelném formátu. Pokud výrobce uživatele produktu s digitálními prvky neinformuje včas, mohou týmy CSIRT určené jako koordinátoři, které obdržely oznámení, tyto informace uživatelům poskytnout, je-li to považováno za přiměřené a nezbytné k předejití nebo zmírnění dopadu této zranitelnosti či incidentu.

9. Do 11. prosince 2025 přijme Komise akty v přenesené pravomoci v souladu s článkem 61 tohoto nařízení za účelem doplnění tohoto nařízení stanovením podmínek pro uplatňování důvodů souvisejících s kybernetickou bezpečností, pokud jde o odklad rozesílání oznámení podle čl. 16 odst. 2 tohoto nařízení. Komise při vypracovávání návrhu aktů v přenesené pravomoci spolupracuje se sítí CSIRT zřízenou podle článku 15 směrnice (EU) 2022/2555 a s agenturou ENISA.

10. Komise může prostřednictvím prováděcích aktů dále upřesnit formát a postupy oznamování uvedené v tomto článku a článcích 15 a 16. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 62 odst. 2. Komise při vypracovávání návrhů těchto prováděcích aktů spolupracuje se sítí CSIRT a s agenturou ENISA.

Článek 15

Dobrovolné podávání zpráv

1. Výrobci i jiné fyzické nebo právnické osoby mohou jakoukoliv zranitelnost produktu s digitálními prvky a rovněž kybernetické hrozby, které by mohly ovlivnit rizikový profil tohoto produktu, dobrovolně oznámit týmu CSIRT určenému jako koordinátor nebo agentuře ENISA.

2. Výrobci i jiné fyzické nebo právnické osoby mohou týmu CSIRT určenému jako koordinátor nebo agentuře ENISA dobrovolně oznámit každý incident, který má dopad na bezpečnost produktu s digitálními prvky, jakož i významné události, které k takovému incidentu téměř vedly.

3. Tým CSIRT určený jako koordinátor nebo agentura ENISA zpracuje oznámení uvedená v odstavcích 1 a 2 tohoto článku v souladu s postupem stanoveným v článku 16.

Tým CSIRT určený jako koordinátor může před zpracováním dobrovolných oznámení upřednostnit zpracování povinných oznámení.

4. Pokud aktivně zneužívanou zranitelnost nebo závažný incident, který má dopad na bezpečnost produktu s digitálními prvky, oznámí v souladu s odstavcem 1 nebo 2 fyzická nebo právnická osoba jiná než výrobce, informuje o tom tým CSIRT určený jako koordinátor bez zbytečného odkladu výrobce.

5. Tým CSIRT určený jako koordinátor a agentura ENISA zajistí důvěrnost a odpovídající ochranu informací poskytnutých oznamující fyzickou nebo právnickou osobou. Aniž je dotčena prevence, vyšetřování, odhalování a stíhání trestných činů, nesmí vést dobrovolné oznámení vést k tomu, aby oznamující právnické nebo fyzické osobě byly uloženy další povinnosti, které by neměla, pokud by dané oznámení nepodala.

Článek 16

Zřízení jednotné platformy pro podávání zpráv

1. Pro účely oznámení uvedených v čl. 14 odst. 1 a 3 a čl. 15 odst. 1 a 2 a s cílem zjednodušit povinnosti výrobců podávat zprávy zřídí agentura ENISA jednotnou platformu pro podávání zpráv. Každodenní provoz této platformy řídí a udržuje agentura ENISA. Struktura jednotné platformy pro podávání zpráv umožní členským státům a agentuře ENISA zavést vlastní koncové body elektronického oznamování.

2. Tým CSIRT určený jako koordinátor, který obdrží oznámení jako první, jej prostřednictvím jednotné platformy pro podávání zpráv neprodleně rozešle týmům CSIRT určeným jako koordinátoři, na jejichž území byl podle informací výrobce produkt s digitálními prvky zpřístupněn.

Za výjimečných okolností, a zejména na žádost výrobce a s ohledem na úroveň citlivosti oznámených informací uvedenou výrobcem podle čl. 14 odst. 2 písm. a) tohoto nařízení, může být rozesílání oznámení z opodstatněných důvodů souvisejících s kybernetickou bezpečností po nezbytně nutnou dobu odloženo, a to i tehdy, když se na zranitelnost vztahuje postup koordinovaného zveřejňování zranitelností podle čl. 12 odst. 1 směrnice (EU) 2022/2555. Pokud se tým CSIRT rozhodne rozesílání oznámení odložit, neprodleně o tomto rozhodnutí informuje agenturu ENISA, odklad zdůvodní a zároveň uvede, kdy bude v souladu s postupem pro rozesílání informací stanoveným v tomto odstavci oznámení rozesílat. Při uplatňování důvodů souvisejících s kybernetickou bezpečností v souvislosti s odkladem rozesílání uvedených oznámení může být týmu CSIRT nápomocna agentura ENISA.

Za zvláště výjimečných okolností, pokud výrobce v oznámení podle čl. 14 odst. 2 písm. b) uvede, že:

a) oznámená zranitelnost je aktivně zneužívána škodlivým aktérem a podle dostupných informací není zneužívána v žádném jiném členském státě, než je členský stát týmu CSIRT, který byl určen jako koordinátor, jemuž výrobce zranitelnost oznámil,

b) okamžité další rozesílání oznámení o dané zranitelnosti by pravděpodobně vedlo k poskytnutí informací, jejichž zveřejnění by bylo v rozporu se zásadními zájmy tohoto členského státu, nebo

c) oznámená zranitelnost představuje bezprostřední vysoké kybernetické bezpečnostní riziko vyplývající z dalšího šíření těchto informací,

jsou agentuře ENISA souběžně zpřístupněny pouze informace o tom, že výrobce podal oznámení, obecné informace o produktu, informace o obecné povaze zneužívání a informace o tom, že byly uvedeny důvody související s bezpečností, a to až do chvíle, než bude dotčeným týmům CSIRT a agentuře ENISA rozesláno úplné oznámení. Pokud se agentura ENISA na základě těchto informací domnívá, že existuje systémové riziko ovlivňující bezpečnost na vnitřním trhu, doporučí týmu CSIRT, který získal oznámení jako první, aby ostatním týmům CSIRT určeným jako koordinátoři i samotné agentuře ENISA zaslal úplné oznámení.

3. Po obdržení oznámení o aktivně zneužívané zranitelnosti produktu s digitálními prvky nebo o závažném incidentu, který má dopad na bezpečnost produktu s digitálními prvky, poskytnou týmy CSIRT určené jako koordinátoři orgánům dozoru nad trhem ve svých příslušných členských státech oznámené informace nezbytné k tomu, aby orgány dozoru nad trhem mohly plnit své povinnosti podle tohoto nařízení.

4. Agentura ENISA přijme vhodná a přiměřená technická, provozní a organizační opatření k řízení rizik ohrožujících bezpečnost jednotné platformy pro podávání zpráv a informací předkládaných nebo rozesílaných prostřednictvím jednotné platformy pro podávání zpráv. Každý bezpečnostní incident, který má dopad na jednotnou platformu pro podávání zpráv, oznámí bez zbytečného odkladu síti CSIRT a Komisi.

5. Agentura ENISA ve spolupráci se sítí CSIRT poskytuje a uplatňuje specifikace technických, provozních a organizačních opatření týkajících se zřízení, údržby a bezpečného provozu jednotné platformy pro podávání zpráv uvedené v odstavci 1, a to včetně alespoň bezpečnostních opatření týkajících se zřízení, provozu a údržby jednotné platformy pro podávání zpráv, jakož i koncových bodů elektronického oznamování zřízených na úrovni členských států týmy CSIRT určenými jako koordinátoři a na úrovni Unie agenturou ENISA, včetně procesních aspektů, a sice s cílem zajistit, aby v případě, že pro oznámenou zranitelnost nejsou k dispozici žádná nápravná ani zmírňující opatření, byly informace o této zranitelnosti poskytovány v souladu s přísnými bezpečnostními protokoly a na základě zásady „vědět jen to nejnutnější“ (need to know).

6. Pokud byl tým CSIRT určený jako koordinátor upozorněn na aktivně zneužívanou zranitelnost v rámci postupu koordinovaného zveřejňování zranitelností podle čl. 12 odst. 1 směrnice (EU) 2022/2555, může tým CSIRT určený jako koordinátor, který obdržel oznámení jako první, odložit rozesílání příslušného oznámení prostřednictvím jednotné platformy pro podávání zpráv na základě oprávněných důvodů souvisejících s kybernetickou bezpečností na nezbytně nutnou dobu, a to až do okamžiku, než získá souhlas stran zapojených do koordinovaného zveřejňování zranitelností. Tento požadavek nebrání výrobcům v dobrovolném oznamování dané zranitelnosti v souladu s postupem stanoveným v tomto článku.

Článek 17

Další ustanovení týkající se podávání zpráv

1. Agentura ENISA může Evropské síti styčných organizací pro řešení kybernetických krizí (EU-CyCLONe) zřízené článkem 16 směrnice (EU) 2022/2555 poskytovat informace oznámené podle čl. 14 odst. 1 a 3 a čl. 15 odst. 1 a 2 tohoto nařízení, pokud jsou tyto informace relevantní z hlediska koordinovaného řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí na operativní úrovni. Při určování toho, zda jsou tyto informace relevantní, může agentura ENISA zohlednit technické analýzy provedené sítí CSIRT, jsou-li k dispozici.

2. Je-li k prevenci nebo ke zmírnění závažného incidentu, který má dopad na bezpečnost produktu s digitálními prvky, nebo k řešení probíhajícího incidentu nezbytná informovanost veřejnosti, nebo pokud je zveřejnění incidentu jinak ve veřejném zájmu, může tým CSIRT určený jako koordinátor v příslušném členském státě po konzultaci s dotčeným výrobcem a případně ve spolupráci s agenturou ENISA o incidentu informovat veřejnost nebo požádat výrobce, aby tak učinil.

3. Agentura ENISA na základě oznámení obdržených podle čl. 14 odst. 1 a 3 a čl. 15 odst. 1 a 2 tohoto nařízení vypracuje každých 24 měsíců odbornou zprávu o nových trendech týkajících se kybernetických bezpečnostních rizik u produktů s digitálními prvky a předloží ji skupině pro spolupráci zřízené podle článku 14 směrnice (EU) 2022/2555. První z těchto zpráv je nutné předložit do 24 měsíců ode dne, kdy se začaly uplatňovat povinnosti stanovené v čl. 14 odst. 1 a 3. Agentura ENISA zahrne příslušné informace ze svých odborných zpráv do své zprávy o stavu kybernetické bezpečnosti v Unii podle článku 18 směrnice (EU) 2022/2555.

4. Pouhé oznámení podle čl. 14 odst. 1 a 3 nebo čl. 15 odst. 1 a 2 nepředstavuje pro oznamující subjekt vyšší míru právní odpovědnosti oznamujícího subjektu..

5. Poté, co je k dispozici bezpečnostní aktualizace nebo jiná forma nápravného či zmírňujícího opatření, přidá agentura ENISA po dohodě s výrobcem dotčeného produktu s digitálními prvky veřejně známou zranitelnost oznámenou podle čl. 14 odst. 1 nebo čl. 15 odst. 1 tohoto nařízení do evropské databáze zranitelností zřízené podle čl. 12 odst. 2 směrnice (EU) 2022/2555.

6. Týmy CSIRT určené jako koordinátoři poskytují v souvislosti s povinností podávat zprávy podle článku 14 helpdesk podporu výrobcům, a to především těm, kteří naplňují definici mikropodniků nebo malých či středních podniků.

Článek 18

Zplnomocnění zástupci

1. Výrobce může písemným pověřením jmenovat zplnomocněného zástupce.

2. Povinnosti stanovené v čl. 13 odst. 1 až 11, čl. 13 odst. 12 prvním pododstavci a čl. 13 odst. 14 nejsou součástí pověření zplnomocněného zástupce.

3. Zplnomocněný zástupce plní úkoly stanovené v pověření, které obdržel od výrobce. Na vyžádání poskytne kopii pověření orgánům dozoru nad trhem. Pověření musí zplnomocněnému zástupci umožňovat alespoň:

a) uchovávat EU prohlášení o shodě podle článku 28 a technickou dokumentaci uvedenou v článku 31 pro potřebu orgánů dozoru nad trhem po dobu nejméně deseti let od uvedení produktu s digitálními prvky na trh nebo po dobu trvání doby podpory, podle toho, které z těchto časových období je delší,

b) poskytnout příslušnému orgánu dozoru nad trhem na základě jeho odůvodněné žádosti veškeré informace a dokumentaci nezbytné k prokázání shody produktu s digitálními prvky,

c) spolupracovat s orgány dozoru nad trhem na jejich žádost při veškerých činnostech, jejichž cílem je odstranit rizika vyvolaná produktem s digitálními prvky, na který se vztahuje pověření zplnomocněného zástupce.

Článek 19

Povinnosti dovozců

1. Dovozci uvádějí na trh pouze produkty s digitálními prvky, které splňují základní požadavky na kybernetickou bezpečnost stanovené v příloze I části I a u nichž jsou postupy zavedené výrobcem v souladu se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I části II.

2. Před uvedením produktu s digitálními prvky na trh dovozci zajistí, aby:

a) výrobce provedl příslušné postupy posuzování shody podle článku 32,

b) výrobce vypracoval technickou dokumentaci,

c) produkt s digitálními prvky byl opatřen označením CE podle článku 30 a bylo k němu přiloženo EU prohlášení o shodě podle čl. 13 odst. 20 a informace a pokyny pro uživatele stanovené v příloze II v jazyce snadno srozumitelném uživatelům a orgánům dozoru nad trhem,

d) výrobce splnil požadavky stanovené v čl. 13 odst. 15, 16 a 19.

Pro účely tohoto odstavce musí být dovozci schopni poskytnout nezbytné dokumenty prokazující splnění požadavků stanovených v tomto článku.

3. Jestliže se dovozce domnívá nebo má důvod se domnívat, že produkt s digitálními prvky nebo postupy zavedené výrobcem nejsou ve shodě s tímto nařízením, neuvede dovozce produkt na trh, dokud u tohoto produktu nebo u postupů zavedených výrobcem nebude dosaženo shody s tímto nařízením. Pokud navíc produkt s digitálními prvky představuje významné kybernetické bezpečnostní riziko, informuje o tom dovozce výrobce a orgány dozoru nad trhem.

Pokud má dovozce důvod se domnívat, že určitý produkt s digitálními prvky může představovat významné kybernetické bezpečnostní riziko s ohledem na rizikové faktory jiné než technické povahy, informuje o tom orgány dozoru nad trhem. Po obdržení takovýchto informací se orgány dozoru nad trhem řídí postupy uvedenými v čl. 54 odst. 2.

4. Dovozci uvedou na produktu s digitálními prvky nebo na jeho obalu či v dokumentu přiloženém k tomuto produktu své jméno, zapsaný obchodní název nebo zapsanou ochrannou známku, poštovní adresu, e-mailovou adresu nebo jiné digitální kontaktní údaje, a případně internetovou stránku, na níž je lze kontaktovat. Kontaktní údaje se uvádějí v jazyce snadno srozumitelném uživatelům a orgánům dozoru nad trhem.

5. Dovozci, kteří vědí nebo mají důvod se domnívat, že produkt s digitálními prvky, který uvedli na trh, není v souladu s tímto nařízením, přijmou okamžitě nápravná opatření nezbytná k zajištění toho, aby byl produkt s digitálními prvky uveden do souladu s tímto nařízením, nebo aby byl v případě potřeby stažen z trhu či z oběhu.

Poté, co se dovozci dozvědí o zranitelnosti produktu s digitálními prvky, informují o této zranitelnosti bez zbytečného odkladu výrobce. Dále, pokud produkt s digitálními prvky představuje významné kybernetické bezpečnostní riziko, informují o tom dovozci neprodleně orgány dozoru nad trhem v členských státech, v nichž produkt s digitálními prvky dodali na trh, a uvedou podrobnosti, zejména o nesouladu a o přijatých nápravných opatřeních.

6. Dovozci po dobu alespoň deseti let od uvedení produktu s digitálními prvky na trh nebo po dobu trvání doby podpory, podle toho, které z těchto časových období je delší, uchovávají kopii EU prohlášení o shodě pro potřebu orgánů dozoru nad trhem a zajišťují, aby těmto orgánům mohla být na žádost předložena technická dokumentace.

7. Dovozci poskytnou orgánu dozoru nad trhem na základě jeho odůvodněné žádosti všechny informace a dokumentaci v tištěné nebo elektronické podobě, které jsou nezbytné k prokázání shody produktu s digitálními prvky se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I části I, jakož i shody postupů zavedených výrobcem se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I části II, a to v jazyce snadno srozumitelném

tomuto orgánu. Spolupracují s tímto orgánem na jeho žádost na veškerých opatřeních přijatých k odstranění kybernetických bezpečnostních rizik představovaných produktem s digitálními prvky, který uvedli na trh.

8. Pokud se dovozce produktu s digitálními prvky dozví, že výrobce tohoto produktu ukončil svou činnost, a v důsledku toho není schopen splnit povinnosti stanovené v tomto nařízení, informuje o této situaci příslušné orgány dozoru nad trhem a jakýmikoli dostupnými prostředky a v co největší míře také uživatele produktů s digitálními prvky uváděných na trh.

Článek 20

Povinnosti distributorů

1. Při dodávání produktu s digitálními prvky na trh distributoři jednají s řádnou péčí, pokud jde o požadavky stanovené v tomto nařízení.

2. Před dodáním produktu s digitálními prvky na trh dovozci ověří, že:

a) produkt s digitálními prvky je opatřen označením CE,

b) výrobce a dovozce splnili povinnosti uvedené v čl. 13 odst. 15, 16, 18, 19 a 20 a čl. 19 odst. 4 a předali veškeré nezbytné dokumenty distributorovi.

3. Jestliže se distributor na základě informací, které má k dispozici, domnívá nebo má důvod se domnívat, že produkt s digitálními prvky nebo postupy zavedené výrobcem nejsou ve shodě se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I, nesmí dodat produkt s digitálními prvky na trh, dokud tento produkt nebo postupy zavedené výrobcem nedosáhnou shody s tímto nařízením. Pokud navíc produkt s digitálními prvky představuje významné kybernetické bezpečnostní riziko, informuje o tom distributor bez zbytečného odkladu výrobce a orgány dozoru nad trhem.

4. Distributoři, kteří na základě informací, jež mají k dispozici, vědí nebo mají důvod se domnívat, že produkt s digitálními prvky, který dodali na trh, nebo postupy zavedené jeho výrobcem nejsou ve shodě s tímto nařízením, zajistí, aby byla přijata nápravná opatření nezbytná k tomu, aby produkt s digitálními prvky nebo postupy zavedené jeho výrobcem dosáhly shody, nebo případně ke stažení tohoto produktu z trhu nebo z oběhu.

Poté, co se dozvědí o zranitelnosti produktu s digitálními prvky, informují distributoři o této zranitelnosti bez zbytečného odkladu výrobce. Dále, pokud produkt s digitálními prvky představuje významné kybernetické bezpečnostní riziko, informují o tom distributoři neprodleně orgány dozoru nad trhem členských států, v nichž produkt s digitálními prvky dodali na trh, a uvedou podrobnosti, zejména o nesouladu a o přijatých nápravných opatřeních.

5. Distributoři poskytnou orgánu dozoru nad trhem na základě jeho odůvodněné žádosti všechny informace a dokumentaci v tištěné nebo elektronické podobě, které jsou nezbytné k prokázání shody produktu s digitálními prvky a postupů zavedených jeho výrobcem s tímto nařízením, a to v jazyce snadno srozumitelném tomuto orgánu. Spolupracují s tímto orgánem na jeho žádost na veškerých opatřeních přijatých k odstranění kybernetických bezpečnostních rizik představovaných produktem s digitálními prvky, který dodali na trh.

6. Pokud distributor produktu s digitálními prvky na základě informací, které má k dispozici, zjistí, že výrobce tohoto produktu ukončil svou činnost, a v důsledku toho není schopen splnit povinnosti stanovené v tomto nařízení, informuje o této situaci bez zbytečného odkladu příslušné orgány dozoru nad trhem a jakýmikoli dostupnými prostředky a v co největší míře také uživatele produktů s digitálními prvky uváděných na trh.

Článek 21

Případy, kdy se povinnosti výrobců vztahují na dovozce a distributory

Dovozce nebo distributor je pro účely tohoto nařízení považován za výrobce a vztahují se na něj ustanovení článku 13 a 14, pokud tento dovozce nebo distributor uvede na trh produkt s digitálními prvky pod svým jménem nebo pod svou ochrannou známkou nebo provede podstatnou změnu produktu s digitálními prvky, který již byl na trh uveden.

Článek 22

Ostatní případy, na něž se vztahují povinnosti výrobců

1. Fyzická nebo právnická osoba jiná než výrobce, dovozce nebo distributor, která provádí podstatnou změnu produktu s digitálními prvky a dodává tento produkt na trh, se pro účely tohoto nařízení považuje za výrobce.

2. Na osobu uvedenou v odstavci 1 tohoto článku se vztahují povinnosti stanovené v článku 13 a 14, ohledně části produktu s digitálními prvky, která je touto podstatnou změnou ovlivněna, nebo jestliže má tato podstatná změna dopad na kybernetickou bezpečnost produktu s digitálními prvky jako celku, ohledně celého produktu.

Článek 23

Identifikace hospodářských subjektů

1. Hospodářské subjekty poskytnou orgánům dozoru nad trhem na žádost následující informace:

a) jméno a adresu každého hospodářského subjektu, který jim dodal produkt s digitálními prvky,

b) název a adresu každého hospodářského subjektu, kterému dodaly produkt s digitálními prvky, jsou-li k dispozici.

2. Hospodářské subjekty musejí být schopny poskytnout informace uvedené v odstavci 1 po dobu deseti let poté, co jim byl produkt s digitálními prvky dodán, a po dobu deseti let poté, co produkt s digitálními prvky dodaly.

Článek 24

Povinnosti správců softwaru s otevřeným zdrojovým kódem

1. Správci softwaru s otevřeným zdrojovým kódem zavedou a ověřitelným způsobem zdokumentují politiku kybernetické bezpečnosti, která podporuje vývoj bezpečného produktu s digitálními prvky a efektivní řešení zranitelností vývojáři daného produktu. Tato politika podporuje také dobrovolné hlášení zranitelností vývojáři daného produktu, jak je stanoveno v článku 15, a zohledňuje specifickou povahu správce softwaru s otevřeným zdrojovým kódem a právní a organizační opatření, která se na něj vztahují. Tato politika zahrnuje především aspekty související s dokumentací, řešením a odstraňováním zranitelností a podporuje sdílení informací týkajících se zjištěných zranitelností v rámci komunity zabývající se vývojem softwaru s otevřeným zdrojovým kódem.

2. Správci softwaru s otevřeným zdrojovým kódem spolupracují, jsou-li o to požádáni, s orgány dozoru nad trhem na zmírnění kybernetických bezpečnostních rizik, která představuje produkt s digitálními prvky považovaný za svobodný software s otevřeným zdrojovým kódem.

Na základě odůvodněné žádosti orgánu dozoru nad trhem poskytnou správci softwaru s otevřeným zdrojovým kódem tomuto orgánu dokumentaci uvedenou v odstavci 1, a to v tištěné nebo elektronické podobě a v jazyce, který je pro něj snadno srozumitelný.

3. Povinnosti stanovené v čl. 14 odst. 1 se na správce softwaru s otevřeným zdrojovým kódem uplatní do té míry, do jaké jsou zapojeni do vývoje produktů s digitálními prvky. Povinnosti stanovené v čl. 14 odst. 3 a 8 se na správce softwaru s otevřeným zdrojovým kódem uplatní do té míry, do jaké závažné incidenty s dopadem na bezpečnost produktů s digitálními prvky ovlivňují síť a informační systémy poskytované správci softwaru s otevřeným zdrojovým kódem k vývoji takových produktů.

Článek 25

Potvrzení o bezpečnosti svobodného softwaru s otevřeným zdrojovým kódem

S cílem usnadnit plnění povinnosti náležité péče stanovené v čl. 13 odst. 5, zejména pokud jde o výrobce, kteří do svých produktů s digitálními prvky začleňují komponenty sestávající ze svobodného softwaru s otevřeným zdrojovým kódem, je Komisi svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 61 za účelem doplnění tohoto nařízení zavedením programů dobrovolného potvrzení o bezpečnosti, které vývojářům nebo uživatelům produktů s digitálními prvky považovaných za svobodný software s otevřeným zdrojovým kódem a dalším třetím stranám umožní posoudit shodu těchto produktů se všemi nebo některými základními požadavky na kybernetickou bezpečnost či jinými povinnostmi stanovenými v tomto nařízení.

Článek 26

Pokyny

1. S cílem usnadnit důsledné uplatňování tohoto nařízení zveřejní Komise doporučující pokyny, které hospodářským subjektům pomohou s jeho uplatňováním, a to zejména s důrazem na usnadnění jeho dodržování mikropodnikům a malým a středním podnikům.

2. Pokud má Komise v úmyslu poskytnout pokyny podle odstavce 1, bude se zabývat přinejmenším následujícími aspekty:

a) oblastí působnosti tohoto nařízení se zvláštním důrazem na řešení pro zpracování dat na dálku a na svobodný software s otevřeným zdrojovým kódem,

b) používáním doby podpory ve vztahu k určitým kategoriím produktů s digitálními prvky,

c) pokyny pro výrobce, na které se vztahuje toto nařízení i jiné harmonizační právní předpisy Unie, než je toto nařízení, či další související právní akty Unie,

d) koncepcí podstatné změny.

Komise rovněž vede snadno přístupný seznam aktů v přenesené pravomoci a prováděcích aktů přijatých podle tohoto nařízení.

3. Při přípravě pokynů podle tohoto článku Komise vede konzultace s příslušnými zúčastněnými stranami.

KAPITOLA III

SHODA PRODUKTU S DIGITÁLNÍMI PRVKY

Článek 27

Předpoklad shody

1. Předpokládá se, 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*, jsou ve shodě se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I, na které se tyto normy nebo jejich části vztahují.

Komise v souladu s čl. 10 odst. 1 nařízení (EU) č. 1025/2012 požádá jednu nebo více evropských normalizačních organizací o vypracování harmonizovaných norem pro základní požadavky na kybernetickou bezpečnost stanovené v příloze I tohoto nařízení. Při přípravě žádosti o normalizaci pro účely tohoto nařízení usiluje Komise o zohlednění stávajících evropských nebo mezinárodních norem pro kybernetickou bezpečnost, které byly zavedeny nebo jsou vyvíjeny, s cílem zjednodušit vypracování harmonizovaných norem, v souladu s nařízením (EU) č. 1025/2012.

2. Komise může přijmout prováděcí akty, jimiž stanoví společné specifikace týkající se technických požadavků, které představují prostředek ke splnění základních požadavků na kybernetickou bezpečnost stanovených v příloze I u produktů s digitálními prvky spadajících do oblasti působnosti tohoto nařízení.

Tyto prováděcí akty se přijmou, pouze pokud jsou splněny tyto podmínky:

a) Komise podle čl. 10 odst. 1 nařízení (EU) č. 1025/2012 požádala jednu nebo více evropských normalizačních organizací o vypracování harmonizované normy pro základní požadavky na kybernetickou bezpečnost stanovené v příloze I a:

   i) tato žádost nebyla přijata,

   ii) harmonizované normy, kterých se žádost týkala, nebyly dodány ve lhůtě stanovené v souladu s čl. 10 odst. 1 nařízení (EU) č. 1025/2012, nebo

   iii) harmonizované normy neodpovídají žádosti a

b) v *Úředním věstníku Evropské unie* nebyl v souladu s nařízením (EU) č. 1025/2012 zveřejněn odkaz na harmonizované normy, které se vztahují na příslušné základní požadavky na kybernetickou bezpečnost stanovené v příloze I tohoto nařízení, ani se neočekává, že takový odkaz bude v přiměřené lhůtě zveřejněn.

Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 62 odst. 2.

3. Před vypracováním návrhu prováděcího aktu podle odstavce 2 tohoto článku informuje Komise výbor uvedený v článku 22 nařízení (EU) č. 1025/2012 o tom, že se domnívá, že podmínky uvedené v odstavci 2 tohoto článku byly splněny.

4. Při vypracovávání návrhu prováděcího aktu podle odstavce 2 zohlední Komise stanoviska příslušných subjektů a vede řádné konzultace se všemi příslušnými zúčastněnými stranami.

5. Předpokládá se, že produkty s digitálními prvky a postupy zavedené výrobcem, které jsou ve shodě se společnými specifikacemi stanovenými v prováděcích aktech uvedených v odstavci 2 tohoto článku, nebo s jejich částmi, splňují základní požadavky na kybernetickou bezpečnost stanovené v příloze I, na které se vztahují tyto společné specifikace nebo jejich části.

6. Pokud je harmonizovaná norma přijata evropskou normalizační organizací a předložena Komisi ke zveřejnění odkazu na ni v *Úředním věstníku Evropské unie*, posoudí Komise tuto harmonizovanou normu v souladu s nařízením (EU) č. 1025/2012. Je-li odkaz na harmonizovanou normu zveřejněn v *Úředním věstníku Evropské unie*, Komise zruší prováděcí akty uvedené v odstavci 2 tohoto článku nebo jejich části, které se týkají stejných základních požadavků na kybernetickou bezpečnost jako požadavky uvedené v této harmonizované normě.

7. Pokud se členský stát domnívá, že společná specifikace zcela nesplňuje základní požadavky na kybernetickou bezpečnost stanovené v příloze I, uvědomí o tom Komisi prostřednictvím podrobného vysvětlení. Komise toto podrobné vysvětlení posoudí a v odůvodněném případě může prováděcí akt, kterým se daná společná specifikace stanovuje, změnit.

8. Předpokládá se, že 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, jsou ve shodě se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I, pokud se na tyto požadavky vztahuje EU prohlášení o shodě nebo evropský certifikát kybernetické bezpečnosti či jeho části.

9. Komisi je za účelem doplnění tohoto nařízení svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 61 tohoto nařízení, jimiž upřesní evropská schémata certifikace kybernetické bezpečnosti přijatá podle nařízení (EU) 2019/881, která lze použít k prokázání shody produktů s digitálními prvky se základními požadavky na kybernetickou bezpečnost nebo jejich částmi stanovenými v příloze I tohoto nařízení. Vydání evropského certifikátu kybernetické bezpečnosti vydaného v rámci těchto schémat alespoň na úrovni záruky „významná“ dále ruší povinnost výrobce nechat provést posouzení shody třetí stranou pro účely příslušných požadavků, jak je stanoveno v čl. 32 odst. 2 písm. a) a b) a čl. 32 odst. 3 písm. a) a b) tohoto nařízení.

Článek 28

EU prohlášení o shodě

1. EU prohlášení o shodě vypracují výrobci v souladu s čl. 13 odst. 12 a je v něm uvedeno, že bylo prokázáno splnění příslušných základních požadavků na kybernetickou bezpečnost stanovených v příloze I.

2. EU prohlášení o shodě je vypracováno podle vzoru uvedeného v příloze V a obsahuje prvky stanovené v příslušných postupech posuzování shody stanovených v příloze VIII. Toto prohlášení je podle potřeby aktualizováno. Prohlášení je k dispozici v jazycích požadovaných členským státem, v němž je produkt s digitálními prvky uváděn nebo dodáván na trh.

Zjednodušené EU prohlášení o shodě podle čl. 13 odst. 20 se vypracuje podle vzoru uvedeného v příloze VI. Je k dispozici v jazycích požadovaných členským státem, v němž je produkt s digitálními prvky uváděn nebo dodáván na trh.

3. Pokud se na produkt s digitálními prvky vztahuje více než jeden právní akt Unie vyžadující EU prohlášení o shodě, vypracuje se pro všechny tyto právní akty Unie jediné EU prohlášení o shodě. V prohlášení se uvedou dotčené právní akty Unie, včetně odkazů na jejich zveřejnění.

4. Vypracováním EU prohlášení o shodě přebírá výrobce odpovědnost za soulad produktu s digitálními prvky s příslušnými požadavky.

5. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 61 za účelem doplnění tohoto nařízení přidáním dalších prvků k minimálnímu obsahu EU prohlášení o shodě stanoveného v příloze V s cílem zohlednit technický vývoj.

Článek 29

Obecné zásady, kterými se řídí označení CE

Označení CE podléhá obecným zásadám uvedeným v článku 30 nařízení (ES) č. 765/2008.

Článek 30

Pravidla a podmínky pro umístění označení CE

1. Označení CE se umístí viditelně, čitelně a nesmazatelně na produkt s digitálními prvky. Pokud to vzhledem k povaze produktu s digitálními prvky není možné nebo opodstatněné, umístí se označení CE na obal a na EU prohlášení o shodě podle článku 28, které je přiloženo k produktu s digitálními prvky. U produktů s digitálními prvky, které jsou ve formě softwaru, se označení CE umístí buď na EU prohlášení o shodě podle článku 28, nebo na internetové stránky doprovázející softwarový produkt. V druhém případě musí být příslušná část internetové stránky snadno a přímo přístupná spotřebitelům.

2. Vzhledem k povaze produktu s digitálními prvky může být výška označení CE umístěného na produkt s digitálními prvky menší než 5 mm za předpokladu, že označení zůstane viditelné a čitelné.

3. Označení CE se umístí před uvedením produktu s digitálními prvky na trh. Za označením může následovat piktogram nebo jakákoli jiná značka označující zvláštní kybernetické bezpečnostní riziko nebo použití stanovené v prováděcích aktech podle odstavce 6.

4. Za označením CE následuje identifikační číslo oznámeného subjektu, je-li tento subjekt zapojen do postupu posuzování shody založeného na komplexním zabezpečování kvality (na základě modulu H) podle článku 32.

Identifikační číslo oznámeného subjektu umístí sám subjekt, nebo jej umístí podle jeho pokynů výrobce či zplnomocněný zástupce výrobce.

5. Členské státy vycházejí ze stávajících mechanismů, aby zajistily řádné uplatňování režimu označování CE, a přijmou vhodná opatření v případě nesprávného použití tohoto označení. Pokud se na produkt s digitálními prvky vztahují jiné harmonizační právní předpisy Unie, než je toto nařízení, které rovněž stanovují umístění označení CE, pak se v tomto označení uvede, že produkt splňuje také požadavky stanovené v těchto jiných harmonizačních právních předpisech Unie.

6. Komise může prostřednictvím prováděcích aktů stanovit technické specifikace pro označování, piktogramy nebo jakékoli jiné značky týkající se bezpečnosti produktů s digitálními prvky, dobu jejich podpory a mechanismy na podporu jejich používání a na zvýšení informovanosti veřejnosti o bezpečnosti produktů s digitálními prvky. Při vypracovávání návrhů prováděcích aktů vede Komise konzultace s příslušnými zúčastněnými stranami a se specializovanou skupinou pro správní spolupráci, pokud již byla zřízena podle čl. 52 odst. 15. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 62 odst. 2.

Článek 31

Technická dokumentace

1. Technická dokumentace musí obsahovat všechny příslušné údaje nebo podrobné informace o prostředcích, které výrobce použil k zajištění toho, aby produkt s digitálními prvky a postupy zavedené výrobcem byly v souladu se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I. Technická dokumentace obsahuje alespoň prvky stanovené v příloze VII.

2. Technická dokumentace se vypracuje před uvedením produktu s digitálními prvky na trh a ve vhodných případech je průběžně aktualizována přinejmenším během doby podpory.

3. Pro produkty s digitálními prvky podle článku 12, které se řídí i jinými právními akty Unie, které se zabývají technickou dokumentaci, se vypracuje jediný soubor technické dokumentace obsahující informace podle přílohy VII a informace požadované těmito právními akty Unie.

4. Technická dokumentace a korespondence týkající se jakéhokoli postupu posuzování shody se vypracuje v úředním jazyce členského státu, v němž je oznámený subjekt usazen, nebo v jazyce pro tento subjekt přijatelném.

5. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 61 za účelem doplnění tohoto nařízení přidáním prvků, které mají být zahrnuty do technické dokumentace stanovené v příloze VII, s cílem zohlednit technický vývoj i vývoj při uplatňování tohoto nařízení. Komise se za tímto účelem snaží zajistit, aby byla administrativní zátěž pro mikropodniky a malé a střední podniky přiměřená.

Článek 32

Postupy posuzování shody u produktů s digitálními prvky

1. Výrobce provede posouzení shody produktu s digitálními prvky a postupů, které zavedl, s cílem určit, zda jsou splněny základní požadavky na kybernetickou bezpečnost stanovené v příloze I. Výrobce prokazuje shodu se základními požadavky na kybernetickou bezpečnost v rámci některého z těchto postupů:

a) postupu interní kontroly (na základě modulu A) stanoveného v příloze VIII,

b) EU přezkoušení typu (na základě modulu B) podle přílohy VIII, po kterém následuje shoda s EU typem založená na interním řízení výroby (na základě modulu C) podle přílohy VIII,

c) posuzování shody založeného na komplexním zabezpečování kvality (na základě modulu H) podle přílohy VIII, nebo

d) případně, pokud je k dispozici, evropského schématu certifikace kybernetické bezpečnosti podle čl. 27 odst. 9.

2. Pokud při posuzování souladu důležitého produktu s digitálními prvky, který spadá do třídy I podle přílohy III, a postupů zavedených jeho výrobcem se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I výrobce nepoužil harmonizované normy, společné specifikace nebo evropská schémata certifikace kybernetické bezpečnosti alespoň na úrovni záruky „významná“ podle článku 27, nebo je použil pouze částečně, nebo jestliže takové harmonizované normy, společné specifikace nebo evropská schémata certifikace kybernetické bezpečnosti neexistují, použije se na dotčený produkt s digitálními prvky a na postupy zavedené výrobcem s ohledem na tyto základní požadavky na kybernetickou bezpečnost kterýkoliv z těchto postupů:

a) EU přezkoušení typu (na základě modulu B) podle přílohy VIII, po kterém následuje shoda s EU typem založená na interním řízení výroby (na základě modulu C) podle přílohy VIII, nebo

b) posuzování shody založené na komplexním zabezpečování kvality (na základě modulu H) podle přílohy VIII.

3. Pokud je produkt důležitým produktem s digitálními prvky, který spadá do třídy II podle přílohy III, výrobce prokáže shodu se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I v rámci některého z těchto postupů:

a) EU přezkoušení typu (na základě modulu B) podle přílohy VIII, po kterém následuje shoda s EU typem založená na interním řízení výroby (na základě modulu C) podle přílohy VIII,

b) posuzování shody založeného na komplexním zabezpečování kvality (na základě modulu H) podle přílohy VIII, nebo

c) případně, pokud je k dispozici, evropského schématu certifikace kybernetické bezpečnosti uvedeného v čl. 27 odst. 9 tohoto nařízení alespoň na úrovni záruky „významná“ podle nařízení (EU) 2019/881.

4. U kritických produktů s digitálními prvky uvedených v příloze IV se prokazuje shoda se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I v rámci jednoho z těchto postupů:

a) evropského schématu certifikace kybernetické bezpečnosti podle čl. 8 odst. 1, nebo

b) pokud nejsou splněny podmínky v čl. 8 odst. 1, některého z postupů uvedených v odst. 3 tohoto článku.

5. Výrobci produktů s digitálními prvky považovaných za svobodný software s otevřeným zdrojovým kódem, které patři do kategorií uvedených v příloze III, mají možnost prokázat shodu se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I v rámci jednoho z postupů uvedených v odst. 1 tohoto článku za předpokladu, že je v okamžiku uvedení těchto produktů na trh zpřístupněna veřejnosti technická dokumentace uvedená v článku 31.

6. Při stanovování poplatků za posuzování shody se vezmou v úvahu specifické zájmy a potřeby mikropodniků a malých a středních podniků, včetně začínajících podniků, a tyto poplatky se přiměřeně k jejich specifickým zájmům a potřebám sníží.

Článek 33

Podpůrná opatření pro mikropodniky a malé a střední podniky, včetně začínajících podniků

1. Členské státy ve vhodných případech přijmou opatření upravená pro potřeby mikropodniků a malých podniků, kterými:

a) zajistí konkrétní osvětovou a školicí činnost týkající se uplatňování tohoto nařízení,

b) zřídí vyhrazený kanál pro komunikaci s mikropodniky a malými podniky a případně s místními orgány veřejné správy s cílem poskytovat poradenství a reagovat na dotazy ohledně provádění tohoto nařízení,

c) podpoří činnost v oblasti testování a posuzování shody, případně s podporou Evropského centra kompetencí pro kybernetickou bezpečnost.

2. Členské státy mohou případně vytvořit regulační sandboxy pro kybernetickou odolnost. Tyto regulační sandboxy představují kontrolované testovací prostředí pro inovativní produkty s digitálními prvky, které by mělo usnadnit jejich vývoj, návrh, validaci a testování pro účely souladu s tímto nařízením po omezenou dobu před jejich uvedením na trh. Komise a případně agentura ENISA může poskytnout technickou podporu, poradenství a nástroje k vytvoření a provozování regulačních sandboxů. Regulační sandboxy se zřizují pod přímým dohledem orgánů dozoru nad trhem, podle jejich pokynů a s jejich podporou. Členské státy informují Komisi a ostatní orgány dozoru nad trhem o zřízení regulačního sandboxu prostřednictvím specializované skupiny pro správní spolupráci. Regulační sandboxy nesmějí mít vliv na pravomoci příslušných orgánů v oblasti dozoru a nápravy. Členské státy zajistí otevřený, spravedlivý a transparentní přístup k regulačním sandboxům, zejména snadnější přístup mikropodniků a malých podniků, včetně začínajících podniků.

3. V souladu s článkem 26 poskytne Komise doporučující pokyny mikropodnikům a malým a středním podnikům v oblasti uplatňování tohoto nařízení.

4. Komise bude informovat o dostupné finanční podpoře v regulačním rámci stávajících programů Unie, zejména s cílem snížit finanční zátěž mikropodniků a malých podniků.

5. Mikropodniky a malé podniky mohou poskytnout veškeré prvky technické dokumentace uvedené v příloze VII ve zjednodušeném formátu. Pro tento účel Komise prostřednictvím prováděcích aktů upřesní zjednodušený formulář technické dokumentace zaměřený na potřeby mikropodniků a malých podniků, včetně toho, jak mají být poskytnuty prvky uvedené v příloze VII. V případě, že se mikropodnik nebo malý podnik rozhodne poskytnout informace stanovené v příloze VII ve zjednodušeném formátu, použije formulář uvedený v tomto odstavci. Oznámené subjekty tento formulář přijmou pro účely posouzení shody.

Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 62 odst. 2.

Článek 34

Dohody o vzájemném uznávání

S ohledem na úroveň technického vývoje a na přístup k posuzování shody v případě třetích zemí může Unie v zájmu podpory a usnadnění mezinárodního obchodu uzavřít se třetími zeměmi dohody o vzájemném uznávání podle článku 218 Smlouvy o fungování EU.

KAPITOLA IV

OZNAMOVÁNÍ SUBJEKTŮ POSUZOVÁNÍ SHODY

Článek 35

Oznámení

1. Členské státy oznámí Komisi a ostatním členským státům subjekty, které jsou oprávněny vykonávat posuzování shody podle tohoto nařízení.

2. Členské státy usilují o zajištění toho, aby do 11. prosince 2026 existoval v Unii dostatečný počet oznámených subjektů k provádění posuzování shody, aby nedocházelo překážkám a problémům, které by bránily vstupu na trh.

Článek 36

Oznamující orgány

1. Každý členský stát jmenuje oznamující orgán odpovědný za stanovení a provádění postupů nezbytných pro posuzování, jmenování a oznamování subjektů posuzování shody a za jejich monitorování, včetně souladu s článkem 41.

2. Členské státy mohou rozhodnout, že posuzování a kontrolu podle odstavce 1 provádí vnitrostátní akreditační orgán ve smyslu nařízení (ES) č. 765/2008 a v souladu s ním.

3. Pokud oznamující orgán přenese posuzování, oznamování nebo kontrolu podle odstavce 1 tohoto článku na subjekt, který není orgánem veřejné správy, nebo tomuto subjektu svěří plnění uvedených úkolů jiným způsobem, musí být tento subjekt právnickou osobou a musí splňovat požadavky článku 37 obdobně. Tento subjekt musí dále přijmout opatření, aby byla pokryta odpovědnost vyplývající z jeho činnosti.

4. Oznamující orgán nese za úkoly vykonávané subjektem uvedeným v odstavci 3 plnou odpovědnost.

Článek 37

Požadavky týkající se oznamujících orgánů

1. Oznamující orgán musí být zřízen takovým způsobem, aby nedošlo ke střetu zájmů se subjekty posuzování shody.

2. Oznamující orgán je organizován a funguje tak, aby byla chráněna objektivita a nestrannost jeho činnosti.

3. Oznamující orgán je organizován takovým způsobem, aby každé rozhodnutí týkající se oznámení subjektu posuzování shody bylo přijato odborně způsobilými osobami jinými než osobami, které provedly posouzení.

4. Oznamující orgán nenabízí ani nezajišťuje žádnou činnost, kterou provádějí subjekty posuzování shody, ani neposkytuje poradenské služby na komerčním či konkurenčním základě.

5. Oznamující orgán chrání důvěrnost informací, které obdržel.

6. Oznamující orgán má k dispozici dostatečný počet odborně způsobilých pracovníků, aby mohl řádně vykonávat své úkoly.

Článek 38

Informační povinnost oznamujících orgánů

1. Členské státy informují Komisi o svých postupech pro posuzování a oznamování subjektů posuzování shody a kontrolu oznámených subjektů a o veškerých změnách týkajících se těchto postupů.

2. Komise informace uvedené v odstavci 1 zveřejní.

Článek 39

Požadavky týkající se oznámených subjektů

1. Pro účely oznámení musí subjekt posuzování shody splňovat požadavky stanovené v odstavcích 2 až 12.

2. Subjekt posuzování shody musí být zřízen podle vnitrostátního práva a mít právní subjektivitu.

3. Subjekt posuzování shody musí být třetí stranou nezávislou na organizaci nebo produktu s digitálními prvky, které posuzuje.

Za subjekt, který je třetí stranou, může být považován subjekt patřící k hospodářskému sdružení nebo profesnímu svazu, které zastupují podniky zapojené do projektování, vývoje, výroby, dodávání, montáže, používání nebo údržby produktů s digitálními prvky, které tento subjekt posuzuje, pokud je prokázána jeho nezávislost a neexistence jakéhokoli střetu zájmů.

4. Subjekt posuzování shody, jeho nejvyšší vedení a pracovníci odpovědní za vykonávání úkolů posuzování shody nesmějí být osobami, které projektují, vyvíjejí, vyrábějí, dodávají, dovážejí, distribuují, instalují, nakupují, vlastní, používají nebo udržují produkty s digitálními prvky, které posuzují, ani zplnomocněnými zástupci kterékoli z těchto stran. To nevylučuje používání posuzovaných produktů, které jsou nezbytné pro činnost subjektu posuzování shody, ani používání takových produktů k osobním účelům.

Subjekt posuzování shody, jeho nejvyšší vedení a pracovníci odpovědní za vykonávání úkolů posuzování shody se nesmějí přímo podílet na projektování, vývoji, výrobě, dovozu, distribuci, nabízení, instalaci, používání ani údržbě produktů s digitálními prvky, které posuzují, ani nesmějí zastupovat strany, které se těmito činnostmi zabývají. Nesmějí vykonávat žádnou činnost, která by mohla ohrozit jejich nezávislý úsudek nebo integritu ve vztahu k činnostem při posuzování shody, k jejímuž vykonávání jsou oznámeni. To platí zejména pro poradenské služby.

Subjekty posuzování shody musí zajistit, aby činnosti jejich dceřiných společností nebo subdodavatelů neohrožovaly důvěrnost, objektivitu a nestrannost jejich činnosti při posuzování shody.

5. Subjekty posuzování shody a jejich pracovníci vykonávají činnost při posuzování shody na nejvyšší úrovni profesní integritu a požadované odborné způsobilosti v konkrétní oblasti a nesmějí být vystaveni žádným tlakům a podnětům, zejména finančním, které by mohly ovlivnit jejich úsudek nebo výsledky jejich činnosti při posuzování shody, zejména ze strany osob nebo skupin osob, které mají na výsledcích této činnosti zájem.

6. Subjekt posuzování shody musí být schopen plnit všechny úkoly spojené s posuzováním shody podle přílohy VIII, v souvislosti s nímž byl oznámen, bez ohledu na to, zda tyto úkoly plní subjekt posuzování shody sám, nebo jsou plněny jeho jménem a na jeho odpovědnost.

Subjekt posuzování shody musí mít vždy a pro každý postup posuzování shody a každý druh nebo kategorii produktů s digitálními prvky, v souvislosti s nímž byl oznámen, k dispozici nezbytné:

a) pracovníky s odbornými znalostmi a dostatečnými zkušenostmi potřebnými k plnění úkolů spojených s posuzováním shody,

b) popisy postupů, podle nichž má být posuzování shody prováděno, aby byla zajištěna transparentnost těchto postupů a možnost jejich zopakování. Musí mít zavedenu náležitou politiku a postupy pro rozlišení mezi úkoly, jež vykonává jako oznámený subjekt, a svou další činností,

c) postupy pro výkon činností, které řádně zohledňují velikost podniku, odvětví, v němž působí, jeho strukturu, míru složitosti technologie daného produktu a hromadný či sériový způsob výroby.

Subjekt posuzování shody musí mít prostředky nezbytné k řádnému plnění technických a administrativních úkolů spojených s činností při posuzování shody a musí mít přístup k veškerému potřebnému vybavení nebo zařízením.

7. Pracovníci odpovědní za provádění činnosti při posuzování shody musí:

a) mít dobrou technickou a odbornou přípravu zahrnující veškerou činnost při posuzování shody, v souvislosti s nímž byl subjekt posuzování shody oznámen,

b) mít uspokojivou znalost požadavků souvisejících s posuzováním, které provádějí, a odpovídající pravomoc toto posuzování provádět,

c) mít náležité znalosti základních požadavků na kybernetickou bezpečnost stanovených v příloze I, použitelných harmonizovaných norem a společných specifikací a příslušných ustanovení právních předpisů Unie a jejich prováděcích aktů a rozumět jim,

d) být schopni vypracovávat certifikáty, záznamy a zprávy prokazující provedení posuzování shody.

8. Musí být zaručena nestrannost subjektů posuzování shody, jejich nejvyššího vedení a pracovníků, kteří posuzování provádějí.

Odměňování nejvyššího vedení a pracovníků subjektu posuzování shody, kteří posuzování provádějí, nesmí záviset na počtu provedených posouzení ani na jejich výsledcích.

9. Subjekty posuzování shody uzavřou pojištění odpovědnosti za škodu, pokud tuto odpovědnost nepřevzal jejich členský stát v souladu s vnitrostátním právem nebo pokud není za posuzování shody přímo odpovědný sám členský stát.

10. Pracovníci subjektu posuzování shody zachovávají služební tajemství, pokud jde o veškeré informace, které obdrželi při plnění svých úkolů podle přílohy VIII nebo podle jakéhokoli ustanovení vnitrostátního práva, kterými se provádí, s výjimkou styku s příslušnými orgány dozoru nad trhem členského státu, v němž vykonávají svou činnost. Vlastnická práva jsou chráněna. Subjekt posuzování shody musí mít dokumentované postupy zajišťující soulad s tímto odstavcem.

11. Subjekty posuzování shody se podílejí na příslušné normalizační činnosti a na činnosti koordinační skupiny oznámených subjektů zřízené podle článku 51 nebo zajistí, aby byli jejich pracovníci o této činnosti informováni, a obecně se řídí správními rozhodnutími a jinými dokumenty, které jsou výsledkem práce této skupiny.

12. Subjekty posuzování shody fungují v souladu se souborem důsledných, spravedlivých, přiměřených a opodstatněných podmínek a zároveň brání zbytečnému zatěžování hospodářských subjektů, zejména s přihlédnutím k zájmům mikropodniků a malých a středních podniků, co se týče poplatků.

Článek 40

Předpoklad shody oznámených subjektů

Pokud subjekt posuzování shody prokáže svou shodu s kritérii stanovenými v příslušných harmonizovaných normách nebo jejich částech, na něž byly zveřejněny odkazy v *Úředním věstníku Evropské unie*, předpokládá se, že splňuje požadavky stanovené v článku 39 v rozsahu, v němž se harmonizované normy na tyto požadavky vztahují.

Článek 41

Dceřiné společnosti oznámených subjektů a zadávání subdodávek

1. Pokud oznámený subjekt zadá konkrétní úkoly týkající se posuzování shody subdodavateli nebo dceřiné společnosti, zajistí, aby subdodavatel nebo dceřiná společnost splňovali požadavky stanovené v článku 39, a informuje o tom oznamující orgán.

2. Oznámené subjekty nesou plnou odpovědnost za úkoly provedené subdodavateli nebo dceřinými společnostmi bez ohledu na to, kde jsou tito subdodavatelé nebo dceřiné společnosti usazeni.

3. Činnost lze zadat subdodavateli nebo dceřiné společnosti pouze se souhlasem výrobce.

4. Oznámený subjekt uchovává pro potřebu oznamujícího orgánu příslušné doklady týkající se posouzení kvalifikace subdodavatele nebo dceřiné společnosti a práce provedené subdodavatelem nebo dceřinou společností podle tohoto nařízení.

Článek 42

Žádost o oznámení

1. Subjekt posuzování shody podává žádost o oznámení oznamujícímu orgánu členského státu, v němž je usazen.

2. Součástí žádosti je popis činnosti při posuzování shody, postupu nebo postupů posuzování shody a produktu nebo produktů s digitálními prvky, pro něž se subjekt prohlašuje za způsobilý, jakož i případné osvědčení o akreditaci vydané vnitrostátním akreditačním orgánem, které potvrzuje, že subjekt posuzování shody splňuje požadavky stanovené v článku 39.

3. Nemůže-li dotčený subjekt posuzování shody předložit osvědčení o akreditaci, poskytne oznamujícímu orgánu veškeré doklady nezbytné k ověření, uznání a pravidelné kontrole svého souladu s požadavky stanovenými v článku 39.

Článek 43

Postup oznamování

1. Oznamující orgány oznámí pouze subjekty posuzování shody, které splňují požadavky stanovené v článku 39.

2. Oznamující orgán uvědomí Komisi a ostatní členské státy prostřednictvím informačního systému oznámených a jmenovaných organizací podle nového přístupu, který vyvinula a spravuje Komise.

3. Oznámení obsahuje veškeré podrobné informace o činnosti při posuzování shody, modulu nebo modulech posuzování shody, dotčeném produktu nebo produktech s digitálními prvky a příslušné osvědčení o akreditaci.

4. Pokud se oznámení nezakládá na osvědčení o akreditaci uvedeném v čl. 42 odst. 2, poskytne oznamující orgán Komisi a ostatním členským státům podklady, které dokládají způsobilost subjektu posuzování shody, a informuje je o opatřeních, jež zajišťují, aby byl subjekt pravidelně kontrolován a i v budoucnu splňoval požadavky uvedené v článku 39.

5. Dotčený subjekt může vykonávat činnost oznámeného subjektu, pouze pokud proti tomu Komise ani ostatní členské státy nevznesly námitky do dvou týdnů po oznámení v případě, že se použije osvědčení o akreditaci, nebo do dvou měsíců po oznámení, jestliže se akreditace nepoužije.

Pouze takový subjekt se považuje za oznámený subjekt pro účely tohoto nařízení.

6. Komisi a ostatním členským státům je třeba oznámit veškeré následné významné změny týkající se oznamování.

Článek 44

Identifikační čísla a seznamy oznámených subjektů

1. Komise oznámenému subjektu přidělí identifikační číslo.

Komise subjektu přidělí jediné číslo i v případě, že je subjekt oznámen podle několika právních aktů Unie.

2. Komise zveřejní seznam subjektů oznámených podle tohoto nařízení, včetně identifikačních čísel, která jim byla přidělena, a činností, pro něž byly oznámeny.

Komise zajistí, aby byl tento seznam průběžně aktualizován.

Článek 45

Změny v oznámeních

1. Pokud oznamující orgán zjistí nebo je upozorněn na to, že oznámený subjekt již nesplňuje požadavky stanovené v článku 39 nebo neplní své povinnosti, omezí, pozastaví nebo případně zruší oznámení podle toho, nakolik je neplnění těchto požadavků nebo povinností závažné. Informuje o tom neprodleně Komisi a ostatní členské státy.

2. V případě omezení, pozastavení nebo zrušení oznámení nebo v případě, že oznámený subjekt ukončil svou činnost, oznamující členský stát přijme příslušné kroky k zajištění toho, aby byly spisy tohoto subjektu buď zpracovány jiným oznámeným subjektem, nebo byly na vyžádání k dispozici příslušným oznamujícím orgánům a orgánům dozoru nad trhem.

Článek 46

Zpochybnění způsobilosti oznámených subjektů

1. Komise vyšetří všechny případy, kdy má pochybnosti nebo kdy je upozorněna na pochybnosti o způsobilosti oznámeného subjektu plnit požadavky a povinnosti, které jsou mu uloženy, nebo o tom, zda je oznámený subjekt nadále plní.

2. Oznamující členský stát předloží Komisi na vyžádání všechny informace týkající se podkladů pro oznámení nebo zachování způsobilosti dotčeného subjektu.

3. Komise zajistí, aby se se všemi citlivými informacemi získanými v průběhu tohoto šetření nakládalo jako s důvěrnými.

4. Pokud Komise zjistí, že oznámený subjekt nesplňuje nebo přestal splňovat požadavky na své oznámení, informuje o tom oznamující členský stát a vyzve ho, aby přijal nezbytná nápravná opatření, včetně případného zrušení oznámení.

Článek 47

Povinnosti týkající se činnosti oznámených subjektů

1. Oznámené subjekty provádějí posuzování shody v souladu s postupy posuzování shody stanovenými v článku 32 a příloze VIII.

2. Posuzování shody se provádí přiměřeným způsobem, aby se zabránilo zbytečné zátěži hospodářských subjektů. Subjekty posuzování shody při výkonu své činnosti řádně zohlední velikost podniků, zejména pokud jde o mikropodniky a malé a střední podniky, odvětví, v němž působí, jejich strukturu, míru složitosti a míru kybernetického rizika produktů s digitálními prvky a dané technologie a hromadnou nebo sériovou povahu výrobního procesu.

3. Oznámený subjekt však musí zachovávat míru přísnosti a úroveň ochrany, jež jsou vyžadovány, aby byly produkty s digitálními prvky v souladu s tímto nařízením.

4. Pokud oznámený subjekt zjistí, že výrobce nesplnil požadavky stanovené v příloze I nebo v odpovídajících harmonizovaných normách či ve společných specifikacích podle článku 27, vyzve výrobce, aby přijal vhodná nápravná opatření, a nevydá certifikát shody.

5. Pokud v průběhu kontroly shody po vydání certifikátu oznámený subjekt zjistí, že produkt s digitálními prvky již nesplňuje požadavky stanovené v tomto nařízení, vyzve výrobce, aby přijal vhodná nápravná opatření, a v případě nutnosti platnost certifikátu pozastaví nebo zruší.

6. Pokud nejsou nápravná opatření přijata nebo pokud nemají požadovaný účinek, oznámený subjekt podle potřeby omezí, pozastaví nebo zruší platnost příslušných certifikátů.

Článek 48

Odvolání proti rozhodnutí oznámených subjektů

Členské státy zajistí, aby bylo možné se proti rozhodnutí oznámených subjektů odvolat.

Článek 49

Informační povinnost oznámených subjektů

1. Oznámené subjekty informují oznamující orgán:

a) o každém zamítnutí, omezení, pozastavení nebo zrušení certifikátu,

b) o všech okolnostech majících vliv na rozsah a podmínky oznámení,

c) o každé žádosti o informace týkající se činnosti při posuzování shody, kterou obdržely od orgánů dozoru nad trhem,

d) na vyžádání o činnosti při posuzování shody vykonané v rámci působnosti jejich oznámení a o jakékoli jiné vykonané činnosti, včetně přeshraniční činnosti a zadávání subdodávek.

2. Oznámené subjekty poskytnou ostatním subjektům oznámeným podle tohoto nařízení, které vykonávají obdobnou činnost při posuzování shody a zabývají se stejnými produkty s digitálními prvky, příslušné informace o otázkách týkajících se negativních a, na vyžádání, pozitivních výsledků posuzování shody.

Článek 50

Výměna zkušeností

Komise organizačně zabezpečuje výměnu zkušeností mezi vnitrostátními orgány členských států, které jsou odpovědné za politiku oznamování.

Článek 51

Koordinace oznámených subjektů

1. Komise zajistí zavedení a řádné provádění vhodné koordinace a spolupráce mezi oznámenými subjekty ve formě meziodvětvové skupiny oznámených subjektů.

2. Členské státy zajistí, aby se jimi oznámené subjekty účastnily práce této skupiny, a to přímo nebo prostřednictvím určených zástupců.

KAPITOLA V

DOZOR NAD TRHEM A VYMÁHÁNÍ PRÁVA

Článek 52

Dozor nad trhem a kontrola produktů s digitálními prvky na trhu Unie

1. Na produkty s digitálními prvky spadající do oblasti působnosti tohoto nařízení se použije nařízení (EU) 2019/1020.

2. Pro účely zajištění účinného uplatňování tohoto nařízení každý členský stát určí jeden nebo více orgánů dozoru nad trhem. Členské státy mohou určit stávající nebo nový orgán, který bude působit jako orgán dozoru nad trhem pro účely tohoto nařízení.

3. Orgány dozoru nad trhem určené podle odstavce 2 tohoto článku odpovídají rovněž za provádění dozoru nad trhem v souvislosti s povinnostmi správců softwaru s otevřeným zdrojovým kódem stanovenými v článku 24. Pokud orgán dozoru nad trhem zjistí, že správce softwaru s otevřeným zdrojovým kódem neplní povinnosti stanovené v uvedeném článku, vyzve jej, aby zajistil přijetí veškerých vhodných nápravných opatření. Správci softwaru s otevřeným zdrojovým kódem zajistí, aby byla přijata veškerá vhodná nápravná opatření s ohledem na jejich povinnosti podle tohoto nařízení.

4. Orgány dozoru nad trhem případně spolupracují s vnitrostátními orgány certifikace kybernetické bezpečnosti určenými v souladu s článkem 58 nařízení (EU) 2019/881 a vyměňují si pravidelně informace. Pokud jde o dohled nad plněním povinností podávat zprávy podle článku 14 tohoto nařízení, určené orgány dozoru nad trhem spolupracují s týmy CSIRT určenými jako koordinátoři a s agenturou ENISA a pravidelně si s nimi vyměňují informace.

5. Orgány dozoru nad trhem mohou tým CSIRT určený jako koordinátor nebo agenturu ENISA požádat o poskytnutí technického poradenství v záležitostech souvisejících s uplatňováním a prosazováním tohoto nařízení. Při provádění šetření podle článku 54 mohou orgány dozoru nad trhem požádat tým CSIRT určený jako koordinátor nebo agenturu ENISA, aby vypracovaly analýzu na podporu hodnocení souladu produktů s digitálními prvky.

6. Orgány dozoru nad trhem případně spolupracují s dalšími orgány dozoru nad trhem určenými na základě harmonizačních právních předpisů Unie jiných než toto nařízení a pravidelně si vyměňují informace.

7. Orgány dozoru nad trhem případně spolupracují s orgány dohledu nad právem Unie v oblasti ochrany údajů. Tato spolupráce zahrnuje informování těchto orgánů o veškerých zjištěních relevantních z hlediska plnění jejich pravomocí, a to i při vydávání pokynů a poskytování poradenství podle odstavce 10, pokud se tyto pokyny a poradenství týkají zpracování osobních údajů.

Orgány vykonávající dohled nad právem Unie v oblasti ochrany údajů mají pravomoc požadovat jakoukoli dokumentaci vytvořenou nebo vedenou podle tohoto nařízení a přístup k ní, pokud je přístup k této dokumentaci nezbytný pro plnění jejich úkolů. O každé takové žádosti informují určené orgány dozoru nad trhem dotčeného členského státu.

8. Členské státy zajistí, aby určeným orgánům dozoru nad trhem byly poskytnuty odpovídající finanční a technické zdroje, včetně nástrojů pro automatické zpracování dat tam, kde je to vhodné, jakož i lidské zdroje s potřebnými dovednostmi v oblasti kybernetické bezpečnosti, které jim umožní plnit úkoly podle tohoto nařízení.

9. Komise podporuje a usnadňuje výměnu zkušeností mezi určenými orgány dozoru nad trhem.

10. Orgány dozoru nad trhem mohou s podporou Komise a případně týmů CSIRT a agentury ENISA poskytovat hospodářským subjektům pokyny a poradenství ohledně uplatňování tohoto nařízení.

11. Orgány dozoru nad trhem informují spotřebitele o tom, kde se podávají stížnosti, které by mohly v souladu s článkem 11 nařízení (EU) 2019/1020 poukazovat na nesoulad s tímto nařízením, a poskytnou spotřebitelům informace o tom, kde a jak získat přístup k mechanismům usnadňujícím oznamování zranitelností, incidentů a kybernetických hrozeb, které mohou ovlivnit produkty s digitálními prvky.

12. Orgány dozoru nad trhem případně usnadňují spolupráci s příslušnými zúčastněnými stranami, včetně vědeckých, výzkumných a spotřebitelských organizací.

13. Orgány dozoru nad trhem každoročně podávají Komisi zprávy o výsledcích příslušné činnosti v oblasti dozoru nad trhem. Určené orgány dozoru nad trhem neprodleně ohlásí Komisi a příslušným vnitrostátním orgánům pro hospodářskou soutěž veškeré informace zjištěné v průběhu činnosti v oblasti dozoru nad trhem, které by mohly mít potenciální význam pro uplatňování práva Unie v oblasti hospodářské soutěže.

14. V případě produktů s digitálními prvky spadajících do oblasti působnosti tohoto nařízení, které jsou klasifikovány jako vysoce rizikové systémy umělé inteligence podle článku 6 nařízení (EU) 2024/1689, jsou orgány odpovědnými za činnost v oblasti dozoru nad trhem požadovanou tímto nařízením orgány dozoru nad trhem určené pro účely nařízení (EU) 2024/1689. Orgány dozoru nad trhem určené podle uvedeného nařízení spolupracují podle potřeby s orgány dozoru nad trhem určenými podle tohoto nařízení, s týmy CSIRT určenými jako koordinátoři a s agenturou ENISA, pokud jde o dohled nad plněním povinností podávat zprávy podle článku 14 tohoto nařízení. Orgány dozoru nad trhem určené podle nařízení (EU) 2024/1689 zejména informují orgány dozoru nad trhem určené podle tohoto nařízení o veškerých zjištěních, která jsou relevantní pro plnění jejich úkolů v souvislosti s uplatňováním tohoto nařízení.

15. Pro jednotné uplatňování tohoto nařízení se zřizuje specializovaná skupina pro správní spolupráci podle čl. 30 odst. 2 nařízení (EU) 2019/1020. Tato skupina se skládá ze zástupců určených orgánů dozoru nad trhem a případně i ze zástupců ústředních styčných úřadů. Zabývá se rovněž konkrétními záležitostmi souvisejícími s činností v oblasti dozoru nad trhem, pokud jde o povinnosti uložené správcům softwaru s otevřeným zdrojovým kódem.

16. Orgány dozoru nad trhem monitorují, jak výrobci při určování doby podpory svých produktů s digitálními prvky uplatňují kritéria uvedená v čl. 13 odst. 8.

Skupina pro správní spolupráci zveřejní ve veřejně přístupné a uživatelsky vstřícné podobě příslušné statistiky o kategoriích produktů s digitálními prvky, včetně průměrných dob podpory, jak je uvedl výrobce podle čl. 13 odst. 8, a poskytne pokyny, které zahrnují orientační doby podpory pro kategorie produktů s digitálními prvky.

Pokud z těchto údajů vyplývá, že doba podpory pro konkrétní kategorie produktů s digitálními prvky není dostatečná, může specializovaná skupina pro správní spolupráci vydat orgánům dozoru nad trhem doporučení, aby svou činnost zaměřily na tyto kategorie produktů s digitálními prvky.

Článek 53

Přístup k údajům a dokumentaci

Je-li to nezbytné k posouzení shody produktů s digitálními prvky a postupů zavedených jejich výrobci se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I, udělí se orgánům dozoru nad trhem na základě odůvodněné žádosti přístup k údajům požadovaným pro posouzení návrhu, vývoje, výroby a řešení zranitelnosti těchto produktů, včetně související interní dokumentace příslušného hospodářského subjektu, a to v jazyce, kterému snadno porozumí.

Článek 54

Postup na vnitrostátní úrovni týkající se produktů s digitálními prvky představujících významné kybernetické bezpečnostní riziko

1. Pokud má orgán dozoru nad trhem členského státu dostatečný důvod domnívat se, že produkt s digitálními prvky, včetně řešení jeho zranitelnosti, představuje významné kybernetické bezpečnostní riziko, provede bez zbytečného odkladu a případně ve spolupráci s příslušným týmem CSIRT hodnocení dotčeného produktu s digitálními prvky z hlediska jeho souladu se všemi požadavky stanovenými v tomto nařízení. Příslušné hospodářské subjekty s orgánem dozoru nad trhem podle potřeby spolupracují.

Pokud v průběhu tohoto hodnocení orgán dozoru nad trhem zjistí, že produkt s digitálními prvky nesplňuje požadavky stanovené v tomto nařízení, neprodleně vyzve příslušný hospodářský subjekt, aby přijal veškerá vhodná nápravná opatření k uvedení produktu s digitálními prvky do souladu s těmito požadavky nebo k jeho stažení z trhu či z oběhu v přiměřené lhůtě úměrné povaze kybernetického bezpečnostního rizika, kterou může stanovit orgán dozoru nad trhem.

Orgán dozoru nad trhem o tom informuje příslušný oznámený subjekt. Na nápravná opatření se použije článek 18 nařízení (EU) 2019/1020.

2. Při určování významu kybernetického bezpečnostního rizika uvedeného v odstavci 1 tohoto článku zohlední orgány dozoru nad trhem rovněž rizikové faktory jiné než technické povahy, zejména ty, které byly stanoveny na základě koordinovaného posouzení bezpečnostních rizik kritických dodavatelských řetězců na úrovni Unie provedeného v souladu s článkem 22 směrnice (EU) 2022/2555. Pokud má orgán dozoru nad trhem dostatečný důvod se domnívat, že určitý produkt s digitálními prvky představuje s ohledem na rizikové faktory jiné než technické povahy významné kybernetické bezpečnostní riziko, vyrozumí příslušné orgány určené nebo zřízené podle článku 8 směrnice (EU) 2022/2555 a podle potřeby s těmito orgány spolupracuje.

3. Domnívá-li se orgán dozoru nad trhem, že se nesoulad netýká pouze území jeho členského státu, informuje Komisi a ostatní členské státy o výsledcích hodnocení a o opatřeních, která má hospodářský subjekt na jeho žádost přijmout.

4. Hospodářský subjekt zajistí, aby byla přijata veškerá vhodná nápravná opatření ohledně všech dotčených produktů s digitálními prvky, které dodal na trh v celé Unii.

5. Pokud hospodářský subjekt ve lhůtě uvedené ve druhém pododstavci odstavce 1 nepřijme přiměřená nápravná opatření, přijme orgán dozoru nad trhem veškerá vhodná dočasná opatření k zákazu nebo omezení dodávání tohoto produktu s digitálními prvky na trh svého členského státu nebo k zajištění toho, aby byl stažen z trhu či z oběhu.

O takových opatřeních tento orgán neprodleně vyrozumí Komisi a ostatní členské státy.

6. Součástí informací uvedených v odstavci 5 jsou všechny dostupné podrobné informace, zejména údaje nezbytné pro identifikaci nevyhovujícího produktu s digitálními prvky, údaje o původu dotčeného produktu s digitálními prvky, povaze údajného nesouladu a souvisejícího rizika, povaze a době trvání opatření přijatých na vnitrostátní úrovni a údaje o stanovisku příslušného hospodářského subjektu. Orgán dozoru nad trhem zejména uvede, zda je důvodem nesouladu jeden nebo více těchto nedostatků:

a) produkt s digitálními prvky nebo postupy zavedené výrobcem nesplňují základní požadavky na kybernetickou bezpečnost stanovené v příloze I,

b) nedostatky v harmonizovaných normách, evropských schématech certifikace kybernetické bezpečnosti nebo společných specifikacích uvedených v článku 27.

7. Orgány dozoru nad trhem členských států jiné než orgán dozoru nad trhem členského státu, který zahájil tento postup, neprodleně informují Komisi a ostatní členské státy o veškerých opatřeních, která přijaly, a o všech doplňujících údajích týkajících se nesouladu dotčeného produktu s digitálními prvky, které mají k dispozici, a v případě nesouhlasu s oznámeným vnitrostátním opatřením o svých námitkách.

8. Jestliže do tří měsíců od přijetí oznámení uvedeného v odstavci 5 tohoto článku nevznese žádný členský stát ani Komise proti předběžnému opatření přijatému členským státem námitku, považuje se opatření za důvodné. Tím nejsou dotčena procesní práva dotčeného hospodářského subjektu v souladu s článkem 18 nařízení (EU) 2019/1020.

9. Orgány dozoru nad trhem všech členských států zajistí, aby byla v souvislosti s dotčeným produktem s digitálními prvky bezodkladně přijata náležitá restriktivní opatření, například stažení daného produktu z jejich trhu.

Článek 55

Ochranný postup Unie

1. Pokud do tří měsíců od obdržení oznámení uvedeného v čl. 54 odst. 5 vznese některý členský stát proti opatření přijatému jiným členským státem námitku nebo pokud se Komise domnívá, že je dané opatření v rozporu s právem Unie, zahájí Komise neprodleně konzultaci s dotčeným členským státem a hospodářským subjektem nebo subjekty a provede hodnocení tohoto vnitrostátního opatření. Na základě výsledků tohoto hodnocení Komise do devíti měsíců od oznámení uvedeného v čl. 54 odst. 5 rozhodne, zda je dané vnitrostátní opatření důvodné či nikoli, a toto rozhodnutí oznámí dotčenému členskému státu.

2. Pokud je vnitrostátní opatření považováno za důvodné, přijmou všechny členské státy nezbytná opatření k zajištění toho, aby byl nevyhovující produkt s digitálními prvky stažen z jejich trhu, a informují o tom Komisi. Pokud vnitrostátní opatření není považováno za důvodné, dotčený členský stát toto opatření zruší.

3. Pokud je vnitrostátní opatření považováno za důvodné a je-li nesoulad produktu s digitálními prvky přisuzován nedostatkům v harmonizovaných normách, použije Komise postup stanovený v článku 11 nařízení (EU) č. 1025/2012.

4. Pokud je vnitrostátní opatření považováno za důvodné a je-li nesoulad produktu s digitálními prvky přisuzován nedostatkům v evropském schématu certifikace kybernetické bezpečnosti podle článku 27, Komise zváží, zda změnit nebo zrušit akt v přenesené pravomoci přijatý podle čl. 27 odst. 9, v němž je stanoven předpoklad shody týkající se daného schématu certifikace.

5. Pokud je vnitrostátní opatření považováno za důvodné a je-li nesoulad produktu s digitálními prvky přisuzován nedostatkům ve společných specifikacích podle článku 27, Komise zváží, zda změnit nebo zrušit některý prováděcí akt přijatý podle čl. 27 odst. 2, v němž jsou stanoveny tyto společné specifikace.

Článek 56

Postup na úrovni Unie týkající se produktů s digitálními prvky představujících významné kybernetické bezpečnostní riziko

1. Pokud má Komise dostatečný důvod se domnívat, a to i na základě informací poskytnutých agenturou ENISA, že produkt s digitálními prvky, který představuje významné kybernetické bezpečnostní riziko, není v souladu s požadavky stanovenými v tomto nařízení, informuje o tom příslušné orgány dozoru nad trhem. Jestliže orgány dozoru nad trhem provádějí hodnocení produktu s digitálními prvky, který by mohl představovat významné kybernetické bezpečnostní riziko, pokud jde o jeho soulad s požadavky stanovenými v tomto nařízení, použijí se postupy uvedené v článcích 54 a 55.

2. Pokud má Komise dostatečný důvod se domnívat, že produkt s digitálními prvky představuje významné kybernetické bezpečnostní riziko s ohledem na rizikové faktory jiné než technické povahy, informuje o tom příslušné orgány dozoru nad trhem, případně příslušné orgány určené nebo zřízené podle článku 8 směrnice (EU) 2022/2555, a podle potřeby s těmito orgány spolupracuje. Komise rovněž zváží v rámci svých úkolů týkajících se koordinovaného posuzování bezpečnostních rizik kritických dodavatelských řetězců na úrovni Unie podle článku 22 směrnice (EU) 2022/2555 význam zjištěných rizik pro daný produkt s digitálními prvky a v případě potřeby konzultuje se skupinou pro spolupráci zřízenou podle článku 14 směrnice (EU) 2022/2555 a s agenturou ENISA.

3. Za okolností, které odůvodňují okamžitý zásah za účelem zachování řádného fungování vnitřního trhu, a pokud má Komise dostatečný důvod domnívat se, že produkt s digitálními prvky uvedený v odstavci 1 nadále nesplňuje požadavky stanovené v tomto nařízení a příslušné orgány dozoru nad trhem nepřijaly účinná opatření, provede Komise hodnocení souladu a může požádat agenturu ENISA, aby vypracovala analýzu na podporu tohoto hodnocení. Komise odpovídajícím způsobem informuje příslušné orgány dozoru nad trhem. Příslušné hospodářské subjekty s agenturou ENISA podle potřeby spolupracují.

4. Na základě hodnocení podle odstavce 3 může Komise rozhodnout, že je třeba nápravné nebo omezující opatření na úrovni Unie. Za tímto účelem neprodleně konzultuje dotčené členské státy a příslušný hospodářský subjekt nebo subjekty.

5. Na základě konzultace uvedené v odstavci 4 tohoto článku může Komise přijmout prováděcí akty, v nichž stanoví nápravná nebo omezující opatření na úrovni Unie, včetně požadavku, aby byly dotčené produkty s digitálními prvky staženy z trhu nebo z oběhu, a to v přiměřené lhůtě úměrné povaze rizika. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 62 odst. 2.

6. Komise o prováděcích aktech podle odstavce 5 neprodleně uvědomí příslušný hospodářský subjekt či subjekty. Členské státy tyto prováděcí akty neodkladně uplatňují a odpovídajícím způsobem informují Komisi.

7. Odstavce 3 až 6 se použijí po dobu trvání výjimečné situace, která odůvodňovala zásah Komise, za předpokladu, že dotčený produkt s digitálními prvky není uveden do souladu s tímto nařízením.

Článek 57

Vyhovující produkty s digitálními prvky, které představují významné kybernetické bezpečnostní riziko

1. Orgán dozoru nad trhem členského státu vyzve hospodářský subjekt, aby přijal veškerá vhodná opatření, pokud po provedení hodnocení podle článku 54 zjistí, že ačkoli jsou produkt s digitálními prvky a postupy zavedené výrobcem v souladu s tímto nařízením, představují významné kybernetické bezpečnostní riziko, jakož i riziko pro:

a) zdraví nebo bezpečnost osob,

b) dodržování povinností podle unijního nebo vnitrostátního práva, jejichž cílem je ochrana základních práv,

c) dostupnost, autenticitu, integritu nebo důvěrnost služeb nabízených prostřednictvím elektronického informačního systému základními subjekty uvedenými v čl. 3 odst. 1 směrnice (EU) 2022/2555 nebo

d) jiné aspekty ochrany veřejného zájmu.

Opatření uvedená v prvním pododstavci mohou zahrnovat opatření k zajištění toho, aby dotčený produkt s digitálními prvky a postupy zavedené výrobcem v době dodání na trh již toto riziko nepředstavovaly, a ke stažení dotčeného produktu s digitálními prvky z trhu nebo z oběhu, přičemž tato opatření jsou přiměřená povaze daných rizik.

2. Výrobce nebo jiné příslušné hospodářské subjekty zajistí, aby bylo přijato nápravné opatření ve vztahu k dotčeným produktům s digitálními prvky, které dodali na trh v rámci celé Unie, ve lhůtě stanovené orgánem dozoru nad trhem členského státu uvedeným v odstavci 1.

3. Členský stát neprodleně informuje Komisi a ostatní členské státy o opatřeních přijatých podle odstavce 1. Tyto informace musejí obsahovat všechny dostupné podrobné informace, zejména údaje nezbytné k identifikaci dotčeného produktu s digitálními prvky, údaje o původu a dodavatelském řetězci těchto produktů s digitálními prvky, údaje o povaze souvisejícího rizika a údaje o povaze a době trvání opatření přijatých na vnitrostátní úrovni.

4. Komise neprodleně zahájí konzultaci s členskými státy a příslušným hospodářským subjektem a vyhodnotí přijatá vnitrostátní opatření. Na základě výsledků tohoto hodnocení Komise rozhodne, zda je opatření důvodné či nikoli, a pokud je to nutné, navrhne vhodná opatření.

5. Rozhodnutí Komise uvedené v odstavci 4 je určeno všem členským státům.

6. Pokud má Komise dostatečný důvod se domnívat, a to i na základě informací poskytnutých agenturou ENISA, že ačkoli je produkt s digitálními prvky v souladu s tímto nařízením, představuje rizika uvedená v odstavci 1 tohoto článku, informuje o tom příslušný orgán nebo orgány dozoru nad trhem a může je požádat, aby provedly hodnocení a řídily se postupy uvedenými v článku 54 a v odstavcích 1, 2 a 3 tohoto článku.

7. Za okolností, které odůvodňují okamžitý zásah za účelem zachování řádného fungování vnitřního trhu, a pokud má Komise dostatečný důvod se domnívat, že produkt s digitálními prvky uvedený v odstavci 6 nadále představuje rizika podle odstavce 1 a příslušné vnitrostátní orgány dozoru nad trhem nepřijaly účinná opatření, provede Komise hodnocení rizik, která tento produkt s digitálními prvky představuje, a může požádat agenturu ENISA, aby vypracovala analýzu na podporu tohoto hodnocení, a informuje o tom příslušné orgány dozoru nad trhem. Příslušné hospodářské subjekty s agenturou ENISA podle potřeby spolupracují.

8. Na základě hodnocení podle odstavce 7 může Komise stanovit, že je zapotřebí nápravného nebo omezujícího opatření na úrovni Unie. Za tímto účelem neprodleně konzultuje s dotčenými členskými státy a s příslušným hospodářským subjektem nebo subjekty.

9. Na základě konzultace uvedené v odstavci 8 tohoto článku může Komise přijmout prováděcí akty s cílem rozhodnout o nápravných nebo omezujících opatřeních na úrovni Unie, včetně požadavku, aby byly dotčené produkty s digitálními prvky staženy z trhu nebo z oběhu, a to v přiměřené lhůtě úměrné povaze rizika. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 62 odst. 2.

10. Komise o prováděcích aktech podle odstavce 9 neprodleně uvědomí příslušný hospodářský subjekt či subjekty. Členské státy tyto prováděcí akty neodkladně uplatňují a odpovídajícím způsobem informují Komisi.

11. Odstavce 6 až 10 se použijí po dobu trvání výjimečné situace, která odůvodňovala zásah Komise, a po dobu, po kterou dotčený produkt s digitálními prvky nadále představuje rizika uvedená v odstavci 1.

Článek 58

Formální nesoulad

1. Orgán dozoru nad trhem daného členského státu vyzve příslušného výrobce, aby odstranil nesoulad spočívající v některé z těchto skutečností::

a) označení CE bylo umístěno v rozporu s články 29 a 30,

b) označení CE nebylo umístěno,

c) nebylo vypracováno EU prohlášení o shodě,

d) EU prohlášení o shodě nebylo vypracováno správně,

e) nebylo případně umístěno identifikační číslo oznámeného subjektu, který je zapojen do postupu posuzování shody,

f) technická dokumentace buď není dostupná, nebo je neúplná.

2. Pokud nesoulad uvedený v odstavci 1 trvá i nadále, přijme dotčený členský stát veškerá vhodná opatření s cílem omezit nebo zakázat dodávání produktu s digitálními prvky na trh, nebo zajistit, aby byl stažen z oběhu či z trhu.

Článek 59

Společné činnosti orgánů dozoru nad trhem

1. Orgány dozoru nad trhem se mohou dohodnout s dalšími příslušnými orgány na provádění společných činností zaměřených na zajištění kybernetické bezpečnosti a ochrany spotřebitelů, pokud jde o konkrétní produkty s digitálními prvky uváděné nebo dodávané na trh, zejména produkty s digitálními prvky, u nichž se často zjišťuje, že představují kybernetické bezpečnostní riziko.

2. Komise nebo agentura ENISA navrhne společné činnosti pro kontrolu souladu s tímto nařízením, které budou provádět orgány dozoru nad trhem na základě údajů nebo informací o možném nesouladu produktů s digitálními prvky, které spadají do oblasti působnosti tohoto nařízení, v několika členských státech s požadavky stanovenými v tomto nařízení.

3. Orgány dozoru nad trhem a případně Komise zajistí, aby dohoda o provádění společných činností nevedla k nekalé soutěži mezi hospodářskými subjekty a nepříznivě nenarušovala objektivitu, nezávislost a nestrannost stran dohody.

4. Orgán dozoru nad trhem může použít jakékoli informace získané při společných činnostech vykonávaných v rámci jakéhokoli jeho šetření, které provádí.

5. Dotčený orgán dozoru nad trhem a případně Komise zveřejní dohodu o společných činnostech, včetně názvů zúčastněných stran.

Článek 60

Společné kontrolní akce

1. Orgány dozoru nad trhem provádějí souběžné koordinované kontrolní akce (dále jen „společné kontrolní akce“) u konkrétních produktů s digitálními prvky nebo jejich kategorií za účelem kontroly souladu s tímto nařízením nebo odhalení jeho porušení. Tyto společné kontrolní akce mohou zahrnovat kontroly produktů s digitálními prvky pořízených pod krycí identitou.

2. Pokud se zapojené příslušné orgány dozoru nad trhem nedohodnou jinak, koordinuje společné kontrolní akce Komise. Koordinátor společné kontrolní akce zveřejní dle potřeby souhrnné výsledky.

3. Pokud agentura ENISA při plnění svých úkolů, mimo jiné na základě oznámení obdržených podle čl. 14 odst. 1 a 3, určí kategorie produktů s digitálními prvky, u nichž mohou být organizovány společné kontrolní akce, předloží koordinátorovi návrh na společnou kontrolní akci podle odstavce 2 tohoto článku k posouzení orgány dozoru nad trhem.

4. Zapojené orgány dozoru nad trhem mohou při provádění společných kontrolních akcí využívat vyšetřovací pravomoci stanovené v článcích 52 až 58 a jakékoli další pravomoci, které jim svěřuje vnitrostátní právo.

5. Orgány dozoru nad trhem mohou k účasti na společných kontrolních akcích přizvat úředníky Komise a další doprovázející osoby pověřené Komisí.

KAPITOLA VI

PŘENESENÉ PRAVOMOCI A POSTUP PROJEDNÁVÁNÍ VE VÝBORU

Článek 61

Výkon přenesení pravomoci

1. Pravomoc přijímat akty v přenesené pravomoci je svěřena Komisi za podmínek stanovených v tomto článku.

2. Pravomoc přijímat akty v přenesené pravomoci uvedená v čl. 2 odst. 5 druhém pododstavci, čl. 7 odst. 3, čl. 8 odst. 1 a 2, čl. 13 odst. 8 čtvrtém pododstavci, čl. 14 odst. 9, článku 25, čl. 27 odst. 9, čl. 28 odst. 5 a čl. 31 odst. 5 je svěřena Komisi na dobu pěti let ode dne 10. prosince 2024. Komise vypracuje zprávu o přenesení pravomoci nejpozději devět měsíců před koncem tohoto pětiletého období. Přenesení pravomoci se automaticky prodlužuje o stejně dlouhá období, pokud Evropský parlament nebo Rada nevysloví proti tomuto prodloužení námitku nejpozději tři měsíce před koncem každého z těchto období.

3. Evropský parlament nebo Rada mohou přenesení pravomoci uvedené v čl. 2 odst. 5 druhém pododstavci, čl. 7 odst. 3, čl. 8 odst. 1 a 2, čl. 13 odst. 8 čtvrtém pododstavci, čl. 14 odst. 9, článku 25, čl. 27 odst. 9, čl. 28 odst. 5 a čl. 31 odst. 5 kdykoli zrušit. Rozhodnutím o zrušení se ukončuje přenesení pravomoci v něm určené. Rozhodnutí nabývá účinku prvním dnem po zveřejnění v *Úředním věstníku Evropské unie,* nebo k pozdějšímu dni, který je v něm upřesněn. Nedotýká se platnosti již platných aktů v přenesené pravomoci.

4. Před přijetím aktu v přenesené pravomoci Komise vede konzultace s odborníky jmenovanými jednotlivými členskými státy v souladu se zásadami stanovenými v interinstitucionální dohodě ze dne 13. dubna 2016 o zdokonalení tvorby právních předpisů.

5. Přijetí aktu v přenesené pravomoci Komise neprodleně oznámí současně Evropskému parlamentu a Radě.

6. Akt v přenesené pravomoci přijatý podle čl. 2 odst. 5 druhého pododstavce, čl. 7 odst. 3, čl. 8 odst. 1 nebo 2, čl. 13 odst. 8 čtvrtého pododstavce, čl. 14 odst. 9, článku 25, čl. 27 odst. 9, čl. 28 odst. 5 nebo čl. 31 odst. 5 vstoupí v platnost pouze tehdy, pokud proti němu Evropský parlament nebo Rada nevysloví námitky ve lhůtě dvou měsíců ode dne, kdy jim byl tento akt oznámen, nebo pokud Evropský parlament i Rada před uplynutím této lhůty informují Komisi o tom, že námitky nevysloví. Z podnětu Evropského parlamentu nebo Rady se tato lhůta prodlouží o dva měsíce.

Článek 62

Postup projednávání ve výboru

1. Komisi je nápomocen výbor. Tento výbor je výborem ve smyslu nařízení (EU) č. 182/2011.

2. Odkazuje-li se na tento odstavec, použije se článek 5 nařízení (EU) č. 182/2011.

3. Má-li být stanovisko výboru získáno písemným postupem, ukončuje se tento postup bez výsledku, pokud o tom ve lhůtě pro vydání stanoviska rozhodne předseda výboru nebo pokud o to požádá člen výboru.

KAPITOLA VII

DŮVĚRNOST A SANKCE

Článek 63

Zachování důvěrnosti

1. Všechny strany, které se podílejí na uplatňování tohoto nařízení, zachovávají důvěrnost informací a údajů, které získají při provádění svých úkolů a činnosti, takovým způsobem, aby chránily zejména:

a) práva duševního vlastnictví a důvěrné obchodní informace nebo obchodní tajemství fyzických nebo právnických osob, včetně zdrojového kódu, s výjimkou případů, na které se vztahuje článek 5 směrnice Evropského parlamentu a Rady (EU) 2016/943 ([37]),

b) účinné uplatňování tohoto nařízení, zejména za účelem inspekcí, šetření nebo auditů,

c) veřejné a národní bezpečnostní zájmy,

d) integritu trestního nebo správního řízení.

2. Aniž je dotčen odstavec 1, informace vyměňované důvěrně mezi orgány dozoru nad trhem a mezi orgány dozoru nad trhem a Komisí se nezpřístupní bez předchozí dohody s orgánem dozoru nad trhem, od kterého informace pocházejí.

3. Ustanoveními odstavců 1 a 2 nejsou dotčena práva a povinnosti Komise, členských států a oznámených subjektů ohledně vzájemného informování a šíření výstrah ani povinnosti dotčených osob poskytovat informace podle trestního práva členských států.

4. Komise a členské státy si mohou v případě potřeby vyměňovat citlivé informace s relevantními orgány třetích zemí, s nimiž uzavřely dvoustranná nebo vícestranná ujednání o ochraně důvěrnosti zaručující přiměřenou úroveň ochrany.

Článek 64

Sankce

1. Členské státy stanoví pravidla pro ukládání sankcí za porušení tohoto nařízení a přijmou veškerá opatření nezbytná k zajištění jejich uplatňování. Tyto sankce musejí být účinné, přiměřené a odrazující. Členské státy bez prodlení uvědomí o takových pravidlech a opatřeních Komisi a neprodleně ji informují o veškerých pozdějších změnách těchto pravidel nebo opatření.

2. Za nedodržení základních požadavků na kybernetickou bezpečnost stanovených v příloze I a povinností stanovených v článcích 13 a 14 se uloží správní pokuty až do výše 15 000 000 EUR, nebo dopustí-li se porušení podnik, až do výše 2,5 % jeho celkového ročního obratu celosvětově za předchozí finanční rok podle toho, která hodnota je vyšší.

3. Za nedodržení povinností stanovených v článcích 18 až 23, článku 28, čl. 30 odst. 1 až 4, čl. 31 odst. 1 až 4, čl. 32 odst. 1, 2 a 3, čl. 33 odst. 5 a v článcích 39, 41, 47, 49 a 53 se uloží správní pokuty až do výše 10 000 000 EUR, nebo dopustí-li se porušení podnik, až do výše 2 % jeho celkového ročního obratu celosvětově za předchozí finanční rok podle toho, která hodnota je vyšší.

4. Za poskytnutí nesprávných, neúplných nebo zavádějících informací oznámeným subjektům a orgánům dozoru nad trhem v reakci na žádost se uloží správní pokuty až do výše 5 000 000 EUR, nebo dopustí-li se porušení podnik, až do výše 1 % jeho celkového ročního obratu celosvětově za předchozí finanční rok podle toho, která hodnota je vyšší.

([37]) Směrnice Evropského parlamentu a Rady (EU) 2016/943 ze dne 8. června 2016 o ochraně nezveřejněného know-how a obchodních informací (obchodního tajemství) před jejich neoprávněným získáním, využitím a zpřístupněním (Úř. věst. L 157, 15.6.2016, s. 1).

5. Při rozhodování o výši správní pokuty se v jednotlivých případech zohlední všechny relevantní okolnosti konkrétní situace a náležitě se přihlédne k následujícím okolnostem:

a) k povaze, závažnosti a době trvání porušení a jeho následkům,

b) k tomu, zda již byly stejnému hospodářskému subjektu za podobné porušení uloženy správní pokuty stejnými nebo jinými orgány dozoru nad trhem,

c) k velikosti hospodářského subjektu, který se porušení dopustil, zejména s ohledem na mikropodniky a malé a střední podniky, včetně začínajících podniků, a k jeho podílu na trhu.

6. Orgány dozoru nad trhem, které ukládají správní pokuty, informují o uložení pokut orgány dozoru nad trhem jiných členských států prostřednictvím informačního a komunikačního systému podle článku 34 nařízení (EU) 2019/1020.

7. Každý členský stát stanovuje pravidla týkající se toho, zda a do jaké míry je možno ukládat správní pokuty orgánům veřejné moci a veřejným subjektům usazeným v daném členském státě.

8. V závislosti na právním systému členských států lze pravidla pro správní pokuty uplatňovat tak, aby pokuty byly ukládány příslušnými vnitrostátními soudy nebo jinými orgány v souladu s pravomocemi stanovenými na vnitrostátní úrovni v těchto členských státech. Uplatňování těchto pravidel v uvedených členských státech má rovnocenný účinek.

9. Správní pokuty mohou být uloženy v závislosti na okolnostech každého jednotlivého případu spolu s jakýmikoli dalšími nápravnými nebo omezujícími opatřeními, které uplatní orgány dozoru nad trhem v souvislosti se stejným porušením.

10. Odchylně od odstavců 3 až 9 se správní pokuty uvedené v těchto odstavcích nevztahují na:

a) výrobce, kteří jsou považováni za mikropodniky nebo malé podniky, pokud jde o jakékoli nedodržení lhůty uvedené v čl. 14 odst. 2 písm. a) nebo čl. 14 odst. 4 písm. a),

b) jakékoli porušení tohoto nařízení správci softwaru s otevřeným zdrojovým kódem.

Článek 65

Zástupné žaloby

Na zástupné žaloby podané proti hospodářským subjektům ve věci porušení ustanovení tohoto nařízení, které poškozuje nebo může poškodit kolektivní zájmy spotřebitelů, se vztahuje směrnice (EU) 2020/1828.

KAPITOLA VIII

PŘECHODNÁ A ZÁVĚREČNÁ USTANOVENÍ

Článek 66

Změna nařízení (EU) 2019/1020

V příloze I nařízení (EU) 2019/1020 se doplňuje nový bod, který zní:

„72. Nařízení Evropského parlamentu a Rady (EU) 2024/2847 (*).

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

Článek 67

Změna směrnice (EU) 2020/1828

V příloze I směrnice (EU) 2020/1828 se doplňuje nový bod, který zní:

„69. Nařízení Evropského parlamentu a Rady (EU) 2024/2847 (*).

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

Článek 68

Změna nařízení (EU) č. 168/2013

V části C1 v tabulce v příloze II nařízení Evropského parlamentu a Rady (EU) č. 168/2013 ([38]) se doplňuje nová položka, která zní:

„

16	18	Ochrana vozidla proti kybernetickým útokům		x	x	x	x	x	x	x	x	x	x	x	x	x	X

“

Článek 69

Přechodná ustanovení

1. Certifikáty 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.

2. Produkty s digitálními prvky, které byly uvedeny na trh před 11. prosincem 2027, se řídí požadavky tohoto nařízení pouze tehdy, pokud po uvedeném datu procházejí tyto produkty podstatnou změnou.

3. Odchylně od odstavce 2 tohoto článku se povinnosti stanovené v článku 14 vztahují na všechny produkty s digitálními prvky spadající do oblasti působnosti tohoto nařízení, které byly uvedeny na trh před 11. prosincem 2027.

Článek 70

Hodnocení a přezkum

1. Do 11. prosince 2030 a poté každé čtyři roky předloží Komise Evropskému parlamentu a Radě zprávu o hodnocení a přezkumu tohoto nařízení. Tyto zprávy se zveřejní.

2. Do 11. září 2028 předloží Komise po konzultaci s agenturou ENISA a sítí CSIRT Evropskému parlamentu a Radě zprávu, ve které posoudí účinnost jednotné platformy pro podávání zpráv stanovené v článku 16 a dopad uplatňování důvodů souvisejících s kybernetickou bezpečností uvedených v čl. 16 odst. 2 týmy CSIRT určenými jako koordinátoři na účinnost jednotné platformy pro podávání zpráv, pokud jde o včasné rozesílání obdržených oznámení dalším příslušným týmům CSIRT.

Článek 71

Vstup v platnost a použitelnost

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

([38]) Nařízení Evropského parlamentu a Rady (EU) č. 168/2013 ze dne 15. ledna 2013 o schvalování dvoukolových nebo tříkolových vozidel a čtyřkolek a dozoru nad trhem s těmito vozidly (Úř. věst. L 60, 2.3.2013, s. 52).

2. Toto nařízení se použije ode dne 11. prosince 2027.

Článek 14 se však použije se ode dne 11. září 2026 a kapitola IV (články 35 až 51) se použije ode dne 11. června 2026.

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

Ve Štrasburku dne 23. října 2024.

Za Evropský parlament	*Za Radu*
předsedkyně	*předseda*
R. METSOLA	ZSIGMOND B. P.

PŘÍLOHA I

ZÁKLADNÍ POŽADAVKY NA KYBERNETICKOU BEZPEČNOST

Část I Požadavky na kybernetickou bezpečnost týkající se vlastností produktů s digitálními prvky

1) Produkty s digitálními prvky musí být navrženy, vyvinuty a vyrobeny tak, aby zajišťovaly odpovídající úroveň kybernetické bezpečnosti zohledňující rizika.

2) na základě posouzení kybernetického bezpečnostního rizika podle čl. 13 odst. 2 jsou v příslušných případech produkty s digitálními prvky:

   a) dodávány na trh bez známých zneužitelných zranitelností,

   b) dodávány na trh v konfiguraci zabezpečené na úrovni standardního nastavení, pokud se výrobce nedohodne s podnikatelským uživatelem v souvislosti s produktem s digitálními prvky uzpůsobeným na míru jinak, včetně možnosti obnovit produkt do původního stavu,

   c) zajišťují, aby bylo možné řešit zranitelnosti prostřednictvím bezpečnostních aktualizací, a automatických bezpečnostních aktualizací tam, kde je to možné, které lze v přiměřeném časovém rámci nainstalovat jako výchozí nastavení, s jasným a snadno použitelným mechanismem výjimky, a to prostřednictvím oznamování dostupných aktualizací uživatelům a možnosti je dočasně odložit,

   d) zajišťují ochranu před neoprávněným přístupem vhodnými kontrolními mechanismy, mimo jiné na základě systémů správy ověřování, identity nebo přístupu, a podávají zprávy o možném neoprávněném přístupu,

   e) chrání důvěrnost uchovávaných, předávaných nebo jinak zpracovávaných údajů, ať již osobních či jiných, například šifrováním příslušných uložených nebo přenášených údajů prostřednictvím nejmodernějších mechanismů a za pomoci jiných technických prostředků,

   f) chrání integritu uchovávaných, předávaných nebo jinak zpracovávaných údajů, osobních či jiných údajů, příkazů, programů a konfigurace před jakoukoli manipulací nebo změnou, které uživatel nepovolil, a podávají zprávy o poškození,

   g) zpracovávají pouze osobní nebo jiné údaje, které jsou přiměřené, relevantní a omezené na to, co je nezbytné ve vztahu k zamýšlenému účelu produktu s digitálními prvky („minimalizace údajů“),

   h) chrání dostupnost základních a klíčových funkcí, a to i po incidentu, prostřednictvím opatření ke zvýšení odolnosti vůči útokům, jejichž důsledkem je odepření služby, a opatření ke zmírňování těchto útoků,

   i) minimalizují svůj vlastní nepříznivý dopad nebo dopad připojených zařízení na dostupnost služeb poskytovaných jinými zařízeními nebo sítěmi,

   j) jsou navrženy, vyvinuty a vyrobeny tak, aby omezily prostory k útoku, včetně vnějších rozhraní,

   k) jsou navrženy, vyvinuty a vyrobeny tak, aby se snížil dopad incidentu použitím vhodných mechanismů a technik zmírňujících zneužití,

   l) poskytují informace související s bezpečností tím, že zaznamenávají a kontrolují příslušnou interní činnost, včetně přístupu k údajům, službám nebo funkcím či jejich změn, s možností využít mechanismus výjimky pro uživatele,

   m) poskytují uživatelům možnost bezpečně a snadno natrvalo odstranit všechny údaje a nastavení, a pokud mohou být tyto údaje přeneseny do jiných produktů nebo systémů, zajišťují, aby se tak stalo bezpečným způsobem.

Část II Požadavky na řešení zranitelností

Výrobci produktů s digitálními prvky:

1) určí a zdokumentují zranitelnosti a komponenty obsažené v produktech s digitálními prvky, mj. na základě vypracování softwarového kusovníku (SBOM) v běžně používaném strojově čitelném formátu, který obsahuje přinejmenším nejdůležitější závislosti produktu,

2) v souvislosti s riziky, která pro produkty s digitálními prvky představují, neprodleně řeší a odstraňují zranitelnosti, mj. na základě poskytování bezpečnostních aktualizací; v případě, že je to technicky možné, jsou bezpečnostní aktualizace poskytovány odděleně od funkčních aktualizací,

3) provádějí účinné a pravidelné testy a pravidelný přezkum bezpečnosti produktu s digitálními prvky,

4) po zveřejnění bezpečnostní aktualizace poskytují a uveřejňují informace o opravených zranitelnostech, včetně popisu těchto zranitelností, informací umožňujících uživatelům zjistit dotčený produkt s digitálními prvky, dopadu zranitelností, jejich závažnosti a jasných a přístupných informací, které uživatelům pomáhají tyto zranitelnosti odstranit; v řádně odůvodněných případech, pokud se výrobci domnívají, že bezpečnostní rizika spojená se zveřejněním převažují nad bezpečnostními přínosy, mohou oddálit zveřejnění informací týkajících se opravy zranitelností až do doby, kdy budou mít uživatelé možnost příslušnou opravu použít,

5) zavádějí a prosazují politiku koordinovaného zveřejňování zranitelností,

6) přijímají opatření ke snadnějšímu sdílení informací o možných zranitelnostech svého produktu s digitálními prvky a o komponentách třetích stran obsažených v daném produktu, mimo jiné poskytnutím kontaktní adresy pro oznamování zranitelností zjištěných v produktu s digitálními prvky,

7) stanovují mechanismy pro bezpečnou distribuci aktualizací produktů s digitálními prvky s cílem zajistit, že zranitelnosti budou včas opraveny nebo zmírněny, a že se tak bude u bezpečnostních aktualizací dít automaticky, je-li to možné,

8) zajišťují, aby v případě, že jsou k dispozici bezpečnostní aktualizace pro řešení zjištěných bezpečnostních problémů, byly neprodleně, a pokud neexistuje jiná dohoda mezi výrobcem a podnikatelským uživatelem s ohledem na produkt s digitálními prvky zhotovený na zakázku, bezplatně šířeny spolu s poradními zprávami, které uživatelům poskytují relevantní informace, včetně informací o možných opatřeních, jež je třeba přijmout.

PŘÍLOHA II

INFORMACE A POKYNY PRO UŽIVATELE

K produktu s digitálními prvky musejí být přiloženy alespoň následující informace:

1. jméno, zapsaný obchodní název nebo zapsaná ochranná známka výrobce, poštovní a e-mailová adresa nebo jiný digitální kontakt a případně internetová stránka, na níž lze výrobce kontaktovat,
2. jednotné kontaktní místo, kde lze oznámit a obdržet informace o zranitelnostech produktu s digitálními prvky a kde lze nalézt výrobcovu politiku koordinovaného zveřejňování zranitelností,
3. název a typ a veškeré další informace umožňující jedinečnou identifikaci produktu s digitálními prvky,
4. zamýšlený účel produktu s digitálními prvky, včetně bezpečnostního prostředí poskytovaného výrobcem, jakož i základní funkce produktu a informace o jeho bezpečnostních vlastnostech,
5. jakékoli známé nebo předvídatelné okolnosti související s používáním produktu s digitálními prvky v souladu s jeho zamýšleným účelem nebo za podmínek rozumně předvídatelného nesprávného použití, které mohou vést k významným kybernetickým bezpečnostním rizikům,
6. případně internetová adresa, na níž je možné získat přístup k EU prohlášení o shodě,
7. druh technické bezpečnostní podpory, kterou výrobce nabízí, a datum skončení doby podpory, během níž uživatelé mohou očekávat, že budou řešeny zranitelnosti a že obdrží bezpečnostní aktualizace;
8. podrobné pokyny nebo internetová adresa odkazující na tyto podrobné pokyny a informace:
   a) o nezbytných opatřeních během počátečního uvedení produktu s digitálními prvky do provozu a po celou dobu jeho životnosti, aby bylo zajištěno jeho bezpečné používání,
   b) o tom, jak mohou změny produktu s digitálními prvky ovlivnit bezpečnost údajů,
   c) o tom, jak lze nainstalovat bezpečnostní aktualizace,
   d) o bezpečném vyřazení produktu s digitálními prvky z provozu, včetně informací o tom, jak lze bezpečně odstranit údaje o uživatelích,
   e) o tom, jak lze vypnout standardní nastavení umožňující automatickou instalaci bezpečnostních aktualizací, jak se požaduje v příloze I části I písm. c),
   f) v případě, že je produkt s digitálními prvky určen k zabudování do jiných produktů s digitálními prvky, informace, které potřebuje ten, kdo produkt kompletuje, k tomu, aby mohl dodržet základní požadavky na kybernetickou bezpečnost stanovené v příloze I a požadavky na dokumentaci stanovené v příloze VII,
9. rozhodne-li se výrobce, že uživateli zpřístupní softwarový kusovník, informace o tom, kde k němu lze získat přístup.

PŘÍLOHA III

DŮLEŽITÉ PRODUKTY S DIGITÁLNÍMI PRVKY

Třída I

1. Software pro systémy správy identity a pro správu privilegovaného přístupu a hardware, včetně čtečky k ověřování totožnosti a ke kontrole přístupu, mj. biometrické čtečky
2. samostatné a vestavěné prohlížeče
3. správci hesel
4. software, který vyhledává škodlivé programy, odstraňuje je nebo je dává do karantény
5. produkty s digitálními prvky s funkcí virtuální soukromé sítě (VPN)
6. systémy řízení sítě
7. systémy řízení bezpečnostních informací a událostí
8. boot manageři
9. infrastruktura veřejných klíčů a software k vydávání digitálních certifikátů
10. fyzická a virtuální síťová rozhraní
11. operační systémy
12. směrovače, modemy určené pro připojení k internetu a přepínače
13. mikroprocesory s bezpečnostními funkcemi
14. mikrořadiče s bezpečnostními funkcemi
15. aplikačně specifické integrované obvody (ASIC) a programovatelná hradlová pole (FPGA) s bezpečnostními funkcemi
16. obecní virtuální asistenti pro chytré domácnosti
17. produkty pro chytré domácnosti s bezpečnostními funkcemi, včetně chytrých dveřních zámků, bezpečnostních kamer, systémů pro monitorování dětí a poplašných systémů
18. hračky připojené k internetu, na které se vztahuje směrnice Evropského parlamentu a Rady 2009/48/ES [1] a které mají sociální interaktivní funkce (např. k mluvení nebo natáčení) nebo funkce ke sledování polohy
19. osobní výrobky k nošení, které se nosí nebo umísťují na lidské tělo, jejichž účelem je sledovat zdravotní stav a na něž se nevztahuje nařízení (EU) 2017/745 ani (EU) 2017/746, nebo osobní výrobky k nošení, které jsou určeny pro děti a k používání u dětí

Třída II

1. hypervizory a systémy runtime kontejnerů, které podporují virtualizované provedení operačních systémů a podobných prostředí
2. firewally, systémy detekce narušení a prevence
3. mikroprocesory odolné proti manipulaci
4. mikrořadiče odolné proti manipulaci

[1] Směrnice Evropského parlamentu a Rady 2009/48/ES ze dne 18. června 2009 o bezpečnosti hraček (Úř. věst. L 170, 30.6.2009, s. 1).

PŘÍLOHA IV

KRITICKÉ PRODUKTY S DIGITÁLNÍMI PRVKY

1. Hardwarová zařízení s bezpečnostními schránkami
2. přístroje (EU) Smart meter gateway v rámci inteligentních měřicích systémů vymezených v čl. 2 bodu 23 směrnice Evropského parlamentu a Rady (EU) 2019/944 ([1]) a další přístroje pro účely zajištění větší bezpečnosti, mj. pro bezpečné přijímání plateb v kryptoměně
3. čipové karty nebo podobná zařízení, včetně zabezpečených prvků

([1]) Směrnice Evropského parlamentu a Rady (EU) 2019/944 ze dne 5. června 2019 o společných pravidlech pro vnitřní trh s elektřinou a o změně směrnice 2012/27/EU (Úř. věst. L 158, 14.6.2019, s. 125).

PŘÍLOHA V

EU PROHLÁŠENÍ O SHODĚ

EU prohlášení o shodě podle článku 28 obsahuje všechny tyto informace:

1. název a druh a veškeré další informace umožňující jedinečnou identifikaci produktu s digitálními prvky
2. jméno a adresu výrobce nebo jeho zplnomocněného zástupce
3. uvedení skutečnosti, že EU prohlášení o shodě se vydává na výhradní odpovědnost poskytovatele
4. předmět prohlášení (identifikace produktu s digitálními prvky umožňující jej zpětně vysledovat, která může v případě potřeby obsahovat fotografii)
5. konstatování, že předmět výše popsaného prohlášení je ve shodě s příslušnými harmonizačními právními předpisy Unie
6. odkazy na veškeré příslušné harmonizované normy, které byly použity, nebo na veškeré další společné specifikace či certifikace kybernetické bezpečnosti, v souvislosti s nimiž se shoda prohlašuje
7. tam, kde je to relevantní, název a číslo oznámeného subjektu, popis postupu posuzování shody a identifikace vydaného certifikátu
8. další informace:

   Podepsáno za a jménem:

   (místo a datum vydání):

   (jméno, funkce) (podpis):

PŘÍLOHA VI

ZJEDNODUŠENÉ EU PROHLÁŠENÍ O SHODĚ

Zjednodušené EU prohlášení o shodě uvedené v čl. 13 odst. 20 se předkládá v této formě:

… [Název/jméno výrobce] tímto prohlašuje, že typ produktu s digitálními prvky … [uvedení typu produktu s digitálními prvky] je v souladu s nařízením (EU) 2024/2847 ([1]).

Úplné znění EU prohlášení o shodě je dostupné na této internetové adrese: …

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

PŘÍLOHA VII

OBSAH TECHNICKÉ DOKUMENTACE

Technická dokumentace podle 31 obsahuje alespoň tyto informace, které se vztahují na příslušný produkt s digitálními prvky:

1. všeobecný popis produktu s digitálními prvky, včetně:
   a) jeho zamýšleného účelu,
   b) verzí softwaru, které mají vliv na soulad se základními požadavky na kybernetickou bezpečnost,
   c) fotografií nebo ilustrací, které zobrazují vnější znaky, označení a vnitřní uspořádání, pokud je produkt s digitálními prvky hardwarovým produktem,
   d) informací a pokynů pro uživatele, jak je uvedeno v příloze II,
2. popis návrhu, vývoje a výroby produktu s digitálními prvky a postupů řešení zranitelností, včetně:
   a) nezbytných informací o návrhu a vývoji produktu s digitálními prvky, případně včetně výkresů a schémat a popisu architektury systému s vysvětlením, jakým způsobem na sebe komponenty softwaru vzájemně navazují nebo jak jsou do sebe začleněny a integrovány do celkového zpracování,
   b) nezbytných informací a specifikací postupů při řešení zranitelností zavedených výrobcem, včetně softwarového kusovníku, politiky koordinovaného zveřejňování zranitelností, důkazů o poskytnutí kontaktní adresy pro podávání zpráv o zranitelnostech a popisu technických řešení zvolených pro bezpečnou distribuci aktualizací,
   c) nezbytných informací a specifikací postupů výroby a monitorování produktu s digitálními prvky a ověření těchto postupů,
3. posouzení kybernetických bezpečnostních rizik, na ochranu před nimiž je produkt s digitálními prvky navrhován, vyvíjen, vyráběn, dodáván a udržován, podle článku 13, včetně toho, jak se uplatní základní požadavky na kybernetickou bezpečnost stanovené v příloze I části I,
4. příslušné informace, které byly vzaty v úvahu při stanovení doby podpory produktu s digitálními prvky, podle čl. 13 odst. 8,
5. seznam harmonizovaných norem, které byly zcela nebo zčásti použity a na které byly zveřejněny odkazy v *Úředním věstníku Evropské unie*, společných specifikací stanovených v článku 27 tohoto nařízení nebo evropských schémat certifikace kybernetické bezpečnosti přijatých podle nařízení (EU) 2019/881 v souladu s čl. 27 odst. 8 tohoto nařízení, a pokud tyto harmonizované normy, společné specifikace nebo evropská schémata certifikace kybernetické bezpečnosti použity nebyly, popis řešení zvolených ke splnění základních požadavků na kybernetickou bezpečnost stanovených v příloze I, části I a II včetně seznamu jiných příslušných technických specifikací, jež byly použity. V případě částečně použitých harmonizovaných norem, společných specifikací nebo evropských schémat certifikace kybernetické bezpečnosti se v technické dokumentaci uvedou ty části, jež byly použity,
6. protokoly o zkouškách provedených za účelem ověření shody produktu s digitálními prvky a postupů při řešení zranitelností s příslušnými základními požadavky na kybernetickou bezpečnost stanovenými v příloze I části I a II,
7. kopie EU prohlášení o shodě,
8. případně softwarový kusovník na základě odůvodněné žádosti orgánu dozoru nad trhem za předpokladu, že je to nezbytné k tomu, aby tento orgán mohl ověřit soulad se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I.

PŘÍLOHA VIII

POSTUPY POSUZOVÁNÍ SHODY

Část I Postup posuzování shody založený na interní kontrole (na základě modulu A)

1. Interní kontrola je postupem posuzování shody, kterým výrobce plní povinnosti stanovené v bodech 2, 3 a 4 této části a na vlastní odpovědnost zaručuje a prohlašuje, že produkty s digitálními prvky splňují všechny základní požadavky na kybernetickou bezpečnost stanovené v příloze I části I a že výrobce splňuje základní požadavky na kybernetickou bezpečnost stanovené v příloze I části II.

2. Výrobce vypracuje technickou dokumentaci podle přílohy VII.

3. Návrh, vývoj, výroba a řešení zranitelností produktů s digitálními prvky

   Výrobce přijme veškerá nezbytná opatření, aby postupy pro návrh, vývoj, výrobu a řešení zranitelností a jejich monitorování zajišťovaly soulad vyráběných nebo vyvíjených produktů s digitálními prvky a postupů zavedených výrobcem se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I části I a II.

4. Označení shody a prohlášení o shodě

   4.1. Výrobce umístí označení CE na každý jednotlivý produkt s digitálními prvky, který splňuje příslušné požadavky stanovené v tomto nařízení.

   4.2. Výrobce vypracuje pro každý produkt s digitálními prvky v souladu s článkem 28 písemné EU prohlášení o shodě a po dobu deseti let poté, co byl produkt s digitálními prvky uveden na trh, nebo po dobu trvání doby podpory, podle toho, které z těchto období je delší, je společně s technickou dokumentací uchovává, aby byly k dispozici vnitrostátním orgánům. V EU prohlášení o shodě je uveden produkt s digitálními prvky, pro nějž bylo vypracováno. Kopie EU prohlášení o shodě se na žádost poskytne příslušným orgánům.

5. Zplnomocnění zástupci

   Povinnosti výrobce stanovené v bodě 4 mohou být jeho jménem a na jeho odpovědnost splněny jeho zplnomocněným zástupcem, pokud jsou příslušné povinnosti uvedeny v pověření.

Část II EU přezkoušení typu (na základě modulu B)

1. EU přezkoušení typu je tou částí postupu posuzování shody, v níž oznámený subjekt přezkoumává technický návrh a vývoj produktu s digitálními prvky a postupy řešení zranitelností zavedené výrobcem a osvědčí, že produkt s digitálními prvky splňuje základní požadavky na kybernetickou bezpečnost stanovené v příloze I části I a že výrobce splňuje základní požadavky na kybernetickou bezpečnost stanovené v příloze I části II.

2. EU přezkoušení typu se provádí posouzením vhodnosti technického návrhu a vývoje produktu s digitálními prvky prostřednictvím přezkoumání technické dokumentace a podkladů podle bodu 3 a přezkoušením vzorků jedné nebo více kritických částí produktu (kombinace výrobního typu a konstrukčního typu).

3. Výrobce podá u jediného oznámeného subjektu, který si zvolil, žádost o EU přezkoušení typu.

   Žádost obsahuje:

   3.1. jméno a adresu výrobce, a pokud žádost podává zplnomocněný zástupce, jméno a adresu tohoto zplnomocněného zástupce,

   3.2. písemné prohlášení, že stejná žádost nebyla podána u jiného oznámeného subjektu,

   3.3. technickou dokumentaci, která musí umožňovat posouzení shody produktu s digitálními prvky s příslušnými základními požadavky na kybernetickou bezpečnost stanovenými v příloze I části I a postupy výrobce pro řešení zranitelností stanovenými v příloze I části II, a zahrnuje odpovídající analýzu a posouzení rizik. V technické dokumentaci musejí být uvedeny příslušné požadavky a v míře nutné pro posouzení se musí vztahovat na návrh, výrobu a fungování produktu s digitálními prvky. Technická dokumentace obsahuje v příslušných případech alespoň prvky stanovené v příloze VII,

3.4. podklady dokládající přiměřenost technických návrhů a vývojových řešení a postupů řešení zranitelností. Tyto podklady musejí odkazovat na všechny příslušné dokumenty, které byly použity, zejména pokud příslušné harmonizované normy nebo technické specifikace nebyly použity v celém rozsahu. Podklady zahrnují v případě potřeby výsledky zkoušek provedených příslušnou laboratoří výrobce nebo jinou zkušební laboratoří jeho jménem a na jeho odpovědnost.

4. Oznámený subjekt:

4.1. přezkoumá technickou dokumentaci a podklady s cílem posoudit přiměřenost technického návrhu a vývoje produktu s digitálními prvky se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I části I a soulad postupů pro řešení zranitelností zavedených výrobcem se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I části II;

4.2. ověří, zda byly vzorky vyvinuty nebo vyrobeny ve shodě s technickou dokumentací, a určí prvky, které byly navrženy a vyvinuty v souladu s použitelnými ustanoveními příslušných harmonizovaných norem nebo technických specifikací, a také prvky, které byly navrženy a vyvinuty, aniž byla použita příslušná ustanovení uvedených norem;

4.3. provede nebo nechá provést vhodná přezkoušení a zkoušky, aby ověřil, zda v případě, že výrobce zvolil pro požadavky stanovené v příloze I řešení podle příslušných harmonizovaných norem nebo technických specifikací, byly tyto normy a specifikace použity správně;

4.4. provede nebo nechá provést příslušná přezkoušení a zkoušky, aby ověřil, zda v případě, že pro požadavky stanovené v příloze I nebyla použita řešení podle příslušných harmonizovaných norem nebo technických specifikací, splňují řešení, která výrobce použil, odpovídající základní požadavky na kybernetickou bezpečnost;

4.5. dohodne se s výrobcem, na kterém místě budou přezkoušení a zkoušky provedeny.

5. Oznámený subjekt vypracuje zprávu o hodnocení, která zaznamená činnosti provedené podle bodu 4 a jejich výstupy. Aniž jsou dotčeny povinnosti oznámeného subjektu vůči oznamujícím orgánům, zveřejní oznámený subjekt obsah této zprávy, v celém rozsahu nebo částečně, pouze se souhlasem výrobce.

6. Pokud typ a postupy řešení zranitelností splňují základní požadavky na kybernetickou bezpečnost stanovené v příloze I, vydá oznámený subjekt výrobci certifikát o EU přezkoušení typu. Certifikát musí obsahovat jméno a adresu výrobce, závěry přezkoušení, podmínky platnosti certifikátu (existují-li) a údaje nezbytné k identifikaci schváleného typu a postupů řešení zranitelností. K certifikátu může být přiložena jedna nebo více příloh.

Certifikát a jeho přílohy obsahují všechny náležité informace umožňující vyhodnotit, zda jsou vyrobené nebo vyvinuté produkty s digitálními prvky ve shodě s přezkoušeným typem a postupy řešení zranitelností, a provést kontrolu za provozu.

Pokud typ a postupy řešení zranitelností nesplňují příslušné základní požadavky na kybernetickou bezpečnost stanovené v příloze I, oznámený subjekt odmítne vydat certifikát o EU přezkoušení typu a uvědomí o tom žadatele, přičemž odmítnutí podrobně odůvodní.

7. Oznámený subjekt dbá na to, aby byl informován o veškerých změnách obecně uznávaného stavu techniky, které by naznačovaly, že schválený typ a postupy řešení zranitelností již nemusí být v souladu se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I, a rozhodne, zda tyto změny vyžadují doplňující šetření. Pokud šetření vyžadují, oznámený subjekt o tom informuje výrobce.

Výrobce informuje oznámený subjekt, který uchovává technickou dokumentaci týkající se certifikátu o EU přezkoušení typu, o veškerých změnách schváleného typu a postupech řešení zranitelností, které mohou ovlivnit shodu se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I nebo podmínky platnosti certifikátu. Tyto změny vyžadují dodatečné schválení formou dodatku k původnímu certifikátu o EU přezkoušení typu.

8. Oznámený subjekt provádí pravidelné audity, aby zajistil příslušné uplatňování postupů řešení zranitelností, které jsou uvedeny v příloze I části II.

9. Každý oznámený subjekt informuje své oznamující orgány o certifikátech o EU přezkoušení typu nebo dodatcích k nim, které vydal nebo zrušil, a pravidelně či na žádost zpřístupní svým oznamujícím orgánům seznam certifikátů nebo dodatků k nim, které zamítl, pozastavil či jinak omezil.

   Každý oznámený subjekt informuje ostatní oznámené subjekty o certifikátech o EU přezkoušení typu nebo dodatcích k nim, které zamítl, zrušil, pozastavil či jinak omezil, a na žádost také o certifikátech nebo dodatcích k nim, které vydal.

   Komise, členské státy a ostatní oznámené subjekty mohou na žádost obdržet kopii certifikátů o EU přezkoušení typu a veškerých jejich dodatků. Komise a členské státy mohou na základě žádosti obdržet kopii technické dokumentace a výsledků přezkoušení provedených oznámeným subjektem. Do uplynutí doby platnosti certifikátu o EU přezkoušení typu uchovává oznámený subjekt kopii uvedeného certifikátu, jeho příloh a dodatků a také soubor technické dokumentace včetně dokumentace předložené výrobcem.

10. Po dobu deseti let od uvedení produktu s digitálními prvky na trh nebo po dobu trvání doby podpory, podle toho, které z těchto období je delší, uchovává výrobce pro potřebu vnitrostátních orgánů kopii certifikátu EU přezkoušení typu, jeho příloh a dodatků spolu s technickou dokumentací.

11. Zplnomocněný zástupce výrobce může podat žádost uvedenou v bodě 3 a plnit povinnosti stanovené v bodech 7 a 10 za předpokladu, že jsou uvedeny v pověření.

Část III Shoda s typem založená na interním řízení výroby (na základě modulu C)

1. Shoda s typem založená na interním řízení výroby je tou částí postupu posuzování shody, kterým výrobce plní povinnosti stanovené v bodech 2 a 3 této části a zaručuje a prohlašuje, že dané produkty s digitálními prvky jsou ve shodě s typem popsaným v certifikátu EU přezkoušení typu a splňují základní požadavky na kybernetickou bezpečnost stanovené v příloze I části I a že výrobce splňuje základní požadavky na kybernetickou bezpečnost stanovené v příloze I části II.

2. Výroba

   Výrobce přijme veškerá nezbytná opatření, aby výroba a její kontrola zajišťovaly shodu vyráběných produktů s digitálními prvky se schváleným typem popsaným v certifikátu EU přezkoušení typu a se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I části I, a zajišťuje, že splňuje základní požadavky na kybernetickou bezpečnost stanovené v příloze I části II.

3. Označení shody a prohlášení o shodě

   3.1. Výrobce umístí označení CE na každý jednotlivý produkt s digitálními prvky, který je ve shodě s typem popsaným v certifikátu EU přezkoušení typu a splňuje příslušné požadavky stanovené v tomto nařízení.

   3.2. Výrobce vypracuje pro daný model produktu písemné prohlášení o shodě a po dobu deseti let od uvedení produktu s digitálními prvky na trh nebo po dobu trvání doby podpory, podle toho, které z těchto časových období je delší, je uchovává pro potřebu vnitrostátních orgánů. V prohlášení o shodě se uvede model produktu, pro nějž bylo vypracováno. Kopie prohlášení o shodě se na žádost poskytne příslušným orgánům.

4. Zplnomocněný zástupce

   Povinnosti výrobce stanovené v bodě 3 mohou být jeho jménem a na jeho odpovědnost splněny jeho zplnomocněným zástupcem, pokud jsou uvedeny v příslušném pověření.

Část IV Shoda založená na komplexním zabezpečování kvality (na základě modulu H)

1. Shoda založená na komplexním zabezpečování kvality je postupem posuzování shody, kterým výrobce plní povinnosti stanovené v bodech 2 a 5 této části a na vlastní odpovědnost zaručuje a prohlašuje, že dané produkty s digitálními prvky nebo kategorie produktů splňují základní požadavky na kybernetickou bezpečnost stanovené v příloze I části I a že postupy pro řešení zranitelností zavedené výrobcem splňují požadavky stanovené v příloze I části II.

2. Návrh, vývoj, výroba a řešení zranitelností produktů s digitálními prvky

Výrobce používá schválený systém kvality podle bodu 3 pro navrhování, vývoj a závěrečnou kontrolu a zkoušení daných produktů s digitálními prvky a pro řešení zranitelností, zachovává jeho účinnost během doby podpory a podléhá dozoru podle bodu 4.

3. Systém kvality

3.1. Výrobce podá u oznámeného subjektu, který si zvolil, žádost o posouzení svého systému kvality pro dané produkty s digitálními prvky.

Žádost obsahuje:

a) jméno a adresu výrobce, a pokud žádost podává zplnomocněný zástupce, jméno a adresu tohoto zplnomocněného zástupce,

b) technickou dokumentaci pro jeden model z každé kategorie produktů s digitálními prvky, které se mají vyrábět nebo vyvíjet. Technická dokumentace obsahuje v příslušných případech přinejmenším prvky stanovené v příloze VII této směrnice,

c) dokumentaci týkající se systému kvality a

d) písemné prohlášení, že stejná žádost nebyla podána u jiného oznámeného subjektu.

3.2. Systém kvality zajistí shodu produktů se základními požadavky na kybernetickou bezpečnost stanovenými v příloze I části I a soulad postupů pro řešení zranitelností zavedených výrobcem s požadavky stanovenými v příloze I části II.

Všechny prvky, požadavky a předpisy používané výrobcem musejí být systematicky a uspořádaně dokumentovány ve formě písemných koncepcí, postupů a návodů. Dokumentace systému kvality musí umožňovat jednotný výklad programů, plánů, příruček a záznamů týkajících se kvality.

Dokumentace systému řízení kvality musí obsahovat zejména přiměřený popis:

a) cílů z hlediska kvality a organizační struktury, odpovědnosti a pravomocí vedení, pokud jde o návrh, vývoj, kvalitu produktu a řešení zranitelností,

b) technických specifikací návrhu a vývoje, včetně norem, které budou použity, a v případě, že se příslušné harmonizované normy nebo technické specifikace nepoužijí v celém rozsahu, popis prostředků, které budou použity, aby bylo zajištěno splnění základních požadavků na kybernetickou bezpečnost stanovených v příloze I části I, které se na produkty s digitálními prvky vztahují,

c) procesních specifikací návrhu, včetně norem, které budou použity, a v případě, že se příslušné harmonizované normy nebo technické specifikace nepoužijí v celém rozsahu, popis prostředků, které budou použity, aby bylo zajištěno splnění základních požadavků na kybernetickou bezpečnost stanovených v příloze I části II, které se na výrobce vztahují,

d) metod, postupů a systematických opatření týkajících se kontroly a ověřování návrhu, které budou použity při navrhování produktů s digitálními prvky náležejících do příslušné kategorie produktu,

e) odpovídajících metod, postupů a systematických opatření, které budou použity při výrobě, kontrole a zabezpečování kvality,

f) kontrol a zkoušek, které budou provedeny před výrobou, během výroby a po výrobě, s uvedením jejich četnosti,

g) záznamů o kvalitě, například protokolů o kontrolách, výsledků zkoušek, záznamů z provedených kalibrací a zpráv o kvalifikaci příslušných pracovníků,

h) prostředků umožňujících monitoring požadované kvality návrhu a produktu a efektivního fungováním systému kvality.

3.3. Oznámený subjekt posoudí systém kvality s cílem určit, zda splňuje požadavky podle bodu 3.2.

U prvků systému kvality, které odpovídají příslušným specifikacím vnitrostátní normy, kterou se provádí příslušná harmonizovaná norma nebo technická specifikace, předpokládá shodu s těmito požadavky.

Auditorský tým musí mít zkušenosti se systémy řízení kvality a znalosti použitelných požadavků stanovených v tomto nařízení a alespoň jeden jeho člen musí mít zkušenosti s hodnocením příslušné oblasti produktu a technologie daného produktu. Audit zahrnuje návštěvu v provozních prostorách výrobce za účelem jejich posouzení, pokud takové prostory existují. Auditorský tým přezkoumá technickou dokumentaci uvedenou v písm. b) bodu 3.1, aby ověřil, že je výrobce schopen určit příslušné požadavky stanovené v tomto nařízení a provádět nezbytná přezkoušení, aby zajistil soulad produktu s digitálními prvky s těmito požadavky.

Rozhodnutí se oznámí výrobci nebo jeho zplnomocněnému zástupci.

Oznámení musí obsahovat závěry auditu a odůvodněné rozhodnutí o posouzení.

3.4. Výrobce se zavazuje, že bude plnit povinnosti vyplývající ze schváleného systému kvality a že jej bude udržovat, aby byl i nadále odpovídající a účinný.

3.5. Výrobce informuje oznámený subjekt, který schválil systém kvality, o každé zamýšlené změně tohoto systému.

Oznámený subjekt navrhované změny posoudí a rozhodne, zda změněný systém kvality bude i nadále splňovat požadavky podle bodu 3.2, nebo zda je třeba provést nové posouzení.

Oznámený subjekt oznámí své rozhodnutí výrobci. Oznámení musí obsahovat závěry kontrol a odůvodněné rozhodnutí o posouzení.

4. Dohled, za který odpovídá oznámený subjekt

4.1. Účelem dozoru je zajistit, aby výrobce řádně plnil povinnosti vyplývající ze schváleného systému kvality.

4.2. Za účelem posouzení umožní výrobce oznámenému subjektu přístup do prostor určených pro navrhování, vývoj, výrobu, kontrolu, zkoušky a skladování a poskytne mu veškeré potřebné informace, zejména:

a) dokumentaci systému kvality,

b) záznamy o kvalitě uvedené v části systému kvality týkající se navrhování, např. výsledky analýz, výpočtů a zkoušek,

c) záznamy o kvalitě uvedené ve výrobní části systému kvality, např. protokoly o kontrolách, výsledky zkoušek, záznamy z provedených kalibrací a zprávy o kvalifikaci příslušných pracovníků.

4.3. Oznámený subjekt provádí pravidelné audity, aby se ujistil, že výrobce udržuje a používá systém kvality, a předkládá výrobci zprávu o auditu.

5. Označení shody a prohlášení o shodě

5.1. Výrobce umístí označení shody a na odpovědnost oznámeného subjektu uvedeného v bodě 3.1. identifikační číslo tohoto subjektu na každý jednotlivý produkt s digitálními prvky, který splňuje požadavky stanovené v příloze I části I.

5.2. Výrobce vypracuje pro daný model produktu písemné prohlášení o shodě a po dobu deseti let od uvedení produktu s digitálními prvky na trh nebo po dobu trvání doby podpory, podle toho, které z těchto časových období je delší, je uchovává pro potřebu vnitrostátních orgánů. V prohlášení o shodě se uvede model produktu, pro nějž bylo vypracováno.

Kopie prohlášení o shodě se na žádost poskytne příslušným orgánům.

6. Výrobce uchovává pro potřebu vnitrostátních orgánů po dobu nejméně deseti let po uvedení produktu s digitálními prvky na trh nebo po dobu trvání doby podpory, podle toho, které z těchto časových období je delší:

a) technickou dokumentaci uvedenou v bodě 3.1,

b) dokumentaci týkající se systému kvality uvedenou v bodě 3.1,

c) informace o schválené změně podle bodu 3.5,

d) rozhodnutí a zprávy oznámeného subjektu podle bodů 3.5 a 4.3.

7. Každý oznámený subjekt informuje své oznamující orgány o schváleních systému kvality, která vydal nebo zrušil, a pravidelně či na žádost zpřístupní svým oznamujícím orgánům seznam schválení systému kvality, která zamítl, pozastavil či jinak omezil.

Každý oznámený subjekt informuje ostatní oznámené subjekty o schváleních systému kvality, která zamítl, pozastavil nebo zrušil, a na žádost o schváleních systému kvality, která vydal.

8. Zplnomocněný zástupce

Povinnosti výrobce stanovené v bodech 3.1, 3.5, 5 a 6 mohou být jeho jménem a na jeho odpovědnost plněny jeho zplnomocněným zástupcem, pokud jsou uvedeny v pověření.

K tomuto aktu bylo učiněno prohlášení, které lze nalézt v Úř. věst. C, 2024/6786, 20.11.2024, ELI: http://data.europa.eu/eli/C/2024/6786/oj.