Rada
Európskej únie

V Bruseli 16. septembra 2022
(OR. en)

12429/22

Medziinštitucionálny spis:
2022/0272(COD)

CYBER 298
JAI 1181
DATAPROTECT 254
TELECOM 369
MI 665
CSC 388
CSCI 133
CODEC 1310
IA 133

NÁVRH

Od:	Martine DEPREZOVÁ, riaditeľka, v zastúpení generálnej tajomníčky Európskej komisie
Dátum doručenia:	15. septembra 2022
Komu:	Generálny sekretariát Rady
Č. dok. Kom.:	COM(2022) 454 final
Predmet:	Návrh NARIADENIA EURÓPSKEHO PARLAMENTU A RADY o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadenia (EÚ) 2019/1020

Delegáciám v prílohe zasielame dokument COM(2022) 454 final.

Príloha: COM(2022) 454 final

EURÓPSKA
KOMISIA

V Bruseli 15. 9. 2022
COM(2022) 454 final

2022/0272 (COD)

Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY

o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadenia (EÚ) 2019/1020

(Text s významom pre EHP)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

DÔVODOVÁ SPRÁVA

1. KONTEXT NÁVRHU

• Dôvody a ciele návrhu

Hardvérové a softvérové produkty sú čoraz častejšie predmetom úspešných kybernetických útokov, ktoré v roku 2021 viedli k odhadovaným celosvetovým ročným nákladom spôsobeným počítačovou kriminalitou vo výške 5,5 bilióna EUR. Takéto produkty majú dva hlavné problémy, ktoré zvyšujú náklady používateľov a spoločnosti: 1. nízku úroveň kybernetickej bezpečnosti, ktorá sa prejavuje rozšíreným výskytom zraniteľností a nedostatočným a nekonzistentným poskytovaním bezpečnostných aktualizácií na ich riešenie, a 2. nedostatočné chápanie používateľov a ich prístup k informáciám, čo im bráni vybrať si produkty s vhodnými vlastnosťami kybernetickej bezpečnosti alebo používať ich bezpečným spôsobom. V prepojenom prostredí môže kybernetický bezpečnostný incident jedného produktu ovplyvniť celú organizáciu alebo celý dodávateľský reťazec, pričom sa často rozšíri naprieč hranicami vnútorného trhu v priebehu niekoľkých minút. Môže to viesť k vážnemu narušeniu hospodárskych a sociálnych činností alebo dokonca k ohrozeniu života.

Kybernetická bezpečnosť produktov s digitálnymi prvkami má výrazný cezhraničný rozmer, keďže produkty vyrobené v jednej krajine sa často používajú na celom vnútornom trhu. Navyše incidenty, ktoré spočiatku ovplyvňujú jeden subjekt alebo jeden členský štát, sa často v priebehu minút rozšíria na celý vnútorný trh.

Hoci sa existujúce právne predpisy o vnútornom trhu uplatňujú na určité produkty s digitálnymi prvkami, na väčšinu hardvérových a softvérových produktov sa v súčasnosti nevzťahujú žiadne právne predpisy EÚ, ktoré by sa zaoberali ich kybernetickou bezpečnosťou. V súčasnom právnom rámci EÚ sa nerieši najmä kybernetická bezpečnosť nezabudovaného softvéru, a to ani vtedy, keď útoky na kybernetickú bezpečnosť sú čoraz častejšie zamerané na zraniteľnosti týchto produktov a spôsobujú značné spoločenské a hospodárske náklady. Existujú početné príklady kybernetických útokov zneužívajúcich suboptimálne zabezpečenie produktu, ktoré stoja za zmienku, napríklad ransomvérový červ WannaCry, ktorý v roku 2017 zneužil zraniteľnosť Windows na 200 000 počítačoch v 150 krajinách a spôsobil škody vo výške niekoľkých miliárd USD; ransomvérový útok na Kaseya VSA, pri ktorom sa použil softvér na správu serverov dodávateľského reťazca Kaseya na útok na vyše 1 000 spoločností a donútil sieť supermarketov zatvoriť všetkých svojich 500 predajní po celom Švédsku; alebo množstvo kybernetických incidentov, pri ktorých boli hacknuté bankové aplikácie s cieľom ukradnúť peniaze od nič netušiacich spotrebiteľov.

V snahe zaistiť riadne fungovanie vnútorného trhu boli identifikované dva hlavné ciele: 1. vytvoriť podmienky pre vývoj bezpečných produktov s digitálnymi prvkami tým, že sa zaistí, aby sa na trh uvádzali hardvérové a softvérové produkty s menším počtom zraniteľností a aby výrobcovia brali vážne bezpečnosť počas celého životného cyklu produktu, a 2. vytvoriť podmienky, ktoré umožnia používateľom zohľadniť kybernetickú bezpečnosť pri výbere a používaní produktov s digitálnymi prvkami. Boli stanovené štyri špecifické ciele: i) zaistiť, aby výrobcovia zlepšili bezpečnosť produktov s digitálnymi prvkami od fázy návrhu a vývoja aj počas celého životného cyklu; ii) zaistiť koherentný rámec kybernetickej bezpečnosti, ktorý uľahčí výrobcom hardvéru a softvéru dodržiavať predpisy; iii) zvýšiť transparentnosť bezpečnostných vlastností produktov s digitálnymi prvkami a iv) umožniť podnikom a spotrebiteľom bezpečné používanie produktov s digitálnymi prvkami.

Z výrazného cezhraničného charakteru kybernetickej bezpečnosti a rastúceho počtu incidentov s účinkami, ktoré presahujú hranice, odvetvia a produkty, vyplýva, že ciele nemožno účinne dosiahnuť len na úrovni členských štátov. Vzhľadom na globálny charakter trhov s produktmi s digitálnymi prvkami čelia členské štáty na svojom území rovnakým rizikám v prípade toho istého produktu s digitálnymi prvkami. Vznikajúci fragmentovaný rámec potenciálne odlišných vnútroštátnych pravidiel prináša riziká, ktoré narúšajú otvorený a konkurencieschopný jednotný trh s produktmi s digitálnymi prvkami. Potrebné je preto spoločné opatrenie na úrovni EÚ, aby sa zvýšila úroveň dôvery medzi používateľmi a atraktívnosť produktov EÚ s digitálnymi prvkami. Prospelo by aj vnútornému trhu, a to tým, že by sa zabezpečila právna istota a dosiahli rovnaké podmienky pre predajcov produktov s digitálnymi prvkami, ako sa zdôrazňuje aj v záverečnej správe z Konferencie o budúcnosti Európy, v ktorej občania vyzývajú na silnejšiu úlohu EÚ v boji proti kybernetickobezpečnostným hrozbám.

- **Súlad s existujúcimi ustanoveniami v tejto oblasti politiky**

Rámec EÚ obsahuje viaceré horizontálne právne predpisy, ktoré sa týkajú určitých aspektov spojených s kybernetickou bezpečnosťou z rôznych hľadísk (produktov, služieb krízového manažmentu a trestnej činnosti). V roku 2013 nadobudla účinnosť smernica o útokoch na informačné systémy[1], ktorou sa harmonizuje kriminalizácia a sankcie za viaceré trestné činy namierené proti informačným systémom. V auguste 2016 nadobudla účinnosť smernica (EÚ) 2016/1148 o bezpečnosti sietí a informačných systémov (smernica NIS)[2] ako prvý právny predpis EÚ o kybernetickej bezpečnosti. Výsledkom jej revízie je smernica [smernica XXX/XXXX (NIS2)], ktorou sa zvyšuje spoločná úroveň ambícií EÚ. V roku 2019 nadobudol účinnosť akt EÚ o kybernetickej bezpečnosti[3], ktorého cieľom je zvýšenie bezpečnosti produktov IKT, služieb IKT a procesov IKT zavedením dobrovoľného európskeho rámca certifikácie kybernetickej bezpečnosti[4].

Kybernetická bezpečnosť celého dodávateľského reťazca je zaistená, iba ak sú kyberneticky bezpečné všetky jeho zložky. Uvedené právne predpisy EÚ však majú v tomto ohľade značné medzery, pretože sa nevzťahujú na povinné požiadavky na bezpečnosť produktov s digitálnymi prvkami.

Hoci sa navrhovaný akt o kybernetickej odolnosti vzťahuje na produkty s digitálnymi prvkami uvádzané na trh, smernica [smernica XXX/XXXX (NIS2)] sa zameriava na zabezpečenie vysokej úrovne kybernetickej bezpečnosti služieb, ktoré poskytujú základné a dôležité subjekty. V smernici [smernica XXX/XXXX (NIS2)] sa od členských štátov vyžaduje zaistiť, aby základné a dôležité subjekty v rozsahu pôsobnosti, ako sú poskytovatelia zdravotnej starostlivosti alebo cloudových služieb a subjekty verejnej správy, prijali vhodné

---

1 Smernica Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV (Ú. v. EÚ L 218, 14.8.2013, s. 8 – 14).

2 Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194/1, 19.7.2016, s. 1).

3 Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7.6.2019, s. 15).

4 Akt o kybernetickej bezpečnosti umožňuje vyvíjať účelové certifikačné systémy. Každý systém obsahuje odkazy na príslušné normy, technické špecifikácie alebo iné požiadavky kybernetickej bezpečnosti vymedzené v systéme. Rozhodnutie vyvíjať certifikáciu kybernetickej bezpečnosti je rozhodnutie založené na rizikách.

a primerané technické, operatívne a organizačné kybernetickobezpečnostné opatrenia. Súčasťou toho okrem iného je požiadavka zaistiť bezpečnosť pri nadobúdaní, vývoji a údržbe sieťových a informačných systémov vrátane riešenia a zverejnenia zraniteľností. V smernici [smernica XXX/XXXX (NIS2)] sa od Komisie vyžaduje, aby do 21 mesiacov odo dňa nadobudnutia účinnosti tejto smernice prijala vykonávacie akty, v ktorých stanoví technické a metodické požiadavky na uvedené opatrenia pre určité druhy subjektov, ako sú poskytovatelia služieb cloud computingu. Pre všetky ostatné subjekty môže Komisia prijať vykonávací akt, v ktorom stanoví technické a metodické požiadavky, ako aj odvetvové požiadavky. Týmto rámcom sa zabezpečí, aby sa technické špecifikácie a opatrenia podobné základným požiadavkám kybernetickej bezpečnosti aktu o kybernetickej odolnosti takisto uskutočňovali pri návrhu, vývoji a riešení zraniteľností softvéru poskytovaného formou služby (softvér ako služba). Mohol by byť napríklad prostriedkom na zaistenie vysokej úrovne kybernetickej bezpečnosti v prípadoch, ako sú systémy elektronických zdravotných záznamov, a to aj vtedy, ak sa dodávajú formou softvéru ako služba alebo ak sa vyvíjajú v rámci zdravotníckych inštitúcií (interne) v súlade s navrhovaným [nariadením o európskom priestore pre zdravotné údaje].

- **Súlad s ostatnými politikami Únie**

Ako sa stanovuje v oznámení „Formovanie digitálnej budúcnosti Európy“[5], je pre EÚ kľúčové využívať všetky výhody digitálneho veku a posilniť svoju priemyselnú a inovačnú kapacitu v rámci bezpečných a etických hraníc. V rámci Európskej dátovej stratégie sa stanovujú štyri piliere – ochrana údajov, základné práva, bezpečnosť a kybernetická bezpečnosť – ktoré sú základnými predpokladmi pre spoločnosť posilnenú využívaním údajov.

Súčasný rámec EÚ[6] vzťahujúci sa na produkty, ktoré môžu mať aj digitálne prvky, pozostáva z viacerých právnych predpisov vrátane právnych predpisov EÚ o konkrétnych produktoch, ktoré sa týkajú bezpečnostných aspektov, a zo všeobecných právnych predpisov o zodpovednosti za výrobok. Návrh je v súlade so súčasným regulačným rámcom EÚ týkajúcim sa produktov, ako aj s poslednými legislatívnymi návrhmi Komisie, napr. s návrhom nariadenia [nariadenie o umelej inteligencii][7].

Navrhované nariadenie by sa uplatňovalo na všetky rádiové zariadenia v rozsahu pôsobnosti delegovaného nariadenia Komisie (EÚ) 2022/30. Požiadavky stanovené v tomto nariadení navyše obsahujú všetky prvky základných požiadaviek uvedených v článku 3 ods. 3 písm. d), e) a f) smernice 2014/53/EÚ vrátane hlavných prvkov stanovených vo [vykonávacom rozhodnutí Komisie XXX/2022 o mandáte na tvorbu normy pre európske normalizačné organizácie] vydanom na základe uvedeného delegovaného nariadenia. S cieľom vyhnúť sa prekrývaniu právnych predpisov sa predpokladá, že Komisia zruší alebo zmení delegované nariadenie, pokiaľ ide o rádiové zariadenia, na ktoré sa vzťahuje navrhované nariadenie, aby sa toto na ne vzťahovalo, keď bude uplatniteľné.

---

5 Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov – Formovanie digitálnej budúcnosti Európy, COM(2020) 67 final z 19. februára 2020.

6 Hlavne právne predpisy nového legislatívneho rámca.

7 Návrh nariadenia Európskeho parlamentu a Rady, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie (akt o umelej inteligencii) a mení niektoré legislatívne akty Únie, COM(2021) 206 final z 21. apríla 2021.

Okrem toho, aby sa zabránilo duplicite prác, predpokladá sa, že Komisia a európske normalizačné organizácie zohľadnia normalizačné práce vykonané v súvislosti s vykonávacím rozhodnutím Komisie C(2022) 5637 o mandáte na tvorbu normy týkajúcom sa delegovaného nariadenia 2022/30, ktorým sa dopĺňa smernica o rádiových zariadeniach, pri príprave a vypracúvaní harmonizovaných noriem na uľahčenie vykonávania tohto nariadenia.

2. PRÁVNY ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

• Právny základ

Právnym základom tohto návrhu je článok 114 Zmluvy o fungovaní Európskej únie (ďalej len „ZFEÚ“), v ktorom sa stanovuje prijímanie opatrení na zabezpečenie vytvorenia a fungovania vnútorného trhu. Účelom návrhu je harmonizovať požiadavky kybernetickej bezpečnosti na produkty s digitálnymi prvkami vo všetkých členských štátoch a odstrániť prekážky voľného pohybu tovaru.

Článok 114 ZFEÚ možno použiť ako právny základ na predchádzanie výskytu týchto prekážok v dôsledku odlišných vnútroštátnych zákonov a prístupov týkajúcich sa spôsobu riešenia právnej neistoty a medzier v existujúcich právnych rámcoch[8]. Súdny dvor navyše uznal, že uplatňovanie rozdielnych technických požiadaviek by mohlo byť platným dôvodom na uplatnenie článku 114 ZFEÚ[9].

Súčasný právny rámec EÚ uplatniteľný na produkty s digitálnymi prvkami je založený na článku 114 ZFEÚ a obsahuje viacero právnych predpisov vrátane predpisov o konkrétnych produktoch a bezpečnostných aspektoch, alebo všeobecných právnych predpisov o zodpovednosti za výrobok. Pokrýva však iba niektoré aspekty spojené s kybernetickou bezpečnosťou hmotných digitálnych produktov a prípadne so softvérom zabudovaným v týchto produktoch. Členské štáty začínajú na vnútroštátnej úrovni prijímať vnútroštátne opatrenia, ktorými sa od predajcov digitálnych produktov vyžaduje posilnenie ich kybernetickej bezpečnosti[10]. Kybernetická bezpečnosť digitálnych produktov má zároveň obzvlášť výrazný cezhraničný rozmer, keďže produkty vyrobené v jednej krajine používajú často organizácie a spotrebitelia na celom vnútornom trhu. Incidenty, ktoré sa spočiatku týkajú jedného subjektu alebo členského štátu sa často za pár minút rozšíria v celých organizáciách, odvetviach a vo viacerých členských štátoch.

Rôzne akty a iniciatívy prijaté dosiaľ na úrovni EÚ a na vnútroštátnych úrovniach riešia identifikované problémy iba čiastočne a spôsobujú riziko vytvorenia zlepenca právnych predpisov na vnútornom trhu, ktorý zvýši právnu neistotu predajcov aj používateľov týchto produktov a pridá zbytočnú záťaž spoločnostiam pri plnení mnohých požiadaviek v súvislosti s podobnými druhmi produktov.

Navrhovaným nariadením by sa harmonizovalo a zjednodušilo regulačné prostredie EÚ zavedením požiadaviek kybernetickej bezpečnosti produktov s digitálnymi prvkami a zabránilo by sa prekrývaniu požiadaviek vyplývajúcich z rôznych právnych predpisov. Vytvorila by sa tak väčšia právna istota pre hospodárske subjekty a používateľov v celej Únii,

---

[8] Rozsudok Súdneho dvora EÚ (veľká komora) z 3. decembra 2019, Česká republika/Európsky parlament a Rada Európskej únie, vec C-482/17, bod 35.

[9] Rozsudok Súdneho dvora EÚ (veľká komora) z 2. mája 2006, Spojené kráľovstvo Veľkej Británie a Severného Írska/Európsky parlament a Rada Európskej únie, vec C-217/04, body 62 – 63.

[10] Napríklad v roku 2019 vytvorilo Fínsko systém označovania internetu vecí, napr. inteligentných televízorov, telefónov a hračiek na základe noriem ETSI. Nemecko nedávno zaviedlo značku bezpečnosti spotrebiteľa pre širokopásmové smerovače, inteligentné televízory, kamery, reproduktory, hračky a upratovacie a záhradnícke roboty.

ako aj lepšia harmonizácia vnútorného trhu vytvorením životaschopnejších podmienok pre hospodárske subjekty, ktoré plánujú vstup na vnútorný trh EÚ.

- **Subsidiarita (v prípade inej ako výlučnej právomoci)**

Z výrazného cezhraničného charakteru kybernetickej bezpečnosti všeobecne a rastúceho počtu rizík a incidentov s účinkami, ktoré presahujú hranice, odvetvia a produkty, vyplýva, že ciele nemožno účinne dosiahnuť len na úrovni členských štátov. Vnútroštátne prístupy k riešeniu problémov a najmä prístupy, ktorými sa zavádzajú povinné požiadavky, vytvoria ďalšiu právnu neistotu a právne prekážky. Spoločnostiam by sa mohlo zabrániť v plynulom rozširovaní do iných členských štátov, a tak pripraviť používateľov o prospech z ich produktov.

Potrebné je preto spoločné opatrenie na úrovni EÚ, aby sa vytvorila vysoká úroveň dôvery medzi používateľmi, ktorá zvýši atraktívnosť produktov EÚ s digitálnymi prvkami. Prospelo by aj digitálnemu jednotnému trhu a vnútornému trhu všeobecne a to tým, že by sa zabezpečila právna istota a dosiahli rovnaké podmienky pre výrobcov produktov s digitálnymi prvkami.

Rada v záveroch o vývoji stavu kybernetickej bezpečnosti Európskej únie z 23. mája 2022 napokon vyzýva Komisiu, aby do konca roka 2022 navrhla spoločné požiadavky kybernetickej bezpečnosti pre pripájané zariadenia.

- **Proporcionalita**

Pokiaľ ide o proporcionalitu navrhovaného nariadenia, opatrenia v rámci uvažovaných možností politiky by neprekročili rámec nevyhnutný na dosiahnutie všeobecného cieľa a špecifických cieľov a nespôsobili by neúmerné náklady. Presnejšie by sa zvažovaným zásahom zabezpečilo, aby produkty s digitálnymi prvkami boli zabezpečené počas ich celého životného cyklu a úmerne k očakávaným rizikám prostredníctvom cielene zameraných a technologicky neutrálnych požiadaviek, ktoré zostávajú odôvodnené a všeobecne zodpovedajú záujmu zúčastnených subjektov.

Základné požiadavky kybernetickej bezpečnosti v návrhu nadväzujú na všeobecne používané normy a proces normalizácie, ktorým sa bude postupovať, by zohľadnil technické špecifiká týchto produktov. To znamená, že ak to bude potrebné vzhľadom na danú úroveň rizika, bezpečnostné kontroly by sa prispôsobili. V predpokladaných horizontálnych pravidlách by sa ďalej navrhlo posudzovanie treťou stranou len kritických produktov. Toto by sa týkalo len úzkeho podielu produktov s digitálnymi prvkami na trhu. Dosah na MSP by závisel od ich prítomnosti na trhu s týmito konkrétnymi kategóriami produktov.

Pokiaľ ide o proporcionalitu nákladov na posudzovanie zhody, notifikované osoby, ktoré vykonávajú posudzovanie treťou stranou, by pri stanovení svojich poplatkov zohľadňovali veľkosť podniku. Poskytlo by sa aj primerané prechodné obdobie 24 mesiacov na prípravu vykonávania, ktorým by sa príslušným trhom poskytol čas na prípravu, pričom by sa stanovilo jasné smerovanie investícií na výskum a vývoj. Akékoľvek náklady na dodržiavanie predpisov pre podniky by sa vyvážili prínosmi vyššej úrovne bezpečnosti produktov s digitálnymi prvkami a v konečnom dôsledku zvýšením dôvery používateľov k týmto produktom.

- **Výber nástroja**

Regulačný zásah by prinieslo prijatie nariadenia a nie smernice. Je to preto, že pri tomto konkrétnom druhu právneho predpisu, ktorý sa týka produktu, by sa nariadením účinnejšie riešili identifikované problémy a dosiahli formulované ciele, keďže ide o zásah, ktorý je podmienený uvedením veľmi širokej kategórie produktov na vnútorný trh. V prípade použitia

smernice na takýto zásah by proces transpozície mohol ponechať príliš veľký priestor na vlastné úvahy na vnútroštátnej úrovni, čo by mohlo viesť k nejednotnosti určitých základných požiadaviek kybernetickej bezpečnosti, právnej neistote, ďalšej fragmentácii alebo dokonca k diskriminačným situáciám naprieč hranicami, a to aj s väčším prihliadaním na skutočnosť, že produkty, na ktoré sa vzťahuje, by mohli mať viacnásobný účel alebo viac použití, a že výrobcovia môžu vyrábať viac kategórií takýchto produktov.

3. VÝSLEDKY HODNOTENÍ *EX POST*, KONZULTÁCIÍ SO ZAINTERESOVANÝMI STRANAMI A POSÚDENÍ VPLYVU

• Konzultácie so zainteresovanými stranami

Komisia viedla konzultácie so širokým spektrom zainteresovaných strán. Členské štáty a zainteresované strany boli vyzvané, aby sa zúčastnili na verejnej konzultácii a na prieskumoch a seminároch organizovaných v kontexte štúdie, ktorú uskutočnilo konzorcium podporujúce prípravné práce Komisie na posúdenie vplyvu, ktoré tvorili: Wavestone, Centrum pre európske politické štúdie (CEPS) a ICF. Zainteresovanými stranami, ktoré sa na konzultácii zúčastnili, boli národné orgány dohľadu nad trhom, orgány Únie, ktoré sa zaoberajú kybernetickou bezpečnosťou, výrobcovia hardvéru a softvéru, dovozcovia a distribútori hardvéru a softvéru, priemyselné združenia, organizácie spotrebiteľov a používateľov produktov s digitálnymi prvkami a občania, výskumní pracovníci a členovia akademickej obce, notifikované osoby a akreditačné orgány a odborníci z oblasti kybernetickej bezpečnosti.

Konzultácie zahŕňali:

- prvú štúdiu, uskutočnenú konzorciom zloženým z ICF, Wavestone, Carsa a CEPS, ktorá bola uverejnená v decembri 2021[11]. V štúdii sa identifikovali viaceré zlyhania trhu a posúdili možné regulačné zásahy.
- Verejná konzultácia, ktorá bola zameraná na občanov, zainteresované strany a odborníkov v oblasti kybernetickej bezpečnosti. Predložených bolo 176 odpovedí. Prispeli k zbierke rozmanitých stanovísk a skúseností zo všetkých skupín zainteresovaných strán.
- Na seminároch organizovaných v rámci štúdie na podporu prípravných prác Komisie v súvislosti s aktom o kybernetickej odolnosti sa zhromaždilo približne 100 zástupcov zo všetkých 27 členských štátov, ktorí zastupovali rôzne zainteresované strany.
- Uskutočnili sa rozhovory s expertmi so zámerom lepšie pochopiť súčasné problémy kybernetickej bezpečnosti vo vzťahu k produktom s digitálnymi prvkami a prerokovať možnosti politiky, pokiaľ ide o potenciálny regulačný zásah.
- Dvojstranné diskusie sa uskutočnili s vnútroštátnymi orgánmi pre kybernetickú bezpečnosť, súkromným sektorom a spotrebiteľskými organizáciami.
- Cielený program bol venovaný kľúčovým zainteresovaným MSP.

[11] *Study on the need of Cybersecurity requirements for ICT products* (Štúdia o potrebe požiadaviek kybernetickej bezpečnosti produktov IKT) – č. 2020-0715, záverečná správa štúdie, k dispozícii na adrese https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products.

- **Získavanie a využívanie expertízy**

Cieľom konzultačných činností bolo získať vstupné informácie o piatich hlavných kritériách hodnotenia na základe usmernení EÚ k lepšej právnej regulácii (účinnosť, efektívnosť, relevantnosť, súdržnosť, pridaná hodnota EÚ), ako aj o potenciálnych účinkoch možných alternatív. Dodávateľ sa nielen obrátil na zainteresované strany, ktoré by boli priamo ovplyvnené navrhovaným nariadením, ale aj konzultoval s celým radom expertov v oblasti kybernetickej bezpečnosti.

- **Posúdenie vplyvu**

Komisia vypracovala posúdenie vplyvu tohto návrhu, ktoré preskúmal výbor Komisie pre kontrolu regulácie. Rokovanie s výborom pre kontrolu regulácie sa uskutočnilo 6. júla 2022, po ktorom nasledovalo priaznivé stanovisko. Posúdenie vplyvu sa upravilo, aby zohľadňovalo odporúčania a pripomienky výboru pre kontrolu regulácie.

Komisia preskúmala rôzne možnosti politiky na dosiahnutie všeobecného cieľa tohto návrhu:

- Tzv. „soft law“ prístup a dobrovoľné opatrenia (možnosť 1): Pri tejto možnosti by neexistoval žiadny povinný regulačný zásah. Namiesto neho by Komisia vydala oznámenia, usmernenia, odporúčania a možno kódexy správania na podnietenie dobrovoľných opatrení. Naďalej by sa vyvíjali vnútroštátne programy, dobrovoľné alebo povinné, s cieľom kompenzovať nedostatok horizontálnych pravidiel EÚ.
- Regulačný zásah *ad hoc* v prospech kybernetickej bezpečnosti hmotných produktov s digitálnymi prvkami a príslušného zabudovaného softvéru (možnosť 2): Táto možnosť by bola regulačným zásahom *ad hoc* zameraným na konkrétny produkt, ktorý by bol obmedzený na doplnenie a/alebo zmenu požiadaviek kybernetickej bezpečnosti v právnych predpisoch, ktoré už existujú, alebo na zavedenie nových právnych predpisov vzhľadom na novovznikajúce riziká prípadne vrátane nezabudovaného softvéru.

Možnosti 3 a 4 sú horizontálne regulačné zásahy s rôznym rozsahom pôsobnosti, väčšinou podľa nového legislatívneho rámca. Týmto rámcom sa stanovujú základné požiadavky ako podmienka uvedenia určitých produktov na vnútorný trh. Nový legislatívny rámec spravidla počíta aj s postupom posudzovania zhody, procesom vykonávaným výrobcom, ktorého cieľom je preukázať, či sú splnené špecifikované požiadavky týkajúce sa produktu.

- Zmiešaný prístup, ktorého súčasťou sú horizontálne kogentné právne normy vzťahujúce sa kybernetickú bezpečnosť hmotných produktov s digitálnymi prvkami a príslušný zabudovaný softvér a stupňovitý prístup v prípade nezabudovaného softvéru (možnosť 3): Táto možnosť by znamenala reguláciu, ktorou by sa zaviedli horizontálne požiadavky kybernetickej bezpečnosti pre všetky hmotné produkty s digitálnymi prvkami a softvér zabudovaný v nich ako podmienka uvedenia na trh, a obsahovala by dve čiastkové možnosti s povinným posúdením treťou stranou (3i) a bez neho (3ii). Nezabudovaný softvér by sa nereguloval.
- Horizontálny regulačný zásah, ktorým sa zavádzajú požiadavky kybernetickej bezpečnosti pre rozsiahlu skupinu hmotných a nehmotných produktov s digitálnymi prvkami, vrátane nezabudovaného softvéru (možnosť 4): Táto možnosť je podobná možnosti 3, okrem rozsahu pôsobnosti. Možnosť 4 by zahŕňala nezabudovaný softvér [s dvoma čiastkovými možnosťami, ktoré by sa

týkali buď iba kritického softvéru (4a), alebo všetkého softvéru (4b)] v rozsahu pôsobnosti potenciálnej regulácie. Pri každej čiastkovej možnosti by sa zvažovali rovnaké čiastkové možnosti týkajúce sa posudzovania zhody ako pri možnosti 3.

Možnosť 4 (s čiastkovými možnosťami vzťahujúcimi sa na všetok softvér a zahŕňajúcimi povinné posúdenie kritických produktov treťou stranou) sa ukázala ako uprednostňovaná možnosť na základe posúdenia účinnosti vzhľadom na špecifické ciele a efektívnosti nákladov v porovnaní s prínosmi. Touto možnosťou by sa zabezpečilo stanovenie špecifických horizontálnych požiadaviek kybernetickej bezpečnosti pre všetky produkty s digitálnymi prvkami uvádzanými na vnútorný trh alebo sprístupnenými na ňom, pričom by bola jedinou možnosťou, ktorá by sa vzťahovala na celý digitálny dodávateľský reťazec. Takýto regulačný zásah by pokryl aj nezabudovaný softvér, ktorý je často vystavený zraniteľnostiam, a zaistil by tak súdržný prístup ku všetkým produktom s digitálnymi prvkami s jasným rozdelením zodpovednosti rôznych hospodárskych subjektov.

Táto možnosť politiky prináša aj pridanú hodnotu zahrnutím aspektov povinnej starostlivosti a celého životného cyklu po uvedení produktov s digitálnymi prvkami na trh s cieľom okrem iného zabezpečiť primerané informácie o bezpečnostnej podpore a poskytovaní aktualizácií zabezpečenia. Táto možnosť politiky by bola aj najúčinnejším doplnkom nedávnej revízie rámca NIS, a to zabezpečením predpokladov posilnenej bezpečnosti dodávateľského reťazca.

Uprednostňovaná možnosť by priniesla značné výhody rôznym zainteresovaným stranám. V prípade podnikov by sa zabránilo rozdielnym bezpečnostným pravidlám pre produkty s digitálnymi prvkami a znížili by sa náklady na dodržiavanie príslušných právnych predpisov v oblasti kybernetickej bezpečnosti. Znížil by sa počet kybernetických bezpečnostných incidentov, náklady na ich riešenie a poškodenie dobrého mena. V prípade celej EÚ sa odhaduje, že iniciatíva by mohla viesť k zníženiu nákladov, ktoré z incidentov vznikajú podnikom približne o 180 až 290 miliárd EUR ročne. Viedla by k zvýšenému obratu vďaka využívaniu produktov s digitálnymi prvkami. Zlepšila by sa celková dobrá povesť spoločností, čo by podnietilo zvýšenie dopytu aj mimo EÚ. Uprednostňovaná možnosť by pre používateľov zvýšila transparentnosť bezpečnostných vlastností a uľahčila by používanie produktov s digitálnymi prvkami. Aj spotrebitelia a občania by mali prínos z lepšej ochrany svojich práv, ako je ochrana súkromia a ochrana osobných údajov.

Pri požiadavke na hodnotenie účinnosti politických zásahov sa respondenti v rámci verejnej konzultácie zhodli na tom, že možnosť 4 by bola najúčinnejším opatrením (4,08 na stupnici od 1 do 5). Patria k nim spotrebiteľské organizácie (5,00), respondenti, ktorí sa identifikovali ako používatelia (4,22), notifikované osoby (4,17), orgány dohľadu nad trhom (5,00) a výrobcovia produktov s digitálnymi prvkami (3,85) vrátane výrobcov malej a strednej veľkosti (4,05).

- **Vhodnosť právnych predpisov a ich zjednodušenie**

V tomto návrhu sa stanovujú požiadavky, ktoré sa budú uplatňovať na výrobcov softvéru a hardvéru. Je potrebné zabezpečiť právnu istotu a vyhnúť sa ďalšej fragmentácii trhu požiadavkami kybernetickej bezpečnosti týkajúcimi sa produktov na vnútornom trhu, čo sa preukázalo širokou podporou rôznych zainteresovaných strán v prípade horizontálneho zásahu. Návrhom sa bude minimalizovať regulačné zaťaženie výrobcov spôsobené viacerými aktmi o bezpečnosti výrobkov. Zosúladenie s novým legislatívnym rámcom znamená lepšie fungovanie zásahu a jeho presadzovanie. Návrhom sa zjednodušuje proces postupov súvisiacich s ochrannou doložkou zahrnutím výrobcov a členských štátov pred notifikáciou Komisie. Veľká časť výrobcov v rozsahu pôsobnosti návrhu sa už podrobne oboznámila

s fungovaním nového legislatívneho rámca, čo prispeje k jeho pochopeniu a vykonávaniu. V prípade spotrebiteľov a spoločností návrh podporí dôveru k produktom s digitálnymi prvkami.

- **Základné práva**

Očakáva sa, že všetky možnosti politiky do určitej miery posilnia ochranu základných práv a slobôd, akými sú súkromie, ochrana osobných údajov, sloboda podnikania a ochrana majetku alebo osobnej dôstojnosti a integrity. Najmä uprednostňovaná možnosť politiky 4 pozostávajúca z horizontálnych regulačných zásahov a široký rozsah pôsobnosti politiky by boli v tomto ohľade najúčinnejšie, keďže s vyššou pravdepodobnosťou napomôžu zníženiu počtu a závažnosti incidentov vrátane porušení ochrany osobných údajov. Takisto by sa ňou zvýšila právna istota a dosiahli by sa rovnaké podmienky pre hospodárske subjekty, celkovo by sa zvýšila dôvera medzi používateľmi a atraktívnosť produktov s digitálnymi prvkami z EÚ a ochránil by sa tak majetok a zlepšili by sa podmienky hospodárskych subjektov na podnikanie.

Horizontálne požiadavky kybernetickej bezpečnosti by prispeli k bezpečnosti osobných údajov ochranou dôvernosti, integrity a dostupnosti informácií v produktoch s digitálnymi prvkami. Dodržiavanie uvedených požiadaviek uľahčí dodržiavanie požiadaviek bezpečnosti spracúvania osobných údajov podľa všeobecného nariadenia o ochrane údajov (EÚ) 2016/679[12]. Návrhom by sa rozšírila transparentnosť a informácie pre používateľov vrátane tých, ktorí sú menej zruční v oblasti kybernetickej bezpečnosti. Používatelia by takisto boli lepšie informovaní o rizikách, možnostiach a obmedzeniach produktov s digitálnymi prvkami, vďaka čomu by lepšie dokázali prijímať potrebné preventívne a zmierňujúce opatrenia na zníženie zvyškových rizík.

4. VPLYV NA ROZPOČET

Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA) na splnenie úloh pridelených týmto nariadením bude musieť prerozdeliť zdroje v rozsahu približne 4,5 ekvivalentu plného pracovného času. Komisia bude musieť vyčleniť sedem ekvivalentov plného pracovného času na splnenie svojich povinností týkajúcich sa presadzovania práva podľa tohto nariadenia.

Podrobný prehľad súvisiacich nákladov je uvedený vo finančnom výkaze, ktorý je pripojený k tomuto návrhu.

5. OSTATNÉ PRVKY

- **Plány vykonávania, spôsob monitorovania, hodnotenia a predkladania správ**

Komisia bude monitorovať vykonávanie a uplatňovanie týchto nových ustanovení, ako aj dosahovanie súladu s nimi, na účely posúdenia ich účinnosti. V nariadení sa bude vyžadovať hodnotenie a preskúmanie uskutočňované Komisiou, ako aj predloženie verejnej správy o nich Európskemu parlamentu a Rade do 36 mesiacov odo dňa začatia uplatňovania a potom každé štyri roky.

- **Podrobné vysvetlenie osobitných ustanovení návrhu**

Všeobecné ustanovenia (kapitola I)

[12] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).

V tomto návrhu nariadenia sa stanovujú a) pravidlá uvádzania produktov s digitálnymi prvkami na trh s cieľom zaistiť kybernetickú bezpečnosť takýchto produktov; b) základné požiadavky na návrh, vývoj a výrobu produktov s digitálnymi prvkami a povinnosti hospodárskych subjektov vo vzťahu k týmto produktom vzhľadom na kybernetickú bezpečnosť; c) základné požiadavky na procesy riešenia zraniteľností zavedené výrobcami s cieľom zaistiť kybernetickú bezpečnosť produktov s digitálnymi prvkami počas celého životného cyklu a povinnosti hospodárskych subjektov vo vzťahu k týmto procesom; d) pravidlá dohľadu nad trhom a presadzovanie uvedených pravidiel a požiadaviek.

Navrhované nariadenie sa bude uplatňovať na všetky produkty s digitálnymi prvkami, ktorých zamýšľané a odôvodnene predvídateľné použitie zahŕňa priame alebo nepriame logické alebo fyzické dátové pripojenie k zariadeniu alebo sieti.

Navrhované nariadenie sa nebude uplatňovať na produkty s digitálnymi prvkami v rozsahu pôsobnosti nariadenia (EÚ) 2017/745 [zdravotnícke pomôcky určené pre ľudí a príslušenstvo takýchto pomôcok] a nariadenia (EÚ) 2017/746 [diagnostické zdravotnícke pomôcky *in vitro* určené pre ľudí a príslušenstvo takýchto pomôcok], keďže obe nariadenia obsahujú požiadavky týkajúce sa zariadení vrátane softvéru a všeobecné povinnosti výrobcov, ktoré sa vzťahujú na celý životný cyklus produktov, ako aj na postupy posudzovania zhody. Toto nariadenie sa nebude uplatňovať na produkty s digitálnymi prvkami, ktoré boli certifikované v súlade s nariadením (EÚ) 2018/1139 [vysoká a jednotná úroveň bezpečnosti civilného letectva], ani na produkty, na ktoré sa uplatňuje nariadenie (EÚ) 2019/2144 [o požiadavkách na typové schvaľovanie motorových vozidiel a ich prípojných vozidiel a systémov, komponentov a samostatných technických jednotiek určených pre tieto vozidlá].

Kritické produkty s digitálnymi prvkami podliehajú osobitným postupom posudzovania zhody a rozdeľujú sa do triedy I a triedy II, ako sa uvádza v prílohe III, podľa ich úrovne kybernetickobezpečnostného rizika, pričom trieda II predstavuje vyššie riziko. Produkt s digitálnymi prvkami sa považuje za kritický a preto zaradený do prílohy III so zreteľom na vplyv potenciálnych zraniteľností, ktoré produkt s digitálnymi prvkami má z hľadiska kybernetickej bezpečnosti. Pri určovaní kybernetickobezpečnostného rizika sa okrem iného zohľadňuje funkčnosť produktu s digitálnymi prvkami a jeho zamýšľané použitie z hľadiska kybernetickej bezpečnosti v citlivých prostrediach, napríklad v priemyselnom prostredí.

Komisia je takisto splnomocnená prijímať delegované akty s cieľom doplniť toto nariadenie o špecifikovanie kategórií vysokokritických produktov s digitálnymi prvkami, pre ktoré sú výrobcovia povinní získať európsky certifikát kybernetickej bezpečnosti v rámci európskeho systému certifikácie kybernetickej bezpečnosti na preukázanie zhody so základnými požiadavkami stanovenými v prílohe I alebo s ich časťami. Pri určovaní týchto kategórií vysokokritických produktov s digitálnymi prvkami Komisia zohľadňuje úroveň kybernetickobezpečnostného rizika týkajúceho sa kategórie produktov s digitálnymi prvkami z hľadiska jedného kritéria alebo viacerých kritérií zvažovaných na účel uvedenia kritických produktov s digitálnymi prvkami v prílohe III, ako aj vzhľadom na posúdenie toho, či uvedenú kategóriu produktov používajú alebo sa na ňu spoliehajú základné subjekty druhu uvedeného v prílohe [príloha I] k smernici [smernica XXX/XXXX (NIS2)] alebo bude mať v budúcnosti význam pre činnosti týchto subjektov, alebo či kategória bude relevantná z hľadiska odolnosti celého dodávateľského reťazca produktov s digitálnymi prvkami proti rušivým udalostiam.

Povinnosti hospodárskych subjektov (kapitola II)

Návrh obsahuje povinnosti výrobcov, dovozcov a distribútorov vychádzajúce z referenčných ustanovení uvedených v rozhodnutí 768/2008/ES. Základné požiadavky a povinnosti súvisiace s kybernetickou bezpečnosťou vyžadujú, aby sa všetky produkty s digitálnymi

prvkami sprístupnili na trhu len vtedy, ak pri riadnom dodaní, náležitej inštalácii, údržbe a používaní na zamýšľaný účel alebo za podmienok, ktoré možno odôvodnene predpokladať, spĺňajú základné požiadavky kybernetickej bezpečnosti stanovené v tomto nariadení.

Podľa týchto základných požiadaviek a povinností by výrobcovia museli zohľadňovať kybernetickú bezpečnosť pri návrhu, vývoji a výrobe produktov s digitálnymi prvkami, venovať náležitú starostlivosť bezpečnostným aspektom pri návrhu a vývoji svojich produktov, správať sa transparentne v prípade aspektoch kybernetickej bezpečnosti, s ktorými je potrebné oboznámiť zákazníkov, primeraným spôsobom zaistiť bezpečnostnú podporu (aktualizácie) a dodržiavať požiadavky súvisiace s riešením zraniteľností.

Povinnosti by sa stanovili hospodárskym subjektom, počínajúc od výrobcov až po distribútorov a dovozcov v súvislosti s uvádzaním produktov s digitálnymi prvkami na trh, ktoré by boli primerané ich úlohe a zodpovednostiam v dodávateľskom reťazci.

Zhoda produktu s digitálnymi prvkami (kapitola III)

Produkt s digitálnymi prvkami, ktorý je v zhode s harmonizovanými normami alebo s ich časťami, na ktoré boli odkazy uverejnené v *Úradnom vestníku Európskej únie*, sa považuje za produkt spĺňajúci základné požiadavky tohto navrhovaného nariadenia. Ak harmonizované normy neexistujú alebo sú nedostatočné, alebo ak nastali v procese normalizácie zbytočné prieťahy, alebo ak európske normalizačné organizácie nevyhoveli žiadosti Komisie, Komisia môže prostredníctvom vykonávacích aktov prijať spoločné špecifikácie.

Navyše sa predpokladá, že produkty s digitálnymi prvkami, ktoré boli certifikované alebo pre ktoré bolo vydané EÚ vyhlásenie o zhode alebo certifikát v rámci európskeho systému certifikácie kybernetickej bezpečnosti podľa nariadenia (EÚ) 2019/881, a pre ktoré Komisia prostredníctvom vykonávacieho aktu špecifikovala, že môže stanoviť predpoklad zhody pre toto nariadenie, sú v súlade so základnými požiadavkami tohto nariadenia alebo jeho častí, pokiaľ sa EÚ vyhlásenie o zhode alebo certifikát kybernetickej bezpečnosti alebo ich časti vzťahujú na tieto požiadavky.

V záujme vyhnutia sa prípadnému neprimeranému administratívnemu zaťaženiu výrobcov by Komisia mala navyše špecifikovať, či certifikát kybernetickej bezpečnosti vydaný v rámci takéhoto európskeho systému certifikácie kybernetickej bezpečnosti ruší povinnosť výrobcov vykonať posúdenie zhody treťou stranou, ako to stanovuje toto nariadenie pri zodpovedajúcich požiadavkách.

Výrobca vykoná posúdenie zhody produktu s digitálnymi prvkami a procesov riešenia zraniteľností, ktoré zaviedol, aby preukázal zhodu so základnými požiadavkami stanovenými v prílohe I jedným z postupov, ktoré sú uvedené v prílohe VI. Výrobcovia kritických produktov tried I a II použijú príslušné moduly potrebné na dosiahnutie súladu. Výrobcovia kritického produktu triedy II musia do svojho posudzovania zhody zapojiť tretiu stranu.

Notifikácia orgánov posudzovania zhody (kapitola IV)

Na zaistenie vysokej úrovne kybernetickej bezpečnosti a pre dôveru všetkých zainteresovaných strán k systému nového prístupu je rozhodujúce riadne fungovanie notifikovaných osôb. V súlade s rozhodnutím 768/2008/ES sa preto v návrhu stanovujú požiadavky pre národné orgány, ktoré zodpovedajú za orgány posudzovania zhody (notifikované osoby). Zodpovednosť za navrhovanie a monitorovanie notifikovaných osôb sa v ňom v plnej miere ponecháva na členské štáty. Členské štáty určia notifikujúci orgán, ktorý zodpovedá za stanovenie a vykonávanie potrebných postupov na posudzovanie a notifikáciu orgánov posudzovania zhody a na monitorovanie notifikovaných osôb.

Dohľad nad trhom a presadzovanie práva (kapitola V)

Dohľad nad trhom na území daného členského štátu vykonávajú národné orgány dohľadu nad trhom v súlade s nariadením (EÚ) 2019/1020. Členské štáty sa môžu rozhodnúť, že určia ktorýkoľvek existujúci alebo nový orgán, aby konal ako orgán dohľadu nad trhom, a to vrátane zriadených vnútroštátnych príslušných orgánov uvedených v článku [článok X] smernice [smernica XXX/XXXX (NIS2)] alebo určených vnútroštátnych orgánov pre certifikáciu kybernetickej bezpečnosti uvedených v článku 58 nariadenia (EÚ) 2019/881. Hospodárske subjekty sa vyzývajú, aby v plnej miere spolupracovali s orgánmi dohľadu nad trhom a s ďalšími príslušnými orgánmi.

Delegované právomoci a postupy výboru (kapitola VI)

S cieľom zabezpečiť, aby regulačný rámec bolo podľa potreby možné prispôsobiť, bola právomoc prijímať akty v súlade s článkom 290 ZFEÚ delegovaná na Komisiu na účely aktualizovania zoznamu kritických produktov triedy I a II a špecifikovania vymedzenia týchto produktov; špecifikovania, či je potrebné obmedzenie alebo vylúčenie produktov s digitálnymi prvkami, na ktoré sa vzťahujú iné pravidlá Únie, ktorými sa stanovujú požiadavky na dosiahnutie rovnakej úrovne ochrany ako týmto nariadením; stanovenia povinnosti certifikácie určitých vysokokritických produktov s digitálnymi prvkami na základe kritérií stanovených v tomto nariadení; špecifikovania minimálneho obsahu EÚ vyhlásenia o zhode a doplnenia prvkov, ktoré sa majú zahrnúť do technickej dokumentácie.

Komisia je takisto splnomocnená prijímať vykonávacie akty, ktorými sa: špecifikuje formát alebo prvky správ podávaných v rámci oznamovacej povinnosti a zoznam softvérových komponentov; špecifikujú európske systémy certifikácie kybernetickej bezpečnosti, ktoré možno použiť na preukázanie zhody so základnými požiadavkami alebo ich časťami, ako sa uvádza v tomto nariadení; prijímajú spoločné špecifikácie; stanovujú technické špecifikácie pre umiestnenie označenia CE; prijímajú nápravné alebo reštriktívne opatrenia na úrovni Únie za mimoriadnych okolností, ktoré odôvodňujú okamžitý zásah na zachovanie riadneho fungovania vnútorného trhu.

Dôvernosť a sankcie (kapitola VII)

Všetky strany, ktoré uplatňujú toto nariadenie musia dodržiavať dôvernosť informácií a údajov získaných pri vykonávaní svojich úloh a činností.

V záujme zabezpečenia účinného presadzovania povinností stanovených v tomto nariadení by každý orgán dohľadu nad trhom mal mať právomoc uložiť alebo požiadať o uloženie správnych pokút. V rovnakom duchu toto nariadenie stanovuje maximálne úrovne administratívnych pokút, ktoré by sa mali stanoviť vo vnútroštátnych zákonoch za nesplnenie povinností stanovených v tomto nariadení.

Prechodné a záverečné ustanovenia (kapitola VIII)

S cieľom umožniť výrobcom, notifikovaným osobám a členským štátom čas na prispôsobenie sa novým požiadavkám sa navrhované nariadenie stane uplatniteľným [24 mesiacov] od nadobudnutia jeho účinnosti s výnimkou oznamovacej povinnosti výrobcov, ktorá by sa uplatňovala od [12 mesiacov] odo dňa nadobudnutia účinnosti.

2022/0272 (COD)

Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY

o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadenia (EÚ) 2019/1020

(Text s významom pre EHP)

EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 114,

so zreteľom na návrh Európskej komisie,

po postúpení návrhu legislatívneho aktu národným parlamentom,

so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru[1],

so zreteľom na stanovisko Výboru regiónov[2],

konajúc v súlade s riadnym legislatívnym postupom,

keďže:

(1) Je potrebné zlepšiť fungovanie vnútorného trhu stanovením jednotného právneho rámca základných požiadaviek kybernetickej bezpečnosti pre uvádzanie produktov s digitálnymi prvkami na trh Únie. Vyriešiť by sa mali dva hlavné problémy, ktoré zvyšujú náklady používateľov a spoločnosti: nízka úroveň kybernetickej bezpečnosti produktov s digitálnymi prvkami, ktorá sa prejavuje rozšíreným výskytom zraniteľností a nedostatočným a nekonzistentným poskytovaním bezpečnostných aktualizácií na ich riešenie, a nedostatočné chápanie používateľov a ich prístup k informáciám, čo im bráni vybrať si produkty s vhodnými vlastnosťami kybernetickej bezpečnosti alebo používať ich bezpečným spôsobom.

(2) Cieľom tohto nariadenia je vytvoriť hraničné podmienky pre vývoj bezpečných produktov s digitálnymi prvkami zabezpečením, aby sa na trh uvádzali hardvérové a softvérové produkty s menším počtom zraniteľností a aby výrobcovia brali bezpečnosť vážne počas celého životného cyklu produktu. Jeho cieľom je aj vytvorenie podmienok, ktoré používateľom umožnia zohľadniť kybernetickú bezpečnosť pri výbere a používaní produktov s digitálnymi prvkami.

(3) Príslušné právne predpisy Únie, ktoré sú v súčasnosti účinné, obsahujú niekoľko súborov horizontálnych pravidiel, ktorými sa riešia určité aspekty súvisiace s kybernetickou bezpečnosťou z rôznych hľadísk vrátane opatrení na zvýšenie bezpečnosti digitálneho dodávateľského reťazca. Existujúce právne predpisy Únie, ktoré sa týkajú kybernetickej bezpečnosti, vrátane [smernice XXX/XXXX (NIS2)]

[1] Ú. v. EÚ C , , s. .
[2] Ú. v. EÚ C , , s. .

a nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881[3] však priamo neobsahujú povinné požiadavky bezpečnosti produktov s digitálnymi prvkami.

(4) Aj keď sa existujúce právne predpisy Únie uplatňujú na určité produkty s digitálnymi prvkami, neexistuje žiadny horizontálny regulačný rámec Únie stanovujúci komplexné požiadavky kybernetickej bezpečnosti pre všetky produkty s digitálnymi prvkami. Rôzne akty a iniciatívy prijaté dosiaľ na úrovni Únie a na vnútroštátnej úrovni riešia identifikované problémy a riziká týkajúce sa kybernetickej bezpečnosti iba čiastočne, čím sa vytvára na vnútornom trhu zmes právnych predpisov, zvyšuje právna neistota výrobcov aj používateľov týchto produktov a pridáva zbytočná záťaž spoločnostiam pri plnení mnohých požiadaviek v súvislosti s podobnými druhmi produktov. Kybernetická bezpečnosť týchto produktov má zároveň obzvlášť výrazný cezhraničný rozmer, keďže produkty vyrobené v jednej krajine používajú často organizácie a spotrebitelia na celom vnútornom trhu. Preto je potrebné regulovať túto oblasť na úrovni Únie. Regulačné prostredie Únie by sa malo harmonizovať zavedením požiadaviek kybernetickej bezpečnosti pre produkty s digitálnymi prvkami. Okrem toho by sa pre hospodárske subjekty a používateľov mala v celej Únii zabezpečiť istota a lepšia harmonizácia jednotného trhu vytvorením životaschopnejších podmienok pre hospodárske subjekty, ktoré plánujú vstup na trh Únie.

(5) Na úrovni Únie obsahujú rôzne programové a politické dokumenty, napríklad stratégia kybernetickej bezpečnosti EÚ v digitálnej dekáde[4], závery Rady z 2. decembra 2020 a z 23. mája 2022 alebo uznesenie Európskeho parlamentu z 10. júna 2021[5], výzvy na zavedenie špecifických požiadaviek Únie týkajúcich sa kybernetickej bezpečnosti digitálnych alebo pripojených produktov, pričom viaceré krajiny na celom svete zavádzajú opatrenia na riešenie tohto problému z vlastnej iniciatívy. V záverečnej správe z Konferencie o budúcnosti Európy[6] občania vyzvali na „silnejšiu úlohu EÚ v boji proti kybernetickobezpečnostným hrozbám“.

(6) Na zvýšenie celkovej úrovne kybernetickej bezpečnosti všetkých produktov s digitálnymi prvkami uvedenými na vnútorný trh je potrebné zaviesť pre tieto produkty cieľovo zamerané a technologicky neutrálne základné požiadavky kybernetickej bezpečnosti, ktoré sa uplatňujú horizontálne.

(7) Za určitých podmienok môžu všetky produkty s digitálnymi prvkami integrované vo väčšom elektronickom informačnom systéme alebo pripojené k takému systému slúžiť ako vektor útoku škodlivých subjektov. V dôsledku toho aj hardvér a softvér považovaný za menej kritický môže uľahčiť počiatočné ohrozenie zariadenia alebo siete, ktoré umožní škodlivým subjektom získať privilegovaný prístup do systému alebo sa pohybovať laterálne naprieč systémami. Výrobcovia by preto mali zabezpečiť, aby všetky pripojiteľné produkty s digitálnymi prvkami boli navrhnuté a vyvíjané v súlade so základnými požiadavkami stanovenými v tomto nariadení. Toto

---

[3] Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7.6.2019, s. 15).

[4] JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/SK/ALL/?uri=JOIN:2020:18:FIN.

[5] 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_SK.html.

[6] *Conference on the Future of Europe – Report on the Final Outcome*, (Konferencia o budúcnosti Európy – správa o konečnom výsledku) máj 2022, návrh 28 opatrenie 2. Konferencia sa konala od apríla 2021 do mája 2022. Išlo o jedinečnú realizáciu deliberatívnej demokracie na celoeurópskej úrovni pod vedením občanov, pričom sa do tohto podujatia zapojili tisíce európskych občanov, ako aj politickí aktéri, sociálni partneri, zástupcovia občianskej spoločnosti a kľúčové zainteresované strany.

sa týka produktov, ktoré možno pripojiť fyzicky prostredníctvom hardvérového rozhrania, aj produktov, ktoré sa pripájajú logicky, napr. pomocou sieťových zásuviek, dátovodov, súborov, aplikačných programovacích rozhraní alebo iných druhov softvérového rozhrania. Keďže kybernetické hrozby sa môžu šíriť rôznymi produktmi s digitálnymi prvkami pred dosiahnutím určitého cieľa, napríklad zreťazením niekoľkých zneužití zraniteľnosti, výrobcovia by mali zaistiť kybernetickú bezpečnosť aj tých produktov, ktoré sú iba nepriamo pripojené k iným zariadeniam alebo sieťam.

(8) Stanovením požiadaviek kybernetickej bezpečnosti na uvádzanie produktov s digitálnymi prvkami na trh sa zlepší kybernetická bezpečnosť týchto produktov pre spotrebiteľov, ako aj pre podniky. Toto zahŕňa aj požiadavky na uvedenie na trh, ktoré sa týkajú spotrebného tovaru s digitálnymi prvkami určeného pre zraniteľných spotrebiteľov, ako napríklad hračky a elektronické pestúnky.

(9) Týmto nariadením sa zabezpečí vysoká úroveň kybernetickej bezpečnosti produktov s digitálnymi prvkami. Neregulujú sa ním služby, napríklad softvér ako služba (SaaS), okrem riešení diaľkového spracúvania údajov týkajúcich sa produktu s digitálnymi prvkami, ktoré sa chápu ako akékoľvek spracúvanie údajov na diaľku, pre ktoré je softvér určený a vyvinutý výrobcom dotknutého produktu alebo na zodpovednosť takého výrobcu, a ktorého neexistencia by zabránila tomu, aby takýto produkt s digitálnymi prvkami plnil jednu zo svojich funkcií. [Smernicou XXX/XXXX (NIS2)] sa zavádzajú požiadavky kybernetickej bezpečnosti a oznamovania incidentov pre kľúčové a dôležité subjekty, napríklad kritickú infraštruktúru, s cieľom zvýšiť odolnosť služieb, ktoré poskytujú. [Smernica XXX/XXXX (NIS2)] sa uplatňuje na služby cloud computingu a cloudové modely služieb, akým je softvér ako služba. Všetky subjekty poskytujúce služby cloud computingu v Únii, ktoré spĺňajú alebo prekračujú prahovú hodnotu pre stredné podniky, patria do pôsobnosti uvedenej smernice.

(10) Aby sa nebránilo inováciám alebo výskumu, na slobodný softvér a softvér s otvoreným zdrojovým kódom vyvinutý alebo dodaný mimo rámca komerčnej činnosti by sa toto nariadenie nemalo vzťahovať. Týka sa to najmä softvéru vrátane jeho zdrojového kódu a upravených verzií, ktorý je voľne zdieľaný a bezplatne dostupný, použiteľný, upraviteľný a opakovane distribuovateľný. V súvislosti so softvérom by komerčná činnosť mohla byť charakterizovaná nielen účtovaním ceny za produkt, ale aj účtovaním ceny za služby technickej podpory, poskytovaním softvérovej platformy, prostredníctvom ktorej výrobca speňažuje ostatné služby, alebo použitím osobných údajov z iných dôvodov ako výlučne z dôvodu zvýšenia bezpečnosti, kompatibility alebo interoperability softvéru.

(11) Bezpečný internet je nevyhnutný pre fungovanie kritickej infraštruktúry a pre spoločnosť ako celok. Cieľom [smernice XXX/XXXX (NIS2)] je zaistiť vysokú úroveň kybernetickej bezpečnosti služieb poskytovaných kľúčovými a dôležitými subjektmi vrátane poskytovateľov digitálnej infraštruktúry, ktorí podporujú základné funkcie otvoreného internetu, zabezpečujú prístup na internet a internetové služby. Je preto dôležité, aby sa produkty s digitálnymi prvkami, ktoré potrebujú poskytovatelia digitálnej infraštruktúry na zabezpečenie fungovania internetu, vyvíjali bezpečným spôsobom a aby boli v súlade so zavedenými normami bezpečnosti internetu. Toto nariadenie, ktoré sa uplatňuje na všetky pripojiteľné hardvérové a softvérové produkty, sa takisto zameriava na uľahčenie dodržiavania požiadaviek dodávateľského reťazca podľa [smernice XXX/XXXX (NIS2)] poskytovateľmi digitálnej infraštruktúry tým, že sa zabezpečí, aby sa produkty s digitálnymi prvkami, ktoré používajú na

poskytovanie svojich služieb, vyvíjali bezpečným spôsobom a aby mali prístup ku včasným bezpečnostným aktualizáciám takýchto produktov.

(12) V nariadení Európskeho parlamentu a Rady (EÚ) 2017/745[7] sú stanovené pravidlá pre zdravotnícke pomôcky a v nariadení Európskeho parlamentu a Rady (EÚ) 2017/746[8] sú stanovené pravidlá pre diagnostické zdravotnícke pomôcky *in vitro*. V oboch nariadeniach sa riešia kybernetickobezpečnostné riziká a uplatňujú sa v nich osobitné prístupy, ktorým sa venuje aj v toto nariadenie. Presnejšie, v nariadeniach (EÚ) 2017/745 a (EÚ) 2017/746 sa stanovujú základné požiadavky na zdravotnícke pomôcky, ktoré fungujú prostredníctvom elektronického systému, alebo ktoré samotné sú softvérom. Uvedené nariadenia sa vzťahujú aj na určitý nezabudovaný softvér a zohľadňovanie celoživotného cyklu. Tieto požiadavky ukladajú výrobcom povinnosť vyvíjať a konštruovať svoje produkty s uplatnením zásad manažérstva rizika a so stanovením požiadaviek, ktoré sa týkajú bezpečnostných opatrení IT a zodpovedajú postupom posudzovania zhody. Okrem toho je od decembra 2019 zavedené osobitné usmernenie ku kybernetickej bezpečnosti zdravotníckych pomôcok, ktorým sa výrobcom zdravotníckych pomôcok vrátane diagnostických pomôcok *in vitro* poskytuje usmernenie k tomu, ako splniť všetky príslušné základné požiadavky prílohy I k uvedeným nariadeniam, čo sa týka kybernetickej bezpečnosti[9]. Produkty s digitálnymi prvkami, na ktoré sa uplatňuje jedno z uvedených nariadení, by preto nemali podliehať tomuto nariadeniu.

(13) V nariadení Európskeho parlamentu a Rady (EÚ) 2019/2144[10] sa stanovujú požiadavky na typové schvaľovanie vozidiel a ich systémov a komponentov, pričom sa zavádzajú určité požiadavky kybernetickej bezpečnosti vrátane požiadaviek na prevádzku certifikovaného systému riadenia kybernetickej bezpečnosti a na aktualizácie softvéru, ktoré sa vzťahujú na politiky a procesy organizácií v oblasti kybernetických rizík počas celého životného cyklu vozidiel, zariadení a služieb v súlade s uplatniteľnými predpismi Organizácie Spojených národov o technických špecifikáciách a kybernetickej bezpečnosti[11], a stanovujú osobitné postupy posudzovania zhody. V oblasti letectva je hlavným cieľom nariadenia Európskeho

---

7 Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/745 z 5. apríla 2017 o zdravotníckych pomôckach, zmene smernice 2001/83/ES, nariadenia (ES) č. 178/2002 a nariadenia (ES) č. 1223/2009 a o zrušení smerníc Rady 90/385/EHS a 93/42/EHS (Ú. v. EÚ L 117, 5.5.2017, s. 1).

8 Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/746 z 5. apríla 2017 o diagnostických zdravotníckych pomôckach *in vitro* a o zrušení smernice 98/79/ES a rozhodnutia Komisie 2010/227/EÚ (Ú. v. EÚ L 117, 5.5.2017, s. 176).

9 MDCG 2019-16, potvrdené Koordinačnou skupinou pre zdravotnícke pomôcky (MDCG) zriadenou článkom 103 nariadenia (EÚ) 2017/745.

10 Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/2144 z 27. novembra 2019 o požiadavkách na typové schvaľovanie motorových vozidiel a ich prípojných vozidiel a systémov, komponentov a samostatných technických jednotiek určených pre tieto vozidlá, pokiaľ ide o ich všeobecnú bezpečnosť a ochranu cestujúcich vo vozidle a zraniteľných účastníkov cestnej premávky, ktorým sa mení nariadenie Európskeho parlamentu a Rady (EÚ) 2018/858 a ktorým sa zrušujú nariadenia Európskeho parlamentu a Rady (ES) č. 78/2009, (ES) č. 79/2009 a (ES) č. 661/2009 a nariadenia Komisie (ES) č. 631/2009, (EÚ) č. 406/2010, (EÚ) č. 672/2010, (EÚ) č. 1003/2010, (EÚ) č. 1005/2010, (EÚ) č. 1008/2010, (EÚ) č. 1009/2010, (EÚ) č. 19/2011, (EÚ) č. 109/2011, (EÚ) č. 458/2011, (EÚ) č. 65/2012, (EÚ) č. 130/2012, (EÚ) č. 347/2012, (EÚ) č. 351/2012, (EÚ) č. 1230/2012 a (EÚ) 2015/166 (Ú. v. EÚ L 325, 16.12.2019, s. 1).

11 Predpis OSN č. 155 – Jednotné ustanovenia na účely typového schvaľovania vozidiel vzhľadom na kybernetickú bezpečnosť a systém riadenia kybernetickej bezpečnosti [2021/387].

parlamentu a Rady (EÚ) 2018/1139[12] dosiahnutie a udržanie vysokej a jednotnej úrovne bezpečnosti civilného letectva v Únii. Nariadením sa vytvára rámec pre základné požiadavky letovej spôsobilosti výrobkov, súčastí a zariadení, vrátane softvéru, leteckej techniky, ktorý zohľadňuje povinnosti ochrany pred ohrozením bezpečnosti informácií. Produkty s digitálnymi prvkami, na ktoré sa uplatňuje nariadenie (EÚ) 2019/2144 a produkty certifikované v súlade s nariadením (EÚ) 2018/1139 preto nepodliehajú základným požiadavkám a postupom posudzovania zhody stanoveným v tomto nariadení. Postup certifikácie podľa nariadenia (EÚ) 2018/1139 zaisťuje úroveň zabezpečenia, ktorá je cieľom tohto nariadenia.

(14) Týmto nariadením sa stanovujú horizontálne pravidlá kybernetickej bezpečnosti, ktoré nie sú špecifické pre odvetvia alebo určité produkty s digitálnymi prvkami. Mohli by sa však zaviesť špecifické pravidlá Únie pre dané odvetvie alebo produkt a stanovili by sa v nich požiadavky, ktorými by sa riešili všetky alebo niektoré riziká, na ktoré sa vzťahujú základné požiadavky stanovené v tomto nariadení. V takýchto prípadoch možno uplatňovanie tohto nariadenia na produkty s digitálnymi prvkami, na ktoré sa vzťahujú iné pravidlá Únie stanovujúce požiadavky, ktorými sa riešia všetky alebo niektoré riziká, ktorých sa týkajú základné požiadavky stanovené v prílohe I k tomuto nariadeniu, obmedziť alebo vylúčiť, ak sa takéto obmedzenie alebo vylúčenie zhoduje s celkovým regulačným rámcom uplatňovaným na tieto produkty a ak sa odvetvovými pravidlami dosiahne rovnaká úroveň ochrany ako úroveň stanovená týmto nariadením. Komisia je splnomocnená prijímať vykonávacie akty s cieľom zmeniť toto nariadenie identifikovaním takýchto produktov a pravidiel. V prípade právnych predpisov Únie, na ktoré by sa mali takéto obmedzenia alebo vylúčenia uplatniť, obsahuje toto nariadenie osobitné ustanovenia na objasnenie jeho vzťahu k uvedeným právnym predpisom Únie.

(15) V delegovanom nariadení (EÚ) 2022/30 sa uvádza, že na určité rádiové zariadenia sa uplatňujú základné požiadavky stanovené v článku 3 ods. 3 písm. d) (nepriaznivý vplyv na sieť a zneužitie zdrojov siete), písm. e) (osobné údaje a súkromie) a písm. f) (podvod) smernice 2014/53/EÚ. Vo [vykonávacom rozhodnutí Komisie XXX/2022 o mandáte na tvorbu normy pre európske normalizačné organizácie] sa stanovujú požiadavky na vypracovanie konkrétnych noriem s ďalším špecifikovaním spôsobu, akým by sa tieto tri základné požiadavky mali riešiť. Základné požiadavky stanovené v tomto nariadení obsahujú všetky prvky základných požiadaviek uvedených v článku 3 ods. 3 písm. d), e) a f) smernice 2014/53/EÚ. Navyše základné požiadavky stanovené v tomto nariadení sú zosúladené s cieľmi požiadaviek na konkrétne normy, ktoré obsahuje uvedený mandát na tvorbu normy. Ak teda Komisia zruší alebo zmení delegované nariadenie (EÚ) 2022/30 s tým dôsledkom, že sa prestane uplatňovať na určité produkty, na ktoré sa vzťahuje toto nariadenie, Komisia a európske normalizačné organizácie by mali pri príprave a vypracúvaní harmonizovaných noriem na uľahčenie vykonávania tohto nariadenia zohľadniť normalizačnú prácu vykonanú v súvislosti s vykonávacím rozhodnutím Komisie C(2022) 5637 o mandáte na tvorbu normy týkajúcom sa delegovaného nariadenia 2022/30, ktorým sa dopĺňa smernica o rádiových zariadeniach.

[12] Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1139 zo 4. júla 2018 o spoločných pravidlách v oblasti civilného letectva, ktorým sa zriaďuje Agentúra Európskej únie pre bezpečnosť letectva a ktorým sa menia nariadenia Európskeho parlamentu a Rady (ES) č. 2111/2005, (ES) č. 1008/2008, (EÚ) č. 996/2010, (EÚ) č. 376/2014 a smernice Európskeho parlamentu a Rady 2014/30/EÚ a 2014/53/EÚ a zrušujú nariadenia Európskeho parlamentu a Rady (ES) č. 552/2004 a (ES) č. 216/2008 a nariadenie Rady (EHS) č. 3922/91 (Ú. v. EÚ L 212, 22.8.2018, s. 1).

(16) Smernica 85/374/EHS[13] dopĺňa toto nariadenie. Uvedenou smernicou sa stanovujú pravidlá zodpovednosti za chybné výrobky, aby poškodené osoby mohli uplatniť nárok na náhradu, keď im škodu spôsobili chybné výrobky. Ustanovuje zásadu, že výrobca výrobku zodpovedá za škody spôsobené nedostatočnou bezpečnosťou svojho výrobku bez ohľadu na chybu (objektívna zodpovednosť). Ak sú príčinou nedostatočnej bezpečnosti nedostatočné bezpečnostné aktualizácie po uvedení produktu na trh, a tie spôsobia škodu, môže sa uplatniť zodpovednosť výrobcu. Povinnosti výrobcu, ktoré sa týkajú poskytovania bezpečnostných aktualizácií, by sa mali stanoviť v tomto nariadení.

(17) Týmto nariadením by nemalo byť dotknuté nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679[14], ktoré obsahuje ustanovenia o zavedení mechanizmov certifikácie ochrany údajov a pečatí a značiek ochrany údajov na účely preukazovania súladu spracovateľských operácií vykonávaných prevádzkovateľmi a sprostredkovateľmi s uvedeným nariadením. Tieto operácie by mohli byť začlenené do produktu s digitálnymi prvkami. Špecificky navrhnutá a štandardná ochrana údajov a kybernetická bezpečnosť vo všeobecnosti sú kľúčovými prvkami nariadenia (EÚ) 2016/679. Základné požiadavky kybernetickej bezpečnosti stanovené v tomto nariadení majú ochranou spotrebiteľov a organizácií pred kybernetickobezpečnostnými rizikami prispieť aj k zvýšeniu ochrany osobných údajov a súkromia jednotlivcov. Mala by sa zvážiť synergia aspektov normalizácie aj certifikácie kybernetickej bezpečnosti prostredníctvom spolupráce medzi Komisiou, európskymi normalizačnými organizáciami, Agentúrou Európskej únie pre kybernetickú bezpečnosť (ENISA), Európskym výborom pre ochranu údajov (EDBP), ktorý bol zriadený nariadením (EÚ) 2016/679, a národnými dozornými orgánmi pre ochranu údajov. Vytvoriť by sa mala synergia aj medzi týmto nariadením a právnymi predpismi Únie o ochrane údajov v oblasti dohľadu nad trhom a presadzovania práva. Na tento účel by národné orgány dohľadu nad trhom vymenované podľa tohto nariadenia mali spolupracovať s orgánmi, ktoré vykonávajú dohľad nad právom Únie v oblasti ochrany údajov. Tie by mali mať prístup aj k informáciám, ktoré sú dôležité pre plnenie ich úloh.

(18) Vydavatelia európskych peňaženiek digitálnej identity uvedení v článku [článok 6a ods. 2 nariadenia (EÚ) č. 910/2014 zmeneného návrhom nariadenia, ktorým sa mení nariadenie (EÚ) č. 910/2014, pokiaľ ide o stanovenie rámca európskej digitálnej identity,] by mali v rozsahu, v akom ich produkty patria do rozsahu pôsobnosti tohto nariadenia, dodržiavať tak horizontálne základné požiadavky stanovené v tomto nariadení, ako aj osobitné bezpečnostné požiadavky stanovené v článku [článok 6a nariadenia (EÚ) č. 910/2014 zmeneného návrhom nariadenia, ktorým sa mení nariadenie (EÚ) č. 910/2014, pokiaľ ide o stanovenie rámca európskej digitálnej identity]. V záujme uľahčenia dodržiavania predpisov by vydavatelia peňaženiek mali byť schopní preukázať súlad európskych peňaženiek digitálnej identity s požiadavkami stanovenými jednotlivo v oboch aktoch certifikovaním svojich produktov v rámci európskeho systému certifikácie kybernetickej bezpečnosti zavedeného podľa nariadenia (EÚ) 2019/881, pre ktorý Komisia prostredníctvom

---

13 Smernica Rady 85/374/EHS z 25. júla 1985 o aproximácii zákonov, iných právnych predpisov a správnych opatrení členských štátov o zodpovednosti za chybné výrobky (Ú. v. ES L 210, 7.8.1985, s. 29).

14 Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).

vykonávacieho aktu špecifikovala predpoklad zhody s týmto nariadením, pokiaľ sa certifikát alebo jeho časti vzťahujú na uvedené požiadavky.

(19) Určité úlohy stanovené v tomto nariadení by mala plniť agentúra ENISA v súlade s článkom 3 ods. 2 nariadenia (EÚ) 2019/881. Úlohou agentúry ENISA je najmä prijímať od výrobcov oznámenia o aktívne zneužívaných zraniteľnostiach, ktoré majú ich produkty s digitálnymi prvkami, ako aj o incidentoch, ktoré ovplyvnili bezpečnosť týchto produktov. Agentúra ENISA by mala takisto posielať tieto oznámenia príslušným jednotkám pre riešenie počítačových bezpečnostných incidentov (ďalej len „CSIRT“) alebo prípadne aj príslušným jednotným kontaktným miestam členských štátov určeným v súlade s článkom [článok X] smernice [smernica XXX/XXXX (NIS2)] a informovať príslušné orgány dohľadu nad trhom o oznámenej zraniteľnosti. Agentúra ENISA by na základe informácií, ktoré zhromažďuje, mala vypracovať každé dva roky technickú správu o vznikajúcich trendoch týkajúcich sa kybernetickobezpečnostných rizík produktov s digitálnymi prvkami a predložiť ju skupine pre spoluprácu uvedenej v smernici [smernica XXX/XXXX (NIS2)]. Vzhľadom na svoje odborné znalosti a mandát by agentúra ENISA mala byť navyše schopná podporovať proces vykonávania tohto nariadenia. Mala by byť najmä schopná navrhovať spoločné činnosti, ktoré by mali vykonávať orgány dohľadu nad trhom na základe údajov alebo informácií o možnom nesúlade produktov s digitálnymi prvkami s týmto nariadením vo viacerých členských štátoch, alebo identifikovať kategórie produktov, pri ktorých by sa mali organizovať súbežné koordinované kontrolné opatrenia. Za mimoriadnych okolností by na žiadosť Komisie mala byť agentúra ENISA schopná vykonať hodnotenie konkrétnych produktov s digitálnymi prvkami, ktoré predstavujú významné kybernetickobezpečnostné riziko, keď sa vyžaduje okamžitý zásah v záujme zachovania riadneho fungovania vnútorného trhu.

(20) Produkty s digitálnymi prvkami by mali niesť označenie CE, ktorým sa preukazuje zhoda s týmto nariadením, aby im bol umožnený voľný pohyb v rámci vnútorného trhu. Členské štáty by nemali vytvárať neodôvodnené prekážky uvedeniu produktov s digitálnymi prvkami, ktoré spĺňajú požiadavky stanovené v tomto nariadení a majú označenie CE, na trh.

(21) S cieľom zabezpečiť, aby výrobcovia mohli uvoľňovať softvér na účely testovania pred podrobením svojich produktov posudzovaniu zhody, by členské štáty nemali brániť sprístupneniu nedokončeného softvéru, ako sú alfa verzie, beta verzie alebo kandidáti na finálnu verziu, pokiaľ sa daná verzia sprístupňuje iba na čas potrebný na jej testovanie a získanie spätnej väzby. Výrobcovia by mali zabezpečiť, aby sa softvér sprístupnený podľa týchto podmienok uvoľnil iba po posúdení rizika a aby v najväčšej možnej miere spĺňal požiadavky bezpečnosti týkajúce sa vlastností produktov s digitálnymi prvkami, ktoré ukladá toto nariadenie. Výrobcovia by takisto mali v najväčšej možnej miere spĺňať požiadavky na riešenia zraniteľností. Výrobcovia by nemali nútiť používateľov, aby prešli na vyššie verzie uvoľnené iba na účely testovania.

(22) V záujme zabezpečenia toho, aby produkty s digitálnymi prvkami uvedené na trh nepredstavovali pre osoby a organizácie kybernetickobezpečnostné riziká, mali by sa pre takéto produkty stanoviť základné požiadavky. Ak sa produkty následne fyzicky alebo digitálne upravia spôsobom, s ktorým výrobca nepočítal a z ktorého môže vyplynúť, že už nespĺňajú príslušné základné požiadavky, táto úprava by sa mala považovať za podstatnú. Napríklad aktualizácie alebo opravy softvéru by sa mohli klásť na rovnakú úroveň ako činnosti údržby za predpokladu, že by sa nimi produkt, ktorý už bol uvedený na trh, neupravil takým spôsobom, ktorý by mohol ovplyvniť

spĺňanie uplatniteľných požiadaviek alebo ktorým by sa mohlo zmeniť zamýšľané použitie, na ktoré sa produkt posudzoval. Rovnako ako v prípade fyzických opráv alebo úprav by sa produkt s digitálnymi prvkami mal považovať za podstatne upravený softvérovou zmenou, pri ktorej sa aktualizáciou softvéru upravujú pôvodne zamýšľané funkcie, druh alebo výkon produktu, a tieto zmeny sa nepredvídali v pôvodnom posúdení rizík, alebo ak sa aktualizáciou softvéru zmenila povaha nebezpečenstva alebo zvýšila úroveň rizika.

(23) V súlade so všeobecne zaužívaným pojmom podstatnej úpravy pri produktoch regulovaných v rámci harmonizačných právnych predpisov Únie je vždy, keď dôjde k podstatnej úprave, ktorá môže ovplyvniť súlad produktu s týmto nariadením, alebo keď sa zmení zamýšľaný účel tohto produktu, vhodné overiť súlad produktu s digitálnymi prvkami s predpismi a prípadne ho podrobiť novému posúdeniu zhody. V prípade, keď sa výrobca rozhodne vykonať posúdenie zhody s účasťou tretej strany, tejto tretej strane by sa mali oznámiť zmeny, ktoré by mohli viesť k podstatným úpravám.

(24) Renovovanie, údržba a oprava produktu s digitálnymi prvkami, ako sa vymedzujú v nariadení [nariadenie o ekodizajne], nemusia nevyhnutne viesť k podstatnej úprave produktu, napríklad ak sa zamýšľané použitie a funkcie nezmenia a neovplyvnená zostane aj úroveň rizika. Ale modernizácia produktu výrobcom by mohla viesť k zmenám v návrhu a vývoji produktu, a teda by mohla ovplyvniť zamýšľané použitie a súlad produktu s požiadavkami stanovenými v tomto nariadení.

(25) Produkty s digitálnymi prvkami by sa mali považovať za kritické, ak nepriaznivý vplyv zneužitia potenciálnych zraniteľností kybernetickej bezpečnosti produktu môže byť závažný okrem iného z dôvodu funkcie súvisiacej s kybernetickou bezpečnosťou alebo zamýšľaného použitia. Zraniteľnosti produktov s digitálnymi prvkami, ktoré majú funkciu súvisiacu s kybernetickou bezpečnosťou, ako sú zabezpečené prvky, môžu viesť k šíreniu bezpečnostných problémov v celom dodávateľskom reťazci. Závažnosť dosahu kybernetického bezpečnostného incidentu sa môže takisto zvýšiť, keď sa zohľadní zamýšľané použitie produktu, napr. v priemyselnom prostredí alebo v súvislosti so základným subjektom druhu, ktorý je uvedený v prílohe [príloha I] k smernici [smernica XXX/XXXX (NIS2)], alebo výkon kritických alebo citlivých funkcií, ako je spracúvanie osobných údajov.

(26) Kritické produkty s digitálnymi prvkami by mali podliehať prísnejším postupom posudzovania zhody pri súčasnom zachovaní primeraného prístupu. Na tento účel by sa mali kritické produkty s digitálnymi prvkami rozdeliť do dvoch tried podľa úrovne kybernetickobezpečnostného rizika spojeného s týmito kategóriami produktov. Potenciálny kybernetický incident produktov triedy II by mohol viesť k väčším nepriaznivým účinkom než incident produktov triedy I, napríklad z dôvodu povahy ich funkcie súvisiacej s kybernetickou bezpečnosťou alebo z dôvodu zamýšľaného použitia v citlivom prostredí, a preto by sa mali podrobiť prísnejšiemu postupu posudzovania zhody.

(27) Kategórie kritických produktov s digitálnymi prvkami uvedené v prílohe III k tomuto nariadeniu by sa mali chápať ako produkty, ktoré majú hlavnú funkciu druhu, ktorý je uvedený v prílohe III k tomuto nariadeniu. Napríklad v prílohe III k tomuto nariadeniu sa uvádzajú produkty, ktoré sú na základe svojej hlavnej funkcie vymedzené ako mikroprocesory na všeobecný účel v triede II. V dôsledku toho sú mikroprocesory na všeobecný účel predmetom povinného posudzovania zhody treťou stranou. Toto neplatí pre iné produkty, ktoré nie sú výslovne uvedené v prílohe III k tomuto

nariadeniu, ktoré môžu mať integrovaný mikroprocesor na všeobecný účel. Komisia by mala prijať delegované akty [do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia] s cieľom špecifikovať vymedzenie kategórií produktov triedy I a triedy II, ako sa uvádzajú v prílohe III.

(28) V tomto nariadení sa riešia kybernetickobezpečnostné riziká cieleným spôsobom. Produkty s digitálnymi prvkami by však mohli predstavovať ďalšie bezpečnostné riziká, ktoré nesúvisia s kybernetickou bezpečnosťou. Tieto riziká by mali byť naďalej regulované inými príslušnými právnymi predpismi Únie o produktoch. Ak nemožno uplatniť žiadne iné harmonizačné právne predpisy Únie, malo by sa na ne vzťahovať nariadenie [nariadenie o všeobecnej bezpečnosti výrobkov]. Preto vzhľadom na cielenú povahu tohto nariadenia by sa odchylne od článku 2 ods. 1 tretieho pododseku písm. b) nariadenia [nariadenie o všeobecnej bezpečnosti výrobkov] mala kapitola III oddiel 1, kapitoly V a VII a kapitoly IX až XI nariadenia [nariadenie o všeobecnej bezpečnosti výrobkov] uplatňovať na produkty s digitálnymi prvkami, pokiaľ ide o bezpečnostné riziká, na ktoré sa nevzťahuje toto nariadenie, ak sa na tieto produkty nevzťahujú osobitné požiadavky uložené inými harmonizačnými právnymi predpismi Únie v zmysle [článku 3 bodu 25 nariadenia o všeobecnej bezpečnosti výrobkov].

(29) Produkty s digitálnymi prvkami klasifikované ako vysokorizikové systémy umelej inteligencie podľa článku 6 nariadenia[15] [nariadenie o umelej inteligencii], ktoré patria do rozsahu pôsobnosti tohto nariadenia, by mali vyhovovať základným požiadavkám stanoveným v tomto nariadení. Keď tieto vysokorizikové systémy umelej inteligencie spĺňajú základné požiadavky tohto nariadenia, mali by sa považovať za systémy spĺňajúce požiadavky kybernetickej bezpečnosti stanovené v článku [článok 15] nariadenia [nariadenie o umelej inteligencii], pokiaľ sa na tieto požiadavky vzťahuje EÚ vyhlásenie o zhode alebo jeho časti vydané podľa tohto nariadenia. Pokiaľ ide o postupy posudzovania zhody týkajúce sa základných požiadaviek kybernetickej bezpečnosti produktu s digitálnymi prvkami, na ktorý sa vzťahuje toto nariadenie a ktorý je klasifikovaný ako vysokorizikový systém umelej inteligencie, namiesto príslušných ustanovení tohto nariadenia by sa mali spravidla uplatňovať príslušné ustanovenia článku 43 nariadenia [nariadenie o umelej inteligencii]. Toto pravidlo by však nemalo viesť k zníženiu potrebného stupňa dôveryhodnosti pre kritické produkty s digitálnymi prvkami, na ktoré sa vzťahuje toto nariadenie. Odchylne od tohto pravidla by preto vysokorizikové systémy umelej inteligencie, ktoré patria do rozsahu pôsobnosti nariadenia [nariadenie o umelej inteligencii] a zároveň sú kvalifikované ako kritické produkty s digitálnymi prvkami podľa tohto nariadenia, na ktoré sa uplatňuje postup posudzovania zhody na základe vnútornej kontroly uvedený v prílohe VI k nariadeniu [nariadenie o umelej inteligencii], mali podliehať ustanoveniam tohto nariadenia týkajúcim sa posudzovania zhody, pokiaľ ide o základné požiadavky tohto nariadenia. V tomto prípade by sa na všetky ostatné aspekty, na ktoré sa vzťahuje nariadenie [nariadenie o umelej inteligencii], mali uplatňovať príslušné ustanovenia o posudzovaní zhody na základe vnútornej kontroly uvedené v prílohe VI k nariadeniu [nariadenie o umelej inteligencii].

(30) Strojnícke výrobky patriace do rozsahu pôsobnosti nariadenia [návrh nariadenia o strojníckych výrobkoch], ktoré sú v zmysle tohto nariadenia produktmi s digitálnymi prvkami a pre ktoré bolo vydané vyhlásenie o zhode na základe tohto nariadenia, by sa mali považovať za výrobky, ktoré sú v zhode so základnými požiadavkami na ochranu

[15] Nariadenie [nariadenie o umelej inteligencii].

zdravia a bezpečnosť stanovenými v [oddieloch 1.1.9 a 1.2.1 prílohy III] k nariadeniu [návrh nariadenia o strojníckych výrobkoch], čo sa týka ochrany pred zneužitím a bezpečnosti a spoľahlivosti ovládacích systémov, pokiaľ je súlad s týmito požiadavkami preukázaný EÚ vyhlásením o zhode vydaným podľa tohto nariadenia.

(31) Nariadenie [návrh nariadenia o európskom priestore pre zdravotné údaje] dopĺňa základné požiadavky stanovené v tomto nariadení. Systémy elektronických zdravotných záznamov patriace do rozsahu pôsobnosti nariadenia [návrh nariadenia o európskom priestore pre zdravotné údaje], ktoré sú v zmysle tohto nariadenia produktmi s digitálnymi prvkami, by preto takisto mali spĺňať základné požiadavky stanovené v tomto nariadení. Ich výrobcovia by mali preukázať zhodu požadovanú podľa nariadenia [návrh nariadenia o európskom priestore pre zdravotné údaje]. Na uľahčenie dosiahnutia súladu môžu výrobcovia vypracovať jednotnú technickú dokumentáciu obsahujúcu prvky požadované oboma právnymi aktmi. Keďže toto nariadenie sa nevzťahuje na softvér ako službu (SaaS) ako taký, systémy elektronických zdravotných záznamov ponúkané prostredníctvom modelu udeľovania licencií a dodávania SaaS nepatria do rozsahu pôsobnosti tohto nariadenia. Podobne do rozsahu pôsobnosti tohto nariadenia nepatria systémy elektronických zdravotných záznamov vyvinuté a používané interne, keďže sa neuvádzajú na trh.

(32) S cieľom zaistiť, aby boli produkty s digitálnymi prvkami zabezpečené tak v čase ich uvedenia na trh, ako aj počas ich celého životného cyklu, je potrebné stanoviť základné požiadavky na riešenie zraniteľností a základné požiadavky kybernetickej bezpečnosti týkajúce sa vlastností produktov s digitálnymi prvkami. Hoci by výrobcovia mali splniť všetky základné požiadavky týkajúce sa riešenia zraniteľností a zaistiť, aby sa všetky ich produkty dodávali bez akýchkoľvek známych zneužiteľných zraniteľností, mali by určiť, ktoré ďalšie základné požiadavky týkajúce sa vlastností produktu sú relevantné pre príslušný druh produktu. Na tento účel by výrobcovia mali vykonať posúdenie kybernetickobezpečnostných rizík spojených s produktom s digitálnymi prvkami, aby identifikovali príslušné riziká a relevantné základné požiadavky a aby primerane uplatňovali vhodné harmonizované normy alebo spoločné špecifikácie.

(33) S cieľom zlepšiť bezpečnosť produktov s digitálnymi prvkami uvádzaných na vnútorný trh je potrebné stanoviť základné požiadavky. Týmito základnými požiadavkami by nemalo byť dotknuté koordinované posudzovanie rizík kritických dodávateľských reťazcov na úrovni EÚ stanovené v [článku X] smernice [smernica XXX/XXXX(NIS2)][16], pri ktorom sa zohľadňujú technické a prípadne aj netechnické faktory rizík, ako je neprimeraný vplyv tretej krajiny na dodávateľov. Okrem toho by nemalo byť dotknuté výsadné právo členských štátov stanoviť ďalšie požiadavky, ktoré zohľadňujú netechnické faktory na účely zaistenia vysokej úrovne odolnosti vrátane požiadaviek vymedzených v odporúčaní (EÚ) 2019/534, v celoúnijnom koordinovanom posúdení rizika bezpečnosti sietí 5G a v súbore nástrojov EÚ pre kybernetickú bezpečnosť 5G, ktoré schválila skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, ako sa uvádza v [smernici XXX/XXXX (NIS2)].

(34) S cieľom zaistiť, aby sa vnútroštátnym jednotkám CSIRT a jednotným kontaktným miestam určeným v súlade s článkom [článok X] smernice [smernica XXX/XXXX

[16] Smernica Európskeho parlamentu a Rady XXX z [dátum] [o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa zrušuje smernica (EÚ) 2016/1148, (Ú. v. EÚ L xx, dátum, s. x)].

(NIS2)] poskytovali informácie potrebné na plnenie ich úloh a zvýšenie celkovej úrovne kybernetickej bezpečnosti kľúčových a dôležitých subjektov, a s cieľom zaistiť účinné fungovanie orgánov dohľadu nad trhom by výrobcovia produktov s digitálnymi prvkami mali agentúre ENISA oznamovať zraniteľnosti, ktoré sa aktívne zneužívajú. Keďže väčšina produktov s digitálnymi prvkami sa predáva na celom vnútornom trhu, akákoľvek zneužitá zraniteľnosť produktu s digitálnymi prvkami by sa mala považovať za ohrozenie fungovania vnútorného trhu. Výrobcovia by mali zvážiť aj zverejnenie opravených zraniteľností v európskej databáze zraniteľností zriadenej podľa smernice [smernica XXX/XXXX (NIS2)] a spravovanej agentúrou ENISA alebo v akejkoľvek inej verejne prístupnej databáze zraniteľností.

(35) Výrobcovia by takisto mali oznámiť agentúre ENISA každý incident, ktorý má vplyv na bezpečnosť produktu s digitálnymi prvkami. Bez ohľadu na povinnosti oznamovania incidentov stanovené pre kľúčové a dôležité subjekty v smernici [smernica XXX/XXXX (NIS2)] je pre agentúru ENISA, jednotné kontaktné miesta určené členskými štátmi v súlade s článkom [článok X] smernice [smernica XXX/XXXX (NIS2)] a orgány dohľadu nad trhom rozhodujúce, aby dostávali informácie od výrobcov produktov s digitálnymi prvkami, ktoré im umožnia posúdiť bezpečnosť týchto produktov. S cieľom zaistiť používateľom možnosť rýchlo reagovať na incidenty, ktoré majú vplyv na bezpečnosť ich produktov s digitálnymi prvkami, by výrobcovia mali informovať svojich používateľov aj o akomkoľvek takomto incidente a prípadne o akýchkoľvek nápravných opatreniach, ktoré môžu používatelia použiť na zmiernenie vplyvu daného incidentu, napríklad uverejnením príslušných informácií na svojich webových sídlach alebo priamym oslovením používateľov, ak výrobca dokáže kontaktovať používateľov a ak je to odôvodnené rizikami.

(36) Výrobcovia produktov s digitálnymi prvkami by mali zaviesť politiky koordinovaného zverejňovania informácií o zraniteľnostiach na uľahčenie oznamovania zraniteľností jednotlivcami alebo subjektmi. V politike koordinovaného zverejňovania informácií o zraniteľnosti by sa mal špecifikovať štruktúrovaný proces, v rámci ktorého sa zraniteľnosti oznamujú výrobcovi takým spôsobom, ktorým sa danému výrobcovi umožňuje diagnostikovať a napraviť takéto zraniteľnosti pred tým, ako sa podrobné informácie o zraniteľnosti poskytnú tretím stranám alebo verejnosti. Vzhľadom na skutočnosť, že informácie o zneužiteľných zraniteľnostiach v bežne používaných produktoch s digitálnymi prvkami sa môžu predávať na čiernom trhu za vysoké ceny, výrobcovia takýchto produktov by mali mať možnosť používať ako súčasť svojich politík koordinovaného zverejňovania informácií o zraniteľnostiach programy na stimulovanie oznamovania zraniteľností tým, že zaistia, aby jednotlivci alebo subjekty dostali uznanie a odmenu za svoje úsilie (tzv. programy odmeňovania za nájdenie chýb).

(37) Výrobcovia by na uľahčenie analýzy zraniteľnosti mali identifikovať a zdokumentovať komponenty obsiahnuté v produktoch s digitálnymi prvkami, a to aj vypracovaním softvérového kusovníka. Softvérový kusovník môže poskytnúť tým, ktorí vyrábajú, kupujú a prevádzkujú softvér, informácie zlepšujúce ich chápanie dodávateľského reťazca, čo má viacero prínosov, predovšetkým pomáha výrobcom a používateľom sledovať známe novovzniknuté zraniteľnosti a riziká. Pre výrobcov má osobitný význam zabezpečiť, aby ich produkty neobsahovali zraniteľné komponenty vyvinuté tretími stranami.

(38) Na uľahčenie posudzovania zhody s požiadavkami stanovenými v tomto nariadení by mal existovať predpoklad zhody v prípade produktov s digitálnymi prvkami, ktoré sú v

zhode s harmonizovanými normami, v ktorých sú základné požiadavky tohto nariadenia premietnuté do podrobných technických špecifikácií a ktoré sú prijaté v súlade s nariadením Európskeho parlamentu a Rady (EÚ) č. 1025/2012[17]. V nariadení (EÚ) č. 1025/2012 sa stanovuje postup týkajúci sa námietok voči harmonizovaným normám, keď tieto normy nespĺňajú v plnej miere požiadavky tohto nariadenia.

(39) Nariadením (EÚ) 2019/881 sa ustanovuje dobrovoľný európsky rámec certifikácie kybernetickej bezpečnosti pre produkty, procesy a služby IKT. Európske systémy certifikácie kybernetickej bezpečnosti sa môžu vzťahovať na produkty s digitálnymi prvkami, na ktoré sa vzťahuje toto nariadenie. Týmto nariadením by sa mala vytvoriť synergia s nariadením (EÚ) 2019/881. Na uľahčenie posudzovania zhody s požiadavkami stanovenými v tomto nariadení sa predpokladá, že produkty s digitálnymi prvkami, ktoré sú certifikované alebo pre ktoré bolo vydané vyhlásenie o zhode v rámci systému kybernetickej bezpečnosti podľa nariadenia (EÚ) 2019/881 a ktorý bol Komisiou identifikovaný vo vykonávacom akte, sú v súlade so základnými požiadavkami tohto nariadenia, pokiaľ sa certifikát kybernetickej bezpečnosti alebo vyhlásenie o zhode alebo ich časti na tieto požiadavky vzťahujú. Potreba nových európskych systémov certifikácie kybernetickej bezpečnosti pre produkty s digitálnymi prvkami by sa mala posúdiť na základe tohto nariadenia. Takéto budúce európske systémy certifikácie kybernetickej bezpečnosti vzťahujúce sa na produkty s digitálnymi prvkami by mali zohľadňovať základné požiadavky stanovené v tomto nariadení a uľahčovať dodržanie súladu s týmto nariadením. Komisia by mala mať právomoc prostredníctvom vykonávacích aktov špecifikovať európske systémy certifikácie kybernetickej bezpečnosti, ktoré sa môžu používať na preukázanie zhody so základnými požiadavkami stanovenými v tomto nariadení. V záujme vyhnutia sa prípadnému neprimeranému administratívnemu zaťaženiu výrobcov by Komisia mala navyše špecifikovať, či certifikát kybernetickej bezpečnosti vydaný v rámci takýchto európskych systémov certifikácie kybernetickej bezpečnosti ruší povinnosť výrobcov vykonať posúdenie zhody treťou stranou, ako to stanovuje toto nariadenie pri zodpovedajúcich požiadavkách.

(40) Po nadobudnutí účinnosti vykonávacieho aktu, ktorým sa stanovuje [vykonávacie nariadenie Komisie (EÚ) č. .../... z XXX o európskom systéme certifikácie kybernetickej bezpečnosti založenom na spoločných kritériách] (EUCC), ktorý sa týka hardvérových produktov, na ktoré sa vzťahuje toto nariadenie, napr. hardvérové bezpečnostné moduly a mikroprocesory, môže Komisia prostredníctvom vykonávacieho aktu špecifikovať, ako sa v systéme EUCC zabezpečí predpoklad zhody so základnými požiadavkami uvedenými v prílohe I k tomuto nariadeniu alebo s ich časťami. Okrem toho sa môže v takomto vykonávacom akte špecifikovať, akým spôsobom certifikát vydaný v rámci systému EUCC ruší povinnosť výrobcov dať vykonať posúdenie tretej strane, ako sa vyžaduje v tomto nariadení pri zodpovedajúcich požiadavkách.

(41) Ak nie sú prijaté žiadne harmonizované normy alebo ak sa v harmonizovaných normách dostatočne neriešia základné požiadavky tohto nariadenia, Komisia by mala mať možnosť prostredníctvom vykonávacích aktov prijať spoločné špecifikácie.

[17] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1025/2012 z 25. októbra 2012 o európskej normalizácii, ktorým sa menia a dopĺňajú smernice Rady 89/686/EHS a 93/15/EHS a smernice Európskeho 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 ktorým sa zrušuje rozhodnutie Rady 87/95/EHS a rozhodnutie Európskeho parlamentu a Rady č. 1673/2006/ES (Ú. v. EÚ L 316, 14.11.2012, s. 12).

K dôvodom na vypracovanie takýchto spoločných špecifikácií namiesto spoliehania sa na harmonizované normy by mohlo patriť zamietnutie mandátu na tvorbu normy ktoroukoľvek z európskych normalizačných organizácií, zbytočné prieťahy pri zavádzaní príslušných harmonizovaných noriem alebo nesúlad vypracovaných noriem s požiadavkami tohto nariadenia alebo so žiadosťou Komisie. Na uľahčenie posudzovania zhody so základnými požiadavkami stanovenými v tomto nariadení by mal existovať predpoklad zhody pre produkty s digitálnymi prvkami, ktoré sú v súlade so spoločnými špecifikáciami prijatými Komisiou podľa tohto nariadenia na účely vyjadrenia podrobných technických špecifikácií týchto požiadaviek.

(42) Výrobcovia by mali vypracovať EÚ vyhlásenie o zhode a poskytnúť tak informácie požadované podľa tohto nariadenia o zhode produktov s digitálnymi prvkami so základnými požiadavkami tohto nariadenia a prípadne iných relevantných harmonizačných právnych predpisov Únie, ktoré sa vzťahujú na produkt. Od výrobcov sa môže vypracovanie EÚ vyhlásenia o zhode vyžadovať aj v iných právnych predpisoch Únie. Na zabezpečenie účinného prístupu k informáciám na účely dohľadu nad trhom by sa malo vypracovať jediné EÚ vyhlásenie o zhode, pokiaľ ide o súlad so všetkými príslušnými aktmi Únie. V záujme zníženia administratívneho zaťaženia hospodárskych subjektov by sa malo umožniť, aby toto jediné EÚ vyhlásenie o zhode tvoril súbor pozostávajúci z príslušných jednotlivých vyhlásení o zhode.

(43) Označenie CE, ktorým sa preukazuje zhoda výrobku, je viditeľným výsledkom celého procesu posudzovania zhody v širokom zmysle. Všeobecné zásady, ktorými sa riadi označenie CE, sú uvedené v nariadení Európskeho parlamentu a Rady (ES) č. 765/2008[18]. Pravidlá umiestňovania označenia CE na produkty s digitálnymi prvkami by sa mali stanoviť v tomto nariadení. Označenie CE by malo byť jediným označením, ktoré zaručuje zhodu produktov s digitálnymi prvkami s požiadavkami tohto nariadenia.

(44) S cieľom umožniť hospodárskym subjektom preukázať zhodu so základnými požiadavkami stanovenými v tomto nariadení a umožniť orgánom dohľadu nad trhom zaistiť, aby produkty s digitálnymi prvkami sprístupnené na trhu spĺňali tieto požiadavky, je potrebné stanoviť postupy posudzovania zhody. Rozhodnutím Európskeho parlamentu a Rady č. 768/2008/ES[19] sa stanovujú moduly pre postupy posudzovania zhody úmerne k úrovni možného rizika a úrovni požadovanej bezpečnosti. V snahe o zaistenie medziodvetvovej súdržnosti a vyhnutie sa *ad hoc* variantom boli postupy posudzovania zhody vhodné na overovanie zhody produktov s digitálnymi prvkami so základnými požiadavkami stanovenými v tomto nariadení založené na týchto moduloch. Postupmi posudzovania zhody by sa mali preskúmať a overiť požiadavky týkajúce sa produktu aj procesu, ktoré sa vzťahujú na celý životný cyklus produktov s digitálnymi prvkami vrátane plánovania, návrhu, vývoja alebo výroby, testovania a údržby produktu.

(45) Posudzovanie zhody produktov s digitálnymi prvkami by mal spravidla vykonávať výrobca na vlastnú zodpovednosť podľa postupu založeného na module A rozhodnutia 768/2008/ES. Výrobca by si mal zachovať flexibilitu pri výbere prísnejšieho postupu posudzovania zhody za účasti tretej strany. Ak je produkt klasifikovaný ako kritický

---

[18] Nariadenie Európskeho parlamentu a Rady (ES) č. 765/2008 z 9. júla 2008, ktorým sa stanovujú požiadavky akreditácie a ktorým sa zrušuje nariadenie (EHS) č. 339/93 (Ú. v. EÚ L 218, 13.8.2008, s. 30).

[19] Rozhodnutie Európskeho parlamentu a Rady č. 768/2008/ES z 9. júla 2008 o spoločnom rámci na uvádzanie výrobkov na trh a o zrušení rozhodnutia 93/465/EHS (Ú. v. EÚ L 218, 13.8.2008, s. 82).

produkt triedy I, vyžaduje sa dodatočné uistenie na preukázanie zhody so základnými požiadavkami stanovenými v tomto nariadení. Výrobca by mal uplatniť harmonizované normy, spoločné špecifikácie alebo systémy certifikácie kybernetickej bezpečnosti podľa nariadenia (EÚ) 2019/881, ktoré Komisia identifikovala vo vykonávacom akte, ak chce vykonať posudzovanie zhody na vlastnú zodpovednosť (modul A). Ak výrobca neuplatňuje takéto harmonizované normy, spoločné špecifikácie alebo systémy certifikácie kybernetickej bezpečnosti, mal by podstúpiť posudzovanie zhody so zapojením tretej strany. Pri zohľadnení administratívneho zaťaženia výrobcov a skutočnosti, že kybernetická bezpečnosť zohráva dôležitú úlohu vo fáze návrhu a vývoja hmotných a nehmotných produktov s digitálnymi prvkami, boli ako najvhodnejšie postupy posudzovania zhody na primerané a účinné posudzovanie zhody kritických produktov s digitálnymi prvkami zvolené postupy posudzovania zhody založené na moduloch B + C alebo module H rozhodnutia 768/2008/ES. Výrobca, ktorý vykonáva posudzovanie zhody treťou stranou, si môže vybrať postup, ktorý najlepšie vyhovuje jeho procesom navrhovania a výroby. Vzhľadom na ešte väčšie kybernetickobezpečnostné riziko spojené s používaním produktov klasifikovaných ako kritické produkty triedy II by sa na posudzovaní zhody mala vždy zúčastniť tretia strana.

(46) Kým pri vytváraní hmotných produktov s digitálnymi prvkami sa od výrobcov obvykle vyžaduje vynaloženie značného úsilia počas fáz návrhu, vývoja a výroby, tvorba produktov s digitálnymi prvkami vo forme softvéru sa takmer výlučne zameriava na návrh a vývoj, zatiaľ čo výrobná fáza zohráva menšiu rolu. Napriek tomu je v mnohých prípadoch stále potrebné pred uvedením na trh softvérové produkty kompilovať, zostaviť, zabaliť, sprístupniť na stiahnutie alebo skopírovať na fyzické médiá. Tieto činnosti by sa mali považovať za činnosti predstavujúce výrobu pri uplatňovaní príslušných modulov posudzovania zhody na overenie súladu produktu so základnými požiadavkami stanovenými v tomto nariadení počas fáz návrhu, vývoja a výroby.

(47) S cieľom vykonávať posudzovanie zhody treťou stranou v prípade produktov s digitálnymi prvkami by vnútroštátne notifikujúce orgány mali Komisii a ostatným členským štátom notifikovať orgány posudzovania zhody za predpokladu, že spĺňajú súbor požiadaviek, najmä pokiaľ ide o nezávislosť, spôsobilosť a neexistenciu konfliktu záujmov.

(48) S cieľom zabezpečiť konzistentnú úroveň kvality výkonu posudzovania zhody produktov s digitálnymi prvkami je takisto potrebné stanoviť požiadavky na notifikujúce orgány a iné orgány zapojené do posudzovania, notifikácie a monitorovania notifikovaných osôb. Systém stanovený v tomto nariadení by sa mal doplniť akreditačným systémom stanoveným v nariadení (ES) č. 765/2008. Keďže akreditácia je základným prostriedkom na overenie odbornej spôsobilosti orgánov posudzovania zhody, mala by sa používať aj na účely notifikácie.

(49) Transparentnú akreditáciu stanovenú v nariadení (ES) č. 765/2008, ktorou sa zabezpečuje potrebná úroveň dôvery v certifikáty zhody, by mali vnútroštátne subjekty verejného sektora v celej Únii považovať za prednostný spôsob preukazovania technickej spôsobilosti orgánov posudzovania zhody. Vnútroštátne orgány sa však môžu domnievať, že majú k dispozícii vhodné prostriedky na to, aby toto hodnotenie uskutočnili samy. V takom prípade by mali v záujme zabezpečenia vhodnej úrovne dôveryhodnosti hodnotenia vykonávaného inými vnútroštátnymi orgánmi poskytnúť Komisii a ostatným členským štátom nevyhnutné listinné dôkazy preukazujúce súlad hodnotených orgánov posudzovania zhody s príslušnými regulačnými požiadavkami.

(50) Orgány posudzovania zhody často zadávajú časť svojich činností spojených s posudzovaním zhody subdodávateľom alebo pomocným orgánom. S cieľom zabezpečiť úroveň ochrany požadovanú v súvislosti s produktmi s digitálnymi prvkami, ktoré sa majú uviesť na trh, je nevyhnutné, aby subdodávatelia a pomocné orgány vykonávajúce posudzovanie zhody spĺňali pri vykonávaní úloh posudzovania zhody rovnaké požiadavky ako notifikované osoby.

(51) Notifikujúci orgán by mal notifikáciu orgánu posudzovania zhody zaslať Komisii a ostatným členským štátom prostredníctvom informačného systému NANDO. NANDO je elektronický nástroj na oznamovanie, ktorý vyvinula a spravuje Komisia a v ktorom sa nachádza zoznam všetkých notifikovaných osôb.

(52) Vzhľadom na to, že notifikované osoby môžu ponúkať svoje služby v celej Únii, je vhodné poskytnúť ostatným členským štátom a Komisii možnosť vzniesť v súvislosti s notifikovanou osobou námietky. Predtým ako začnú orgány posudzovania zhody fungovať ako notifikované osoby, je preto dôležité stanoviť lehotu, počas ktorej možno objasniť akékoľvek pochybnosti alebo obavy, pokiaľ ide o ich odbornú spôsobilosť.

(53) V záujme konkurencieschopnosti je nevyhnutné, aby notifikované osoby uplatňovali postupy posudzovania zhody, ktoré zbytočne nezaťažujú hospodárske subjekty. Z rovnakého dôvodu a s cieľom zaistiť rovnaké zaobchádzanie s hospodárskymi subjektmi je potrebné zabezpečiť konzistentné technické uplatňovanie postupov posudzovania zhody. Najlepšie by sa to malo dosiahnuť prostredníctvom primeranej koordinácie a spolupráce medzi notifikovanými osobami.

(54) Dohľad nad trhom predstavuje nevyhnutný nástroj zaisťovania správneho a jednotného uplatňovania právnych predpisov Únie. Je preto vhodné zaviesť právny rámec, v ktorom sa môže dohľad nad trhom vykonávať primeraným spôsobom. Na produkty s digitálnymi prvkami, na ktoré sa vzťahuje toto nariadenie, sa uplatňujú pravidlá týkajúce sa dohľadu nad trhom a kontroly produktov vstupujúcich na trh Únie, ktoré sú stanovené v nariadení Európskeho parlamentu a Rady (EÚ) 2019/1020[20].

(55) Dohľad nad trhom na území daného členského štátu vykonávajú orgány dohľadu nad trhom v súlade s nariadením (EÚ) 2019/1020. Toto nariadenie by členským štátom nemalo brániť vo výbere príslušných orgánov na vykonávanie uvedených úloh. Každý členský štát by mal určiť na svojom území jeden orgán alebo viac orgánov dohľadu nad trhom. Členské štáty sa môžu rozhodnúť, že určia ktorýkoľvek existujúci alebo nový orgán, aby konal ako orgán dohľadu nad trhom, a to vrátane vnútroštátnych príslušných orgánov uvedených v článku [článok X] smernice [smernica XXX/XXXX (NIS2)] alebo určených vnútroštátnych orgánov pre certifikáciu kybernetickej bezpečnosti uvedených v článku 58 nariadenia (EÚ) 2019/881. Hospodárske subjekty by mali v plnej miere spolupracovať s orgánmi dohľadu nad trhom a s ďalšími príslušnými orgánmi. Každý členský štát by mal oznámiť Komisii a ostatným členským štátom svoje orgány dohľadu nad trhom a oblasti pôsobnosti každého z týchto orgánov a mal by zaistiť potrebné zdroje a zručnosti na vykonávanie úloh dohľadu v súvislosti s týmto nariadením. Podľa článku 10 ods. 2 a 3 nariadenia (EÚ) 2019/1020 by mal každý členský štát vymenovať jednotný úrad pre spoluprácu, ktorý

[20] Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/1020 z 20. júna 2019 o dohľade nad trhom a súlade výrobkov a o zmene smernice 2004/42/ES a nariadení (ES) č. 765/2008 a (EÚ) č. 305/2011 (Ú. v. EÚ L 169, 25.6.2019, s. 1).

by bol zodpovedný okrem iného za to, že zastupuje koordinovanú pozíciu orgánov dohľadu nad trhom a pomáha v rámci spolupráce orgánov dohľadu nad trhom v rôznych členských štátoch.

(56) Na jednotné uplatňovanie tohto nariadenia by sa podľa článku 30 ods. 2 nariadenia (EÚ) 2019/1020 mala zriadiť osobitná skupina pre administratívnu spoluprácu (ADCO). Skupinu ADCO by mali tvoriť zástupcovia určených orgánov dohľadu nad trhom a prípadne zástupcovia jednotných úradov pre spoluprácu. Komisia by mala podporovať a podnecovať spoluprácu medzi orgánmi dohľadu nad trhom prostredníctvom siete Únie pre súlad výrobkov, ktorá bola zriadená na základe článku 29 nariadenia (EÚ) 2019/1020 a ktorá pozostáva zo zástupcov každého členského štátu vrátane zástupcu každého jednotného úradu pre spoluprácu uvedeného v článku 10 nariadenia (EÚ) 2019/1020 a prípadného národného experta, predsedov skupín ADCO a zástupcov z Komisie. Komisia by sa mala zúčastňovať na zasadnutiach siete, jej podskupín a tejto príslušnej skupiny ADCO. Mala by takisto pomáhať tejto skupine ADCO prostredníctvom výkonného sekretariátu, ktorý poskytuje technickú a logistickú podporu.

(57) Na zabezpečenie včasných, primeraných a účinných opatrení týkajúcich sa produktov s digitálnymi prvkami, ktoré predstavujú významné kybernetickobezpečnostné riziko, by sa mal stanoviť ochranný postup Únie, v rámci ktorého sa zainteresované strany informujú o opatreniach, ktoré sa majú prijať v súvislosti s takýmito produktmi. Orgánom dohľadu nad trhom by sa malo takisto umožniť v prípade potreby konať v spolupráci s príslušnými hospodárskymi subjektmi v skoršej fáze. Ak členské štáty a Komisia súhlasia so zdôvodnením opatrenia prijatého členským štátom, nemalo by byť potrebné žiadne ďalšie zapojenie Komisie s výnimkou prípadov, keď nesúlad možno pripísať nedostatkom harmonizovanej normy.

(58) V určitých prípadoch môže produkt s digitálnymi prvkami, ktorý je v súlade s týmto nariadením, napriek tomu predstavovať významné kybernetickobezpečnostné riziko alebo ohrozovať zdravie a bezpečnosť osôb, súlad s povinnosťami podľa práva Únie alebo vnútroštátneho práva určenými na ochranu základných práv, dostupnosť, pravosť, integritu alebo dôvernosť služieb ponúkaných prostredníctvom elektronického informačného systému základnými subjektmi druhu uvedeného v [prílohe I k smernici XXX/XXXX (NIS2)], alebo iné aspekty ochrany verejného záujmu. Preto je potrebné stanoviť pravidlá, ktorými sa zaistí zmiernenie týchto rizík. V dôsledku toho by orgány dohľadu nad trhom mali prijať opatrenia, ktorými by sa od hospodárskeho subjektu vyžadovalo v závislosti od rizika zaistenie stiahnutia produktu od používateľa alebo z trhu, aby už nepredstavoval uvedené riziko. Keď týmto spôsobom orgán dohľadu nad trhom obmedzí alebo zakáže voľný pohyb produktu, členský štát by mal bezodkladne oznámiť predbežné opatrenia Komisii a ostatným členským štátom, pričom uvedie dôvody a opodstatnenie rozhodnutia. Ak orgán dohľadu nad trhom prijme takéto opatrenia proti produktom predstavujúcim riziko, Komisia by mala bezodkladne začať konzultácie s členskými štátmi a príslušným hospodárskym subjektom alebo hospodárskymi subjektmi a mala by vyhodnotiť dané vnútroštátne opatrenie. Na základe výsledkov tohto hodnotenia by Komisia mala rozhodnúť, či vnútroštátne opatrenie je alebo nie je opodstatnené. Komisia by mala svoje rozhodnutie adresovať všetkým členským štátom a okamžite ho oznámiť týmto členským štátom a príslušnému hospodárskemu subjektu či hospodárskym subjektom. Ak sa opatrenie považuje za opodstatnené, Komisia môže zvážiť aj prijatie návrhov na revíziu príslušných právnych predpisov Únie.

(59) V prípade produktov s digitálnymi prvkami, ktoré predstavujú významné kybernetickobezpečnostné riziko, a ak existuje dôvod domnievať sa, že nie sú v súlade s týmto nariadením, alebo v prípade produktov, ktoré nie sú v súlade s týmto nariadením, ale predstavujú iné významné riziká, napríklad ohrozenie zdravia alebo bezpečnosti osôb, základných práv alebo poskytovania služieb základnými subjektmi druhu uvedeného v [prílohe I k smernici XXX/XXXX (NIS2)], môže Komisia požiadať agentúru ENISA o vykonanie hodnotenia. Na základe tohto hodnotenia môže Komisia prostredníctvom vykonávacích aktov prijať nápravné alebo reštriktívne opatrenia na úrovni Únie vrátane príkazu na stiahnutie príslušných produktov z trhu alebo od používateľov v primeranej lehote úmernej charakteru rizika. Komisia môže využiť takýto zásah len za mimoriadnych okolností, ktoré opodstatňujú okamžitý zásah s cieľom zachovať riadne fungovanie vnútorného trhu, a len vtedy, ak orgány dohľadu neprijali na nápravu situácie žiadne účinné opatrenia. Takýmito mimoriadnymi okolnosťami môžu byť núdzové situácie, keď napríklad výrobca rozsiahlo sprístupňuje vo viacerých členských štátoch nevyhovujúci produkt, ktorý používajú aj subjekty v kľúčových odvetviach v rámci rozsahu pôsobnosti [smernice XXX/XXXX (NIS2)], i keď obsahuje známe zraniteľnosti, ktoré zneužívajú škodlivé subjekty a na ktoré výrobca neposkytuje dostupné záplaty. Komisia môže v takýchto núdzových situáciách zasiahnuť len počas trvania mimoriadnych okolností a ak pretrváva nesúlad s týmto nariadením alebo prezentované významné riziká.

(60) V prípadoch, keď existujú náznaky nesúladu s týmto nariadením vo viacerých členských štátoch, orgány dohľadu nad trhom by mali mať možnosť vykonávať spoločné činnosti s ostatnými orgánmi s cieľom overiť dodržiavanie súladu a identifikovať kybernetickobezpečnostné riziká produktov s digitálnymi prvkami.

(61) Bezpečnosť produktov môžu ďalej zvýšiť súbežné koordinované kontrolné akcie (ďalej len „kontrolné akcie“), ktoré sú osobitnými opatreniami orgánov dohľadu nad trhom na presadzovanie práva. Kontrolné akcie by sa mali vykonávať najmä vtedy, keď z trhových trendov, sťažností spotrebiteľov alebo iných náznakov vyplýva, že pri určitých kategóriách produktov sa často zisťuje, že predstavujú kybernetickobezpečnostné riziká. Agentúra ENISA by mala orgánom dohľadu nad trhom predložiť návrhy kategórií produktov, v prípade ktorých by sa mohli organizovať kontrolné akcie okrem iného na základe prijatých oznámení o zraniteľnostiach produktov a incidentoch.

(62) S cieľom zaistiť, aby sa regulačný rámec mohol v prípade potreby prispôsobiť, mala by sa na Komisiu delegovať právomoc prijímať akty v súlade s článkom 290 zmluvy v súvislosti s aktualizáciami zoznamu kritických produktov v prílohe III a so spresnením vymedzenia týchto kategórií produktov. Právomoc prijímať akty v súlade s uvedeným článkom by sa mala na Komisiu delegovať s cieľom identifikovať produkty s digitálnymi prvkami, na ktoré sa vzťahujú iné pravidlá Únie, ktorými sa dosahuje rovnaká úroveň ochrany ako týmto nariadením, pričom sa špecifikuje, či by bolo potrebné obmedzenie alebo vylúčenie z rozsahu pôsobnosti tohto nariadenia, ako aj prípadný rozsah uvedeného obmedzenia. Právomoc prijímať akty v súlade s uvedeným článkom by sa mala delegovať na Komisiu aj v súvislosti s možným poverením týkajúcim sa certifikácie určitých vysokokritických produktov s digitálnymi prvkami na základe kritérií kritickosti stanovených v tomto nariadení, ako aj na špecifikovanie minimálneho obsahu EÚ vyhlásenia o zhode a na doplnenie prvkov, ktoré sa majú zahrnúť do technickej dokumentácie. Je osobitne dôležité, aby Komisia počas prípravných prác uskutočnila príslušné konzultácie, a to aj na úrovni expertov, a aby tieto konzultácie vykonávala v súlade so zásadami stanovenými

v Medziinštitucionálnej dohode z 13. apríla 2016 o lepšej tvorbe práva[21]. Predovšetkým v záujme rovnakého zastúpenia pri príprave delegovaných aktov sa všetky dokumenty doručujú Európskemu parlamentu a Rade v rovnakom čase ako expertom z členských štátov a experti Európskeho parlamentu a Rady majú systematicky prístup na zasadnutia skupín expertov Komisie, ktoré sa zaoberajú prípravou delegovaných aktov.

(63) V záujme zaistenia jednotných podmienok na vykonávanie tohto nariadenia by sa mali na Komisiu preniesť vykonávacie právomoci s cieľom: špecifikovať formát a prvky softvérového kusovníka, ďalej špecifikovať druh informácií, formát a postup predkladania oznamov o aktívne zneužívaných zraniteľnostiach a incidentoch, ktoré výrobcovia predkladajú agentúre ENISA, špecifikovať európske systémy certifikácie kybernetickej bezpečnosti prijaté podľa nariadenia (EÚ) 2019/881, ktoré možno použiť na preukázanie zhody so základnými požiadavkami alebo ich časťami, ako sa uvádza v prílohe I k tomuto nariadeniu, prijať spoločné špecifikácie v súvislosti so základnými požiadavkami uvedenými v prílohe I, stanoviť technické špecifikácie pre piktogramy alebo akékoľvek iné značky týkajúce sa zabezpečenia produktov s digitálnymi prvkami a mechanizmy na podporu ich používania, rozhodovať o nápravných a reštriktívnych opatreniach na úrovni Únie za mimoriadnych okolností, ktoré odôvodňujú okamžitý zásah na zachovanie riadneho fungovania vnútorného trhu. Tieto právomoci by sa mali vykonávať v súlade s nariadením Európskeho parlamentu a Rady (EÚ) č. 182/2011[22].

(64) Na zabezpečenie dôveryhodnej a konštruktívnej spolupráce orgánov dohľadu nad trhom na úrovni Únie a na vnútroštátnej úrovni by mali všetky strany zapojené do uplatňovania tohto nariadenia rešpektovať dôvernosť informácií a údajov získaných pri plnení svojich úloh.

(65) V záujme zabezpečenia účinného presadzovania povinností stanovených v tomto nariadení by každý orgán dohľadu nad trhom mal mať právomoc uložiť alebo požiadať o uloženie správnych pokút. Mali by sa preto zaviesť maximálne úrovne správnych pokút, ktoré sa majú stanoviť vo vnútroštátnych právnych predpisoch za nesplnenie povinností stanovených v tomto nariadení. Pri rozhodovaní o výške správnej pokuty v každom jednotlivom prípade by sa mali zohľadniť všetky relevantné okolnosti konkrétnej situácie a minimálne tie, ktoré sú výslovne uvedené v tomto nariadení vrátane toho, či už tomu istému hospodárskemu subjektu uložili iné orgány dohľadu nad trhom správne poplatky za podobné porušenia. Takéto okolnosti môžu byť buď zhoršujúce v situáciách, keď porušenie tým istým hospodárskym subjektom pretrváva na území iných členských štátov, než je členský štát, v ktorom už bola uložená správna pokuta, alebo zmierňujúce, pričom sa zaistí, aby sa pri každej ďalšej správnej pokute, ktorú zvažuje iný orgán dohľadu nad trhom pre ten istý hospodársky subjekt alebo ten istý druh porušenia, už zohľadnila spolu s ostatnými relevantnými osobitnými okolnosťami pokuta a jej výška uložená v iných členských štátoch. Vo všetkých takýchto prípadoch by sa súhrnnou správnou pokutou, ktorú by mohli orgány dohľadu nad trhom z viacerých členských štátov uložiť tomu istému hospodárskemu subjektu za rovnaký druh porušenia, malo zaistiť dodržanie zásady proporcionality.

---

[21] Ú. v. EÚ L 123, 12.5.2016, s. 1.

[22] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 182/2011 zo 16. februára 2011, ktorým sa ustanovujú pravidlá a všeobecné zásady mechanizmu, na základe ktorého členské štáty kontrolujú vykonávanie vykonávacích právomocí Komisie (Ú. v. EÚ L 55, 28.2.2011, s. 13).

(66) Ak sa správne pokuty ukladajú osobám, ktoré nie sú podnikom, príslušný orgán by mal pri rozhodovaní o primeranej výške pokuty zohľadniť všeobecnú úroveň príjmov v členskom štáte, ako aj majetkové pomery danej osoby. Členské štáty by mali určiť, či a do akej miery by orgány verejnej moci mali podliehať správnym pokutám.

(67) Vo svojich vzťahoch s tretími krajinami sa EÚ snaží podporovať medzinárodný obchod s regulovanými výrobkami. Na uľahčenie obchodu sa môže uplatniť široká paleta opatrení vrátane viacerých právnych nástrojov, ako sú dvojstranné (medzivládne) dohody o vzájomnom uznávaní týkajúcom sa posudzovania zhody a označovania regulovaných produktov. Dohody o vzájomnom uznávaní sa uzatvárajú medzi Úniou a tretími krajinami, ktoré sú na porovnateľnej úrovni technického rozvoja a majú kompatibilný prístup, pokiaľ ide o posudzovanie zhody. Tieto dohody sú založené na vzájomnom uznávaní certifikátov, označení zhody a protokolov o skúškach vydaných orgánmi posudzovania zhody každej strany v súlade s právnymi predpismi druhej strany. V súčasnosti sú dohody o vzájomnom uznávaní zavedené v niekoľkých krajinách. Tieto dohody sú uzatvorené v mnohých špecifických odvetviach, ktoré sa môžu v závislosti od jednotlivých krajín líšiť. Na ďalšie uľahčenie obchodu a vzhľadom na to, že dodávateľské reťazce produktov s digitálnymi prvkami sú celosvetové, môže Únia v súlade s článkom 218 ZFEÚ uzatvoriť dohody o vzájomnom uznávaní týkajúce sa posudzovania zhody pre produkty regulované podľa tohto nariadenia. Dôležitá je aj spolupráca s partnerskými krajinami s cieľom celosvetovo posilniť kybernetickú odolnosť, keďže z dlhodobého hľadiska to prispeje k posilnenému rámcu kybernetickej bezpečnosti v EÚ aj mimo nej.

(68) Komisia by mala toto nariadenie pravidelne preskúmavať a radiť sa pritom so zainteresovanými stranami najmä s cieľom určiť, či ho treba zmeniť na základe zmien spoločenských, politických, technologických alebo trhových podmienok.

(69) Hospodárskym subjektom by sa mal poskytnúť dostatočný čas na prispôsobenie sa požiadavkám stanoveným v tomto nariadení. Toto nariadenie by sa malo uplatňovať [24 mesiacov] od nadobudnutia jeho účinnosti s výnimkou oznamovacích povinností týkajúcich sa aktívne zneužívaných zraniteľností a incidentov, ktoré by sa mali uplatňovať [12 mesiacov] od nadobudnutia účinnosti tohto nariadenia.

(70) Keďže cieľ tohto nariadenia nie je možné uspokojivo dosiahnuť na úrovni samotných členských štátov, ale z dôvodu dôsledkov činnosti ho možno lepšie dosiahnuť na úrovni Únie, môže Únia prijať opatrenia v súlade so zásadou subsidiarity podľa článku 5 Zmluvy o Európskej únii. V súlade so zásadou proporcionality podľa uvedeného článku toto nariadenie neprekračuje rámec nevyhnutný na dosiahnutie uvedeného cieľa.

(71) V súlade s článkom 42 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725[23] sa uskutočnili konzultácie s európskym dozorným úradníkom pre ochranu údajov, ktorý doručil svoje stanovisko […],

[23] Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39).

PRIJALI TOTO NARIADENIE:

KAPITOLA I

VŠEOBECNÉ USTANOVENIA

Článok 1

Predmet úpravy

V tomto nariadení sa stanovujú:

a) pravidlá uvádzania produktov s digitálnymi prvkami na trh s cieľom zaistiť kybernetickú bezpečnosť takýchto produktov;

b) základné požiadavky na návrh, vývoj a výrobu produktov s digitálnymi prvkami a povinnosti hospodárskych subjektov v súvislosti s týmito produktmi, pokiaľ ide o kybernetickú bezpečnosť;

c) základné požiadavky na procesy riešenia zraniteľností zavedené výrobcami s cieľom zaistiť kybernetickú bezpečnosť produktov s digitálnymi prvkami počas celého životného cyklu, a povinnosti hospodárskych subjektov v súvislosti s týmito procesmi;

d) pravidlá dohľadu nad trhom a presadzovanie vyššie uvedených pravidiel a požiadaviek.

Článok 2

Rozsah pôsobnosti

1. Toto nariadenie sa uplatňuje na všetky produkty s digitálnymi prvkami, ktorých zamýšľané alebo odôvodnene predvídateľné použitie zahŕňa priame alebo nepriame logické alebo fyzické dátové pripojenie k zariadeniu alebo sieti.

2. Toto nariadenie sa neuplatňuje na produkty s digitálnymi prvkami, na ktoré sa uplatňujú tieto akty Únie:

   a) nariadenie (EÚ) 2017/745;

   b) nariadenie (EÚ) 2017/746;

   c) nariadenie (EÚ) 2019/2144.

3. Toto nariadenie sa neuplatňuje na produkty s digitálnymi prvkami, ktoré boli certifikované v súlade s nariadením (EÚ) 2018/1139.

4. Uplatňovanie tohto nariadenia na produkty s digitálnymi prvkami, na ktoré sa vzťahujú iné pravidlá Únie stanovujúce požiadavky, ktoré sa týkajú všetkých alebo niektorých rizík, na ktoré sa vzťahujú základné požiadavky uvedené v prílohe I, sa môže obmedziť alebo vylúčiť, ak:

   a) je takéto obmedzenie alebo vylúčenie v súlade s celkovým regulačným rámcom, ktorý sa na tieto produkty uplatňuje, a

   b) sektorovými pravidlami sa dosahuje rovnaká úroveň ochrany, ako je úroveň stanovená v tomto nariadení.

Komisia je v súlade s článkom 50 splnomocnená prijímať delegované akty s cieľom zmeniť toto nariadenie, pričom špecifikuje, či je takéto obmedzenie alebo vylúčenie potrebné a uvedie dotknuté produkty a pravidlá, ako aj prípadný rozsah obmedzenia.

5. Toto nariadenie sa neuplatňuje na produkty s digitálnymi prvkami vyvinuté výlučne na účely národnej bezpečnosti alebo na vojenské účely alebo na produkty osobitne určené na spracúvanie utajovaných skutočností.

Článok 3

Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňuje toto vymedzenie pojmov:

1. „produkt s digitálnymi prvkami“ je akýkoľvek softvérový alebo hardvérový produkt a jeho riešenia diaľkového spracovania údajov vrátane softvérových alebo hardvérových komponentov, ktoré sa majú uviesť na trh samostatne;

2. „diaľkové spracovanie údajov“ je akékoľvek spracovanie údajov na diaľku, pre ktoré je softvér navrhnutý a vyvinutý výrobcom alebo na zodpovednosť výrobcu a ktorého neexistencia by bránila produktu s digitálnymi prvkami plniť jednu z jeho funkcií;

3. „kritický produkt s digitálnymi prvkami“ je produkt s digitálnymi prvkami, ktorý predstavuje kybernetickobezpečnostné riziko v súlade s kritériami stanovenými v článku 6 ods. 2 a ktorého hlavná funkcia je stanovená v prílohe III;

4. „vysokokritický produkt s digitálnymi prvkami“ je produkt s digitálnymi prvkami, ktorý predstavuje kybernetickobezpečnostné riziko v súlade s kritériami stanovenými v článku 6 ods. 5;

5. „operačná technológia“ sú programovateľné digitálne systémy alebo zariadenia, ktoré interagujú s fyzickým prostredím alebo riadia zariadenia, ktoré interagujú s fyzickým prostredím;

6. „softvér“ je časť elektronického informačného systému, ktorý pozostáva z počítačového kódu;

7. „hardvér“ je fyzický elektronický informačný systém alebo jeho časti so schopnosťou spracúvať, uchovávať alebo prenášať digitálne údaje;

8. „komponent“ je softvér alebo hardvér určený na integráciu do elektronického informačného systému;

9. „elektronický informačný systém“ je akýkoľvek systém vrátane elektrických alebo elektronických zariadení, ktorý je schopný spracúvať, uchovávať alebo prenášať digitálne údaje;

10. „logické pripojenie“ je virtuálna forma dátového spojenia realizovaná prostredníctvom softvérového rozhrania;

11. „fyzické pripojenie“ je akékoľvek spojenie medzi elektronickými informačnými systémami alebo komponentmi realizované s použitím fyzických prostriedkov vrátane elektrických alebo mechanických rozhraní, vodičov alebo rádiových vĺn;

12. „nepriame pripojenie“ je pripojenie k zariadeniu alebo sieti, ktoré sa nevykonáva priamo, ale skôr ako súčasť väčšieho systému, ktorý je priamo pripojiteľný k takémuto zariadeniu alebo sieti;

13. „privilégium“ je prístupové právo udelené konkrétnym používateľom alebo programom na vykonávanie operácií súvisiacich s bezpečnosťou v rámci elektronického informačného systému;

14. „vyššie privilégium“ je prístupové právo udelené konkrétnym používateľom alebo programom na vykonávanie rozšíreného súboru operácií súvisiacich s bezpečnosťou v rámci elektronického informačného systému, ktoré by v prípade zneužitia alebo vyzradenia mohlo umožniť škodlivému subjektu získať širší prístup k zdrojom systému alebo organizácie;

15. „koncový bod“ je akékoľvek zariadenie, ktoré je pripojené k sieti a slúži ako vstupný bod do danej siete;

16. „sieťové alebo výpočtové zdroje“ sú dátové alebo hardvérové alebo softvérové funkcie, ktoré sú prístupné buď lokálne, alebo prostredníctvom siete alebo iného pripojeného zariadenia;

17. „hospodársky subjekt“ je výrobca, splnomocnený zástupca, dovozca, distribútor alebo akákoľvek iná fyzická alebo právnická osoba, na ktorú sa vzťahujú povinnosti stanovené týmto nariadením;

18. „výrobca“ je každá fyzická alebo právnická osoba, ktorá vyvíja alebo vyrába produkty s digitálnymi prvkami, alebo si dáva navrhnúť, vyvinúť alebo vyrobiť produkty s digitálnymi prvkami a predáva ich pod svojím menom alebo svojou ochrannou známkou, či už za odplatu alebo bezodplatne;

19. „splnomocnený zástupca“ je každá fyzická alebo právnická osoba usadená v Únii, ktorá dostala písomné poverenie od výrobcu konať v jeho mene v súvislosti s konkrétnymi úlohami;

20. „dovozca“ je každá fyzická alebo právnická osoba usadená v Únii, ktorá uvádza na trh produkt s digitálnymi prvkami označený menom alebo ochrannou známkou fyzickej alebo právnickej osoby usadenej mimo Únie;

21. „distribútor“ je každá fyzická alebo právnická osoba v dodávateľskom reťazci okrem výrobcu alebo dovozcu, ktorá na trhu Únie sprístupňuje produkt s digitálnymi prvkami bez toho, aby ovplyvňovala jeho vlastnosti;

22. „uvedenie na trh“ je prvé sprístupnenie produktu s digitálnymi prvkami na trhu Únie;

23. „sprístupnenie na trhu“ je každá dodávka produktu s digitálnymi prvkami na distribúciu alebo použitie na trhu Únie v rámci obchodnej činnosti, či už za odplatu alebo bezodplatne;

24. „zamýšľaný účel“ je použitie produktu s digitálnymi prvkami, ktoré určil výrobca, vrátane osobitného kontextu a podmienok používania, ako sa uvádza v informáciách od výrobcu v návode na použitie, v propagačných alebo predajných materiáloch a vyhláseniach, ako aj v technickej dokumentácii;

25. „odôvodnene predvídateľné použitie“ je použitie, ktoré nemusí byť nevyhnutne zamýšľaným účelom, ktorý výrobca uvádza v návode na použitie, v propagačných alebo predajných materiáloch a vyhláseniach, ako aj v technickej dokumentácii, ale ktoré pravdepodobne vyplynie z odôvodnene predvídateľného ľudského správania alebo technických operácií či interakcií;

26. „odôvodnene predvídateľné nesprávne použitie“ je použitie produktu s digitálnymi prvkami, ktoré nie je v súlade so zamýšľaným účelom, ale ktoré môže vyplynúť

z odôvodnene predvídateľného ľudského správania alebo interakcie s inými systémami;

27. „notifikujúci orgán“ je vnútroštátny orgán zodpovedný za stanovenie a vykonávanie nevyhnutných postupov na posudzovanie, určovanie a notifikáciu orgánov posudzovania zhody a za ich monitorovanie;

28. „posudzovanie zhody“ je postup, ktorým sa overuje, či boli splnené základné požiadavky uvedené v prílohe I;

29. „orgán posudzovania zhody“ je orgán vymedzený v článku 2 bode 13 nariadenia (ES) č. 765/2008;

30. „notifikovaná osoba“ je orgán posudzovania zhody určený v súlade s článkom 33 tohto nariadenia a inými relevantnými harmonizačnými právnymi predpismi Únie;

31. „podstatná úprava“ je zmena produktu s digitálnymi prvkami po jeho uvedení na trh, ktorá ovplyvňuje súlad produktu s digitálnymi prvkami so základnými požiadavkami uvedenými v oddiele 1 prílohy I alebo ktorá vedie k úprave zamýšľaného použitia, pre ktoré bol produkt s digitálnymi prvkami posudzovaný;

32. „označenie CE“ je označenie, ktorým výrobca vyjadruje, že produkt s digitálnymi prvkami a procesy zavedené výrobcom sú v súlade so základnými požiadavkami uvedenými v prílohe I a s inými uplatniteľnými právnymi predpismi Únie, ktorými sa harmonizujú podmienky uvádzania produktov na trh (ďalej len „harmonizačné právne predpisy Únie“), ktoré stanovujú umiestnenie tohto označenia;

33. „orgán dohľadu nad trhom“ je orgán vymedzený v článku 3 bode 4 nariadenia (EÚ) 2019/1020;

34. „harmonizovaná norma“ je harmonizovaná norma vymedzená v článku 2 bode 1 písm. c) nariadenia (EÚ) č. 1025/2012;

35. „kybernetickobezpečnostné riziko“ je riziko vymedzené v článku [článok X] smernice [smernica XXX/XXXX (NIS2)];

36. „významné kybernetickobezpečnostné riziko“ je kybernetickobezpečnostné riziko, pri ktorom možno na základe jeho technických charakteristík predpokladať vysokú pravdepodobnosť incidentu, ktorý by mohol viesť k závažnému negatívnemu vplyvu, a to aj spôsobením značnej majetkovej alebo nemajetkovej ujmy či narušenia;

37. „softvérový kusovník“ je formálny záznam obsahujúci podrobnosti a vzťahy v rámci dodávateľského reťazca komponentov zahrnutých v softvérových prvkoch produktu s digitálnymi prvkami;

38. „zraniteľnosť“ je zraniteľnosť vymedzená v článku [článok X] smernice [smernica XXX/XXXX (NIS2)];

39. „aktívne zneužívaná zraniteľnosť“ je zraniteľnosť, v prípade ktorej existuje spoľahlivý dôkaz, že určitý subjekt vykonal v systéme spustenie škodlivého kódu bez povolenia vlastníka systému;

40. „osobné údaje“ sú údaje vymedzené v článku 4 bode 1 nariadenia (EÚ) 2016/679.

Článok 4

Voľný pohyb

1. Členské štáty nesmú v prípade záležitostí, na ktoré sa vzťahuje toto nariadenie, brániť sprístupneniu produktov s digitálnymi prvkami, ktoré sú v súlade s týmto nariadením, na trhu.

2. Na obchodných veľtrhoch, výstavách a predvádzacích akciách alebo podobných podujatiach nesmú členské štáty brániť prezentovaniu a používaniu produktu s digitálnymi prvkami, ktorý nie je v súlade s týmto nariadením.

3. Členské štáty nesmú brániť sprístupneniu nedokončeného softvéru, ktorý nie je v súlade s týmto nariadením, za predpokladu, že softvér sa sprístupní len na obmedzený čas potrebný na účely testovania a že viditeľné označenie jasne uvádza, že nie je v súlade s týmto nariadením a nebude dostupný na trhu na iné účely, než je testovanie.

Článok 5

Požiadavky na produkty s digitálnymi prvkami

Produkty s digitálnymi prvkami sa na trhu sprístupnia, len ak:

1. spĺňajú základné požiadavky uvedené v oddiele 1 prílohy I pod podmienkou, že sú riadne nainštalované, udržiavané, používané na svoj zamýšľaný účel alebo za podmienok, ktoré možno odôvodnene predvídať, a prípadne aktualizované, a

2. procesy zavedené výrobcom sú v súlade so základnými požiadavkami uvedenými v oddiele 2 prílohy I.

Článok 6

Kritické produkty s digitálnymi prvkami

1. Produkty s digitálnymi prvkami, ktoré patria do kategórie, ktorá je uvedená v prílohe III, sa považujú za kritické produkty s digitálnymi prvkami. Produkty, ktoré majú hlavnú funkciu kategórie, ktorá je uvedená v prílohe III k tomuto nariadeniu, sa považujú za produkty patriace do tejto kategórie. Kategórie kritických produktov s digitálnymi prvkami sa rozdeľujú na triedu I a triedu II, ako sa stanovuje v prílohe III, pričom vyjadrujú úroveň kybernetickobezpečnostného rizika týkajúceho sa týchto produktov.

2. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 50 s cieľom zmeniť prílohu III zaradením novej kategórie do zoznamu kategórií kritických produktov s digitálnymi prvkami alebo vypustením existujúcej kategórie z tohto zoznamu. Pri posudzovaní potreby zmeniť zoznam v prílohe III Komisia zohľadňuje úroveň kybernetickobezpečnostného rizika týkajúceho sa kategórie produktov s digitálnymi prvkami. Pri určovaní úrovne kybernetickobezpečnostného rizika sa zohľadňuje jedno alebo viacero z týchto kritérií:

   a) funkcia produktu s digitálnymi prvkami týkajúca sa kybernetickobezpečnostného rizika a to, či produkt s digitálnymi prvkami má aspoň jeden z týchto atribútov:

      i) je určený na činnosť s vyšším privilégiom alebo na spravovanie privilégií;

      ii) má priamy alebo privilegovaný prístup k sieťovým alebo výpočtovým zdrojom;

iii) je navrhnutý na riadenie prístupu k údajom alebo operačnej technológii;

iv) plní funkciu, ktorá je rozhodujúca pre dôveru, najmä bezpečnostné funkcie, ako je riadenie siete, bezpečnosť koncových bodov a ochrana siete;

b) zamýšľané použitie v citlivých prostrediach, a to aj v priemyselných prostrediach, alebo na použitie základnými subjektmi druhu uvedeného v prílohe [príloha I] k smernici [smernica XXX/XXXX (NIS2)];

c) zamýšľané použitie na vykonávanie kritických alebo citlivých funkcií, ako je spracúvanie osobných údajov;

d) potenciálny rozsah nepriaznivého vplyvu, najmä pokiaľ ide o jeho intenzitu a schopnosť zasiahnuť veľký počet osôb;

e) rozsah, v akom použitie produktov s digitálnymi prvkami už spôsobilo majetkovú alebo nemajetkovú ujmu alebo narušenie alebo vzbudilo značné obavy v súvislosti s prejavením sa nepriaznivého vplyvu.

3. Komisia je splnomocnená prijať delegovaný akt v súlade s článkom 50 s cieľom doplniť toto nariadenie, a to špecifikovaním vymedzenia kategórií produktov v rámci triedy I a triedy II, ako sa stanovuje v prílohe III. Delegovaný akt sa prijme [do 12 mesiacov od nadobudnutia účinnosti tohto nariadenia].

4. Kritické produkty s digitálnymi prvkami podliehajú postupom posudzovania zhody uvedeným v článku 24 ods. 2 a 3.

5. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 50 s cieľom doplniť toto nariadenie, a to špecifikovaním kategórií vysokokritických produktov s digitálnymi prvkami, pre ktoré sú výrobcovia povinní získať európsky certifikát kybernetickej bezpečnosti v rámci európskeho systému certifikácie kybernetickej bezpečnosti podľa nariadenia (EÚ) 2019/881 na preukázanie zhody so základnými požiadavkami stanovenými v prílohe I alebo s ich časťami. Pri určovaní takýchto kategórií vysokokritických produktov s digitálnymi prvkami Komisia zohľadňuje úroveň kybernetickobezpečnostného rizika týkajúceho sa kategórie produktov s digitálnymi prvkami vzhľadom na jedno kritérium alebo viacero kritérií uvedených v odseku 2, ako aj v záujme posúdenia toho, či je táto kategória produktov:

a) používaná základnými subjektmi druhu uvedeného v prílohe [príloha I] k smernici [smernica XXX/XXXX (NIS2)] alebo či sa na ňu tieto subjekty spoliehajú, alebo či bude mať potenciálny budúci význam pre činnosti týchto subjektov, alebo či je

b) relevantná z hľadiska odolnosti celého dodávateľského reťazca produktov s digitálnymi prvkami voči rušivým udalostiam.

Článok 7

Všeobecná bezpečnosť výrobkov

Odchylne od článku 2 ods. 1 tretieho pododseku písm. b) nariadenia [nariadenie o všeobecnej bezpečnosti výrobkov], keď produkty s digitálnymi prvkami nepodliehajú osobitným požiadavkám stanoveným v iných harmonizačných právnych predpisoch Únie v zmysle [článku 3 bodu 25 nariadenia o všeobecnej bezpečnosti výrobkov], uplatňujú sa na tieto produkty, pokiaľ ide o bezpečnostné

riziká, na ktoré sa toto nariadenie nevzťahuje, kapitola III oddiel 1, kapitoly V a VII a kapitoly IX až XI nariadenia [nariadenie o všeobecnej bezpečnosti výrobkov].

Článok 8

Vysokorizikové systémy umelej inteligencie

1. Produkty s digitálnymi prvkami klasifikované ako vysokorizikové systémy umelej inteligencie v súlade s článkom [článok 6] nariadenia [nariadenie o umelej inteligencii], ktoré patria do rozsahu pôsobnosti tohto nariadenia a spĺňajú základné požiadavky uvedené v oddiele 1 prílohy I k tomuto nariadeniu, a ak sú procesy zavedené výrobcom v súlade so základnými požiadavkami uvedenými v oddiele 2 prílohy I, sa považujú za produkty v súlade s požiadavkami týkajúcimi sa kybernetickej bezpečnosti stanovenými v článku [článok 15] nariadenia [nariadenie o umelej inteligencii] bez toho, aby boli dotknuté iné požiadavky týkajúce sa presnosti a spoľahlivosti zahrnuté v uvedenom článku, a pokiaľ dosiahnutie úrovne ochrany požadovanej týmito požiadavkami je preukázané EÚ vyhlásením o zhode vydaným podľa tohto nariadenia.

2. V prípade výrobkov a požiadaviek na kybernetickú bezpečnosť uvedených v odseku 1 sa uplatňuje príslušný postup posudzovania zhody, ako sa vyžaduje v článku [článok 43] nariadenia [nariadenie o umelej inteligencii]. Na účely uvedeného posudzovania sú notifikované osoby, ktoré sú oprávnené kontrolovať zhodu vysokorizikových systémov umelej inteligencie podľa nariadenia [nariadenie o umelej inteligencii] oprávnené kontrolovať aj zhodu vysokorizikových systémov umelej inteligencie v rámci rozsahu pôsobnosti tohto nariadenia s požiadavkami uvedenými v prílohe I k tomuto nariadeniu za predpokladu, že súlad týchto notifikovaných osôb s požiadavkami stanovenými v článku 29 tohto nariadenia bol posúdený v kontexte postupu notifikácie podľa nariadenia [nariadenie o umelej inteligencii].

3. Odchylne od odseku 2 kritické produkty s digitálnymi prvkami uvedené v prílohe III k tomuto nariadeniu, pri ktorých sa musia uplatňovať postupy posudzovania zhody uvedené v článku 24 ods. 2 písm. a) a b), článku 24 ods. 3 písm. a) a b) tohto nariadenia a ktoré sú zároveň klasifikované ako vysokorizikové systémy umelej inteligencie podľa článku [článok 6] nariadenia [nariadenie o umelej inteligencii] a na ktoré sa uplatňuje postup posudzovania zhody založený na vnútornej kontrole uvedenej v prílohe [príloha VI] k nariadeniu [nariadenie o umelej inteligencii], podliehajú postupom posudzovania zhody, ako sa vyžaduje v tomto nariadení, pokiaľ ide o základné požiadavky tohto nariadenia.

Článok 9

Strojnícke výrobky

Strojnícke výrobky v rozsahu pôsobnosti nariadenia [návrh nariadenia o strojníckych výrobkoch], ktoré sú v zmysle tohto nariadenia produktmi s digitálnymi prvkami a pre ktoré bolo vydané vyhlásenie o zhode na základe tohto nariadenia, sa považujú za výrobky, ktoré sú v súlade so základnými požiadavkami na ochranu zdravia a bezpečnosť stanovenými v prílohe [príloha III oddiely 1.1.9 a 1.2.1] k nariadeniu [návrh nariadenia o strojníckych výrobkoch], čo sa týka ochrany pred zneužitím a bezpečnosti a spoľahlivosti ovládacích systémov, a pokiaľ je dosiahnutie úrovne

ochrany požadovanej týmito požiadavkami preukázané v EÚ vyhlásení o zhode vydanom podľa tohto nariadenia.

KAPITOLA II

POVINNOSTI HOSPODÁRSKYCH SUBJEKTOV

Článok 10

Povinnosti výrobcov

1. Výrobcovia pri uvádzaní produktu s digitálnymi prvkami na trh zaistia, aby bol navrhnutý, vyvinutý a vyrobený v súlade so základnými požiadavkami uvedenými v oddiele 1 prílohy I.

2. Na účely dodržania povinnosti stanovenej v odseku 1 výrobcovia vykonávajú posúdenie kybernetickobezpečnostných rizík spojených s produktom s digitálnymi prvkami a výsledok tohto posúdenia zohľadňujú počas fáz plánovania, návrhu, vývoja, výroby, dodania a údržby produktu s digitálnymi prvkami s cieľom minimalizovať kybernetickobezpečnostné riziká, predchádzať bezpečnostným incidentom a minimalizovať vplyvy takýchto incidentov, a to aj v súvislosti so zdravím a bezpečnosťou používateľov.

3. Pri uvádzaní produktu s digitálnymi prvkami na trh výrobca zahrnie posudzovanie kybernetickobezpečnostných rizík do technickej dokumentácie, ako sa uvádza v článku 23 a prílohe V. V prípade produktov s digitálnymi prvkami uvedených v článku 8 a článku 24 ods. 4, ktoré podliehajú aj iným aktom Únie, môže byť posudzovanie kybernetickobezpečnostných rizík súčasťou posudzovania rizík vyžadovaného v týchto príslušných aktoch Únie. Ak na produkt s digitálnymi prvkami uvádzaný na trh nemožno uplatniť určité základné požiadavky, výrobca zahrnie do uvedenej dokumentácie jasné odôvodnenie.

4. Na účely splnenia povinnosti stanovenej v odseku 1 výrobcovia pri integrovaní komponentov pochádzajúcich od tretích strán do produktov s digitálnymi prvkami uplatňujú náležitú starostlivosť. Zaistia, aby takéto komponenty neohrozovali bezpečnosť produktu s digitálnymi prvkami.

5. Výrobca systematicky dokumentuje spôsobom, ktorý je primeraný charakteru a kybernetickobezpečnostným rizikám, príslušné aspekty kybernetickej bezpečnosti týkajúce sa produktu s digitálnymi prvkami vrátane zraniteľností, o ktorých sa dozvedel a akýchkoľvek relevantných informácií získaných od tretích strán a prípadne aktualizuje posúdenie rizík produktu.

6. Pri uvádzaní produktu s digitálnymi prvkami na trh a počas predpokladanej životnosti produktu alebo počas piatich rokov od uvedenia produktu na trh, podľa toho, čo je kratšie, výrobcovia zaistia, aby sa zraniteľnosti tohto produktu riešili účinne a v súlade so základnými požiadavkami uvedenými v oddiele 2 prílohy I.

   Výrobcovia majú vhodné politiky a postupy vrátane politík koordinovaného zverejňovania informácií o zraniteľnosti, ktoré sú uvedené v oddiele 2 bode 5 prílohy I, na spracovanie a nápravu možných zraniteľností produktu s digitálnymi prvkami oznámených z interných alebo externých zdrojov.

7. Výrobcovia pred uvedením produktu s digitálnymi prvkami na trh vypracujú technickú dokumentáciu uvedenú v článku 23.

Vykonajú alebo dajú vykonať zvolené postupy posudzovania zhody uvedené v článku 24.

Keď bol súlad produktu s digitálnymi prvkami so základnými požiadavkami uvedenými v oddiele 1 prílohy I a procesov zavedených výrobcom so základnými požiadavkami uvedenými v oddiele 2 prílohy I preukázaný týmto postupom posudzovania zhody, výrobcovia vypracujú EÚ vyhlásenie o zhode v súlade s článkom 20 a umiestnia označenie CE v súlade s článkom 22.

8. Pre potreby orgánov dohľadu nad trhom výrobcovia uchovávajú technickú dokumentáciu a prípadne EÚ vyhlásenie o zhode počas desiatich rokov od uvedenia produktu s digitálnymi prvkami na trh.

9. Výrobcovia zaistia, aby boli zavedené postupy, vďaka ktorým bude v sériovej výrobe zachovaná zhoda produktov s digitálnymi prvkami. Výrobca primerane zohľadní zmeny v procese vývoja a výroby alebo v návrhu či vlastnostiach produktu s digitálnymi prvkami a zmeny v harmonizovaných normách, európskych systémoch certifikácie kybernetickej bezpečnosti alebo spoločných špecifikáciách uvedených v článku 19, na základe ktorých sa zhoda produktu s digitálnymi prvkami vyhlásila alebo ktorých uplatnením sa zhoda overila.

10. Výrobcovia zaistia, aby boli k produktom s digitálnymi prvkami priložené informácie a pokyny uvedené v prílohe II, a to v elektronickej alebo fyzickej forme. Takéto informácie a pokyny musia byť v jazyku, ktorý je pre používateľov ľahko zrozumiteľný. Musia byť jasné, zrozumiteľné, ľahko pochopiteľné a čitateľné. Musia umožniť bezpečnú inštaláciu, prevádzku a používanie produktov s digitálnymi prvkami.

11. Výrobcovia buď poskytnú EÚ vyhlásenie o zhode spolu s produktom s digitálnymi prvkami, alebo v pokynoch a informáciách stanovených v prílohe II uvedú internetovú adresu, na ktorej je EÚ vyhlásenie o zhode k dispozícii.

12. Od uvedenia produktu s digitálnymi prvkami na trh a počas predpokladanej životnosti produktu alebo počas piatich rokov od jeho uvedenia na trh, podľa toho, čo je kratšie, výrobcovia, ktorí vedia alebo majú dôvod domnievať sa, že produkt s digitálnymi prvkami alebo procesy zavedené výrobcom nie sú v súlade so základnými požiadavkami uvedenými v prílohe I, bezodkladne prijmú nápravné opatrenia potrebné na to, aby tento produkt s digitálnymi prvkami alebo procesy výrobcu spĺňali príslušné požiadavky, prípadne na stiahnutie produktu z trhu alebo od používateľa.

13. Výrobcovia poskytnú orgánu dohľadu nad trhom na základe jeho odôvodnenej žiadosti a v jazyku, ktorý je preň ľahko zrozumiteľný, všetky informácie a dokumenty v papierovej alebo elektronickej forme, ktoré sú potrebné na preukázanie zhody produktu s digitálnymi prvkami a procesov zavedených výrobcom so základnými požiadavkami uvedenými v prílohe I. Na žiadosť tohto orgánu s ním spolupracujú pri akýchkoľvek opatreniach prijatých na odstránenie kybernetickobezpečnostných rizík, ktoré predstavuje produkt s digitálnymi prvkami, ktorý uviedli na trh.

14. Výrobca, ktorý ukončí svoju činnosť a v dôsledku toho nie je schopný dodržiavať povinnosti stanovené v tomto nariadení, informuje o tejto situácii ešte pred tým, než toto ukončenie nadobudne platnosť, príslušné orgány dohľadu nad trhom a akýmikoľvek dostupnými prostriedkami a v čo najväčšej možnej miere aj používateľov dotknutých produktov s digitálnymi prvkami uvedených na trh.

15. Komisia môže prostredníctvom vykonávacích aktov špecifikovať formát a prvky softvérového kusovníka stanoveného v oddiele 2 bode 1 prílohy I. Tieto vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 51 ods. 2.

Článok 11

Oznamovacie povinnosti výrobcov

1. Výrobca bez zbytočného odkladu a v každom prípade do 24 hodín od zistenia danej skutočnosti oznámi agentúre ENISA akúkoľvek aktívne zneužívanú zraniteľnosť, ktorú obsahuje produkt s digitálnymi prvkami. Oznámenie musí obsahovať podrobnosti týkajúce sa tejto zraniteľnosti a prípadne akékoľvek prijaté nápravné alebo zmierňujúce opatrenia. Agentúra ENISA bez zbytočného odkladu, pokiaľ nejde o opodstatnené dôvody týkajúce sa kybernetickobezpečnostného rizika, postúpi oznámenie po jeho doručení jednotke CSIRT dotknutých členských štátov, určenej na účely koordinovaného zverejňovania informácií o zraniteľnostiach v súlade s článkom [článok X] smernice [smernica XXX/XXXX (NIS2)], a informuje orgán dohľadu nad trhom o oznámenej zraniteľnosti.

2. Výrobca bez zbytočného odkladu a v každom prípade do 24 hodín od zistenia danej skutočnosti oznámi agentúre ENISA akýkoľvek incident, ktorý má vplyv na bezpečnosť produktu s digitálnymi prvkami. Agentúra ENISA bez zbytočného odkladu, pokiaľ nejde o opodstatnené dôvody týkajúce sa kybernetickobezpečnostného rizika, postúpi oznámenia jednotnému kontaktnému miestu dotknutých členských štátov, určenému v súlade s článkom [článok X] smernice [smernica XXX/XXXX (NIS2)], a informuje orgán dohľadu nad trhom o oznámených incidentoch. Oznámenie incidentu musí obsahovať informácie o závažnosti a vplyve incidentu a prípadne to, či má výrobca podozrenie, že incident bol spôsobený nezákonným alebo škodlivým konaním, alebo či sa domnieva, že má cezhraničný dosah.

3. Agentúra ENISA predloží Európskej sieti styčných organizácií pre kybernetické krízy (EU-CyCLONe) zriadenej článkom [článok X] smernice [smernica XXX/XXXX (NIS2)] informácie oznámené podľa odsekov 1 a 2, ak sú takéto informácie relevantné pre koordinované riadenie rozsiahlych kybernetických bezpečnostných incidentov a kríz na operačnej úrovni.

4. Keď sa výrobca o incidente dozvie, bez zbytočného odkladu o ňom informuje používateľov produktu s digitálnymi prvkami a prípadne aj o nápravných opatreniach, ktoré môže používateľ zaviesť na zmiernenie vplyvu tohto incidentu.

5. Komisia môže prostredníctvom vykonávacích aktov ďalej špecifikovať druh informácií, formát a postup oznámení predkladaných podľa odsekov 1 a 2. Tieto vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 51 ods. 2.

6. Agentúra ENISA na základe oznámení prijatých podľa odsekov 1 a 2 vypracuje každé dva roky technickú správu o vznikajúcich trendoch týkajúcich sa kybernetickobezpečnostných rizík v prípade produktov s digitálnymi prvkami a predloží ju skupine pre spoluprácu uvedenej v článku [článok X] smernice [smernica XXX/XXXX (NIS2)]. Prvá takáto správa sa predloží do 24 mesiacov od začatia uplatňovania povinností stanovených v odsekoch 1 a 2.

7. Výrobcovia po identifikovaní zraniteľnosti komponentu vrátane komponentu s otvoreným zdrojovým kódom, ktorý je integrovaný v produkte s digitálnymi

prvkami, oznámia zraniteľnosť osobe alebo subjektu, ktorý má na starosti údržbu komponentu.

Článok 12

Splnomocnení zástupcovia

1. Výrobca môže písomným poverením vymenovať splnomocneného zástupcu.
2. Povinnosti stanovené v článku 10 ods. 1 až 7 prvej zarážke a ods. 9 nie sú súčasťou poverenia splnomocneného zástupcu.
3. Splnomocnený zástupca vykonáva úlohy uvedené v poverení od výrobcu. Poverenie umožňuje splnomocnenému zástupcovi prinajmenšom:
   a) uchovávať k dispozícii pre orgány dohľadu nad trhom EÚ vyhlásenie o zhode uvedené v článku 20 a technickú dokumentáciu uvedenú v článku 23 počas desiatich rokov od uvedenia produktu s digitálnymi prvkami na trh;
   b) poskytnúť orgánu dohľadu nad trhom na základe jeho odôvodnenej žiadosti všetky informácie a dokumenty potrebné na preukázanie zhody produktu s digitálnymi prvkami;
   c) spolupracovať s orgánmi dohľadu nad trhom na ich žiadosť pri každom prijatom opatrení s cieľom odstrániť riziká, ktoré predstavuje produkt s digitálnymi prvkami, na ktorý sa vzťahuje poverenie splnomocneného zástupcu.

Článok 13

Povinnosti dovozcov

1. Dovozcovia uvádzajú na trh len produkty s digitálnymi prvkami, ktoré spĺňajú základné požiadavky uvedené v oddiele 1 prílohy I, a len ak sú procesy zavedené výrobcom v súlade so základnými požiadavkami uvedenými v oddiele 2 prílohy I.
2. Pred uvedením produktu s digitálnymi prvkami na trh sa dovozcovia uistia, že:
   a) výrobca vykonal náležité postupy posudzovania zhody uvedené v článku 24;
   b) výrobca vypracoval technickú dokumentáciu;
   c) na produkte s digitálnymi prvkami je umiestnené označenie CE uvedené v článku 22 a sú k nemu pripojené informácie a návod na použitie, ako sa stanovuje v prílohe II.
3. Ak sa dovozca domnieva alebo má dôvod sa domnievať, že produkt s digitálnymi prvkami alebo procesy zavedené výrobcom nie sú v zhode so základnými požiadavkami uvedenými v prílohe I, dovozca neuvedie produkt na trh, kým sa v prípade tohto produktu alebo procesov zavedených výrobcom nedosiahne zhoda so základnými požiadavkami uvedenými v prílohe I. Okrem toho, ak produkt s digitálnymi prvkami predstavuje významné kybernetickobezpečnostné riziko, dovozca informuje o tom výrobcu a orgány dohľadu nad trhom.
4. Dovozcovia uvedú buď na produkte s digitálnymi prvkami, alebo ak to nie je možné, na jeho obale alebo v sprievodnej dokumentácii produktu s digitálnymi prvkami svoje meno, registrované obchodné meno alebo zapísanú ochrannú známku, poštovú adresu a e-mailovú adresu, na ktorej sa s nimi možno skontaktovať. Kontaktné údaje

sú v jazyku, ktorý je pre používateľov a orgány dohľadu nad trhom ľahko zrozumiteľný.

5. Dovozcovia zaistia, aby boli k produktu s digitálnymi prvkami pripojené pokyny a informácie uvedené v prílohe II v jazyku, ktorý je pre používateľov ľahko zrozumiteľný.

6. Dovozcovia, ktorí vedia alebo majú dôvod sa domnievať, že produkt s digitálnymi prvkami, ktorý uviedli na trh, alebo procesy zavedené jeho výrobcom nie sú v zhode so základnými požiadavkami uvedenými v prílohe I, bezodkladne prijmú nápravné opatrenia potrebné na to, aby tento produkt s digitálnymi prvkami alebo procesy zavedené jeho výrobcom spĺňali základné požiadavky uvedené v prílohe I, alebo prípadne na stiahnutie produktu z trhu alebo od používateľa.

   Po identifikovaní zraniteľnosti produktu s digitálnymi prvkami dovozcovia bez zbytočného odkladu informujú výrobcu o tejto zraniteľnosti. Okrem toho, ak produkt s digitálnymi prvkami predstavuje významné kybernetickobezpečnostné riziko, dovozcovia o tom bezodkladne informujú orgány dohľadu nad trhom členských štátov, v ktorých produkt s digitálnymi prvkami sprístupnili na trhu, pričom uvedú podrobnosti najmä o nezhode a o všetkých prijatých nápravných opatreniach.

7. Dovozcovia uchovávajú pre orgány dohľadu nad trhom počas desiatich rokov od uvedenia produktu s digitálnymi prvkami na trh k dispozícii kópiu EÚ vyhlásenia o zhode a zaistia, aby bola týmto orgánom na ich žiadosť sprístupnená technická dokumentácia.

8. Dovozcovia poskytnú orgánu dohľadu nad trhom na základe jeho odôvodnenej žiadosti všetky informácie a dokumenty v papierovej alebo elektronickej forme potrebné na preukázanie zhody produktu s digitálnymi prvkami so základnými požiadavkami uvedenými v oddiele 1 prílohy I, ako aj procesov zavedených výrobcom so základnými požiadavkami uvedenými v oddiele 2 prílohy I, a to v jazyku, ktorý je pre tento orgán ľahko zrozumiteľný. Na žiadosť tohto orgánu s ním spolupracujú pri akýchkoľvek opatreniach prijatých na odstránenie kybernetickobezpečnostných rizík, ktoré predstavuje produkt s digitálnymi prvkami, ktorý uviedli na trh.

9. Keď sa dovozca produktu s digitálnymi prvkami dozvie, že výrobca tohto produktu ukončil svoju činnosť a v dôsledku toho nie je schopný splniť povinnosti stanovené v tomto nariadení, dovozca informuje o tejto situácii príslušné orgány dohľadu nad trhom a akýmikoľvek dostupnými prostriedkami a v čo najväčšej možnej miere aj používateľov produktov s digitálnymi prvkami uvedených na trh.

Článok 14

Povinnosti distribútorov

1. Pri sprístupňovaní produktu s digitálnymi prvkami na trhu distribútori konajú s náležitou starostlivosťou vo vzťahu k požiadavkám stanoveným v tomto nariadení.

2. Pred sprístupnením produktu s digitálnymi prvkami na trhu distribútori overia, či:

   a) je na produkte s digitálnymi prvkami umiestnené označenie CE;

   b) výrobca a dovozca splnili povinnosti stanovené v článku 10 ods. 10 a 11 a článku 13 ods. 4.

3. Ak sa distribútor domnieva alebo má dôvod sa domnievať, že produkt s digitálnymi prvkami alebo procesy zavedené výrobcom nie sú v zhode so základnými požiadavkami uvedenými v prílohe I, produkt s digitálnymi prvkami nesmie sprístupniť na trhu, kým sa v prípade tohto produktu alebo procesov zavedených výrobcom nedosiahne zhoda. Okrem toho, ak produkt s digitálnymi prvkami predstavuje významné kybernetickobezpečnostné riziko, distribútor o tom informuje výrobcu a orgány dohľadu nad trhom.

4. Distribútori, ktorí vedia alebo majú dôvod sa domnievať, že produkt s digitálnymi prvkami, ktorý sprístupnili na trhu, alebo procesy zavedené jeho výrobcom nie sú v zhode so základnými požiadavkami uvedenými v prílohe I, zaistia, aby boli prijaté nápravné opatrenia potrebné na to, aby tento produkt s digitálnymi prvkami alebo procesy zavedené jeho výrobcom spĺňali príslušné požiadavky, alebo prípadne na stiahnutie produktu z trhu alebo od používateľa.

   Po identifikovaní zraniteľnosti produktu s digitálnymi prvkami distribútori bez zbytočného odkladu informujú výrobcu o tejto zraniteľnosti. Okrem toho, ak produkt s digitálnymi prvkami predstavuje významné kybernetickobezpečnostné riziko, distribútori o tom bezodkladne informujú orgány dohľadu nad trhom členských štátov, v ktorých produkt s digitálnymi prvkami sprístupnili na trhu, pričom uvedú podrobnosti najmä o nezhode a o všetkých prijatých nápravných opatreniach.

5. Distribútori poskytnú orgánu dohľadu nad trhom na základe jeho odôvodnenej žiadosti všetky informácie a dokumenty v papierovej alebo elektronickej forme potrebné na preukázanie zhody produktu s digitálnymi prvkami a procesov zavedených jeho výrobcom so základnými požiadavkami uvedenými v prílohe I, a to v jazyku, ktorý je pre tento orgán ľahko zrozumiteľný. Na žiadosť tohto orgánu s ním spolupracujú pri akýchkoľvek opatreniach prijatých na odstránenie kybernetickobezpečnostných rizík, ktoré predstavuje produkt s digitálnymi prvkami, ktorý sprístupnili na trhu.

6. Keď sa distribútor produktu s digitálnymi prvkami dozvie, že výrobca tohto produktu ukončil svoju činnosť a v dôsledku toho nie je schopný dodržiavať povinnosti stanovené v tomto nariadení, distribútor informuje o tejto situácii príslušné orgány dohľadu nad trhom a akýmikoľvek dostupnými prostriedkami a v čo najväčšej možnej miere aj používateľov produktov s digitálnymi prvkami uvedených na trh.

Článok 15

Prípady, v ktorých sa povinnosti výrobcov uplatňujú na dovozcov a distribútorov

Dovozca alebo distribútor sa na účely tohto nariadenia považuje za výrobcu a vzťahujú sa naňho povinnosti výrobcu podľa článku 10 a článku 11 ods. 1, 2, 4 a 7, ak tento dovozca alebo distribútor uvedie produkt s digitálnymi prvkami na trh pod svojím menom alebo svojou ochrannou známkou, alebo ak vykoná podstatnú úpravu produktu s digitálnymi prvkami, ktorý už bol uvedený na trh.

Článok 16

Iné prípady, v ktorých sa uplatňujú povinnosti výrobcov

Fyzická alebo právnická osoba iná ako výrobca, dovozca alebo distribútor, ktorá vykoná podstatnú úpravu produktu s digitálnymi prvkami, sa na účely tohto nariadenia považuje za výrobcu.

Na túto osobu sa vzťahujú povinnosti výrobcu podľa článku 10 a článku 11 ods. 1, 2, 4 a 7 v prípade tej časti produktu, ktorá je ovplyvnená podstatnou úpravou, alebo v prípade celého produktu, ak má podstatná úprava vplyv na kybernetickú bezpečnosť produktu s digitálnymi prvkami ako celku.

Článok 17

Identifikácia hospodárskych subjektov

1. Hospodárske subjekty poskytnú orgánom dohľadu nad trhom na požiadanie tieto informácie, ak sú k dispozícii:

   a) meno a adresu každého hospodárskeho subjektu, ktorý im dodal produkt s digitálnymi prvkami;

   b) meno a adresu každého hospodárskeho subjektu, ktorému dodali produkt s digitálnymi prvkami.

2. Hospodárske subjekty musia byť schopné predložiť informácie uvedené v odseku 1 počas desiatich rokov po tom, čo im bol produkt s digitálnymi prvkami dodaný, a počas desiatich rokov po tom, čo produkt s digitálnymi prvkami dodali.

KAPITOLA III

ZHODA PRODUKTU S DIGITÁLNYMI PRVKAMI

Článok 18

Predpoklad zhody

1. Produkty s digitálnymi prvkami a procesy zavedené výrobcom, ktoré sú v zhode s harmonizovanými normami alebo ich časťami, na ktoré boli uverejnené odkazy v *Úradnom vestníku Európskej únie*, sa považujú za produkty a procesy, ktoré sú v zhode so základnými požiadavkami uvedenými v prílohe I, na ktoré sa vzťahujú tieto normy alebo ich časti.

2. Produkty s digitálnymi prvkami a procesy zavedené výrobcom, ktoré sú v zhode so spoločnými špecifikáciami uvedenými v článku 19, sa považujú za produkty a procesy, ktoré sú v zhode so základnými požiadavkami uvedenými v prílohe I, pokiaľ sa uvedené spoločné špecifikácie na tieto požiadavky vzťahujú.

3. Produkty s digitálnymi prvkami a procesy zavedené výrobcom, pre ktoré bolo vydané EÚ vyhlásenie o zhode alebo certifikát v rámci európskeho systému certifikácie kybernetickej bezpečnosti prijatého podľa nariadenia (EÚ) 2019/881 a špecifikovaného podľa odseku 4, sa považujú za produkty a procesy, ktoré sú v zhode so základnými požiadavkami stanovenými v prílohe I, pokiaľ sa na tieto požiadavky vzťahuje EÚ vyhlásenie o zhode alebo certifikát kybernetickej bezpečnosti, alebo ich časti.

4. Komisia je splnomocnená prostredníctvom vykonávacích aktov špecifikovať európske systémy certifikácie kybernetickej bezpečnosti prijaté podľa nariadenia (EÚ) 2019/881, ktoré sa môžu použiť na preukázanie zhody so základnými požiadavkami alebo s ich časťami stanovenými v prílohe I. Komisia naďalej prípadne špecifikuje, či certifikát kybernetickej bezpečnosti vydaný v rámci takýchto systémov ruší povinnosť výrobcu, aby dal vykonať posúdenie zhody treťou stranou

na účely zodpovedajúcich požiadaviek, ako sa stanovuje v článku 24 ods. 2 písm. a) a b) a ods. 3 písm. a) a b). Tieto vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 51 ods. 2.

Článok 19

Spoločné špecifikácie

Ak harmonizované normy uvedené v článku 18 neexistujú alebo ak sa Komisia domnieva, že príslušné harmonizované normy sú nedostatočné na splnenie požiadaviek tohto nariadenia alebo na vyhovenie mandátu Komisie na tvorbu normy, alebo ak v procese normalizácie nastanú zbytočné prieťahy, alebo ak európske normalizačné organizácie nevyhoveli žiadosti Komisie o harmonizované normy, Komisia je splnomocnená prostredníctvom vykonávacích aktov prijať spoločné špecifikácie v súvislosti so základnými požiadavkami uvedenými v prílohe I. Tieto vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 51 ods. 2.

Článok 20

EÚ vyhlásenie o zhode

1. EÚ vyhlásenie o zhode vypracujú výrobcovia v súlade s článkom 10 ods. 7 a uvedú v ňom, že bolo preukázané splnenie uplatniteľných základných požiadaviek stanovených v prílohe I.

2. EÚ vyhlásenie o zhode sa vypracúva podľa vzoru stanoveného v prílohe IV a obsahuje prvky špecifikované v príslušných postupoch posudzovania zhody stanovených v prílohe VI. Takéto vyhlásenie sa priebežne aktualizuje. Sprístupní sa v jazyku alebo jazykoch požadovaných členským štátom, v ktorom sa produkt s digitálnymi prvkami uvádza na trh alebo sprístupňuje na trhu.

3. Ak sa na produkt s digitálnymi prvkami vzťahuje viac ako jeden právny akt Únie, v ktorom sa vyžaduje EÚ vyhlásenie o zhode, vypracuje sa pre všetky tieto akty Únie jediné EÚ vyhlásenie o zhode. Príslušné akty Únie sa uvedú v tomto vyhlásení, a to vrátane odkazov na ich uverejnenie.

4. Vydaním EÚ vyhlásenia o zhode výrobca preberá zodpovednosť za súlad výrobku so stanovenými požiadavkami.

5. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 50 s cieľom doplniť toto nariadenie, a to pridaním prvkov do minimálneho obsahu EÚ vyhlásenia o zhode stanoveného v prílohe IV s cieľom zohľadniť technologický vývoj.

Článok 21

Všeobecné zásady týkajúce sa označenia CE

Na označenie CE vymedzené v článku 3 bode 32 sa vzťahujú všeobecné zásady stanovené v článku 30 nariadenia (ES) č. 765/2008.

Článok 22

Pravidlá a podmienky umiestnenia označenia CE

1. Označenie CE sa na produkt s digitálnymi prvkami umiestni viditeľne, čitateľne a nezmazateľne. Ak to vzhľadom na povahu produktu s digitálnymi prvkami nie je možné alebo odôvodnené, toto označenie sa umiestni na obal a na EÚ vyhlásenie o zhode uvedené v článku 20, ktoré sa pripojí k produktu s digitálnymi prvkami. V prípade produktov s digitálnymi prvkami, ktoré sú vo forme softvéru, sa označenie CE umiestni buď na EÚ vyhlásenie o zhode uvedené v článku 20, alebo na sprievodné webové sídlo softvérového produktu.

2. Vzhľadom na povahu produktu s digitálnymi prvkami môže byť výška označenia CE umiestneného na produkte s digitálnymi prvkami menšia ako 5 mm za predpokladu, že označenie bude naďalej viditeľné a čitateľné.

3. Označenie CE sa na produkt s digitálnymi prvkami umiestni pred uvedením tohto produktu na trh. Za označením môže nasledovať piktogram alebo akákoľvek iná značka poukazujúca na osobitné riziko alebo použitie stanovené vo vykonávacích aktoch uvedených v odseku 6.

4. Za označením CE nasleduje identifikačné číslo notifikovanej osoby, ak je táto osoba zapojená do postupu posudzovania zhody založeného na úplnom zabezpečení kvality (na základe modulu H) uvedeného v článku 24.

   Identifikačné číslo notifikovanej osoby umiestňuje samotná osoba alebo na základe jej pokynov výrobca alebo splnomocnený zástupca výrobcu.

5. Členské štáty vychádzajú pri zabezpečovaní správneho uplatňovania režimu úpravy označenia CE z existujúcich mechanizmov a v prípade nesprávneho používania tohto označenia prijmú primerané opatrenia. Ak sa na produkt s digitálnymi prvkami vzťahujú iné právne predpisy Únie, v ktorých sa takisto vyžaduje umiestnenie označenia CE, v označení CE sa uvedie, že produkt spĺňa aj požiadavky týchto iných právnych predpisov.

6. Komisia môže prostredníctvom vykonávacích aktov stanoviť technické špecifikácie piktogramov alebo akýchkoľvek iných značiek týkajúcich sa bezpečnosti produktov s digitálnymi prvkami a mechanizmy na podporu ich používania. Tieto vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 51 ods. 2.

Článok 23

Technická dokumentácia

1. Technická dokumentácia obsahuje všetky príslušné údaje alebo podrobnosti týkajúce sa prostriedkov, ktoré výrobca použil na zaistenie toho, aby produkt s digitálnymi prvkami a procesy zavedené výrobcom boli v súlade so základnými požiadavkami uvedenými v prílohe I. Obsahuje aspoň prvky stanovené v prílohe V.

2. Technická dokumentácia sa vypracuje pred uvedením produktu s digitálnymi prvkami na trh a v prípade potreby sa priebežne aktualizuje počas predpokladanej životnosti produktu alebo počas obdobia piatich rokov po uvedení produktu s digitálnymi prvkami na trh, podľa toho, čo je kratšie.

3. V prípade produktov s digitálnymi prvkami uvedených v článku 8 a článku 24 ods. 4, na ktoré sa vzťahujú aj iné akty Únie, sa vypracuje jediná technická dokumentácia, ktorá obsahuje informácie uvedené v prílohe V k tomuto nariadeniu a informácie požadované týmito príslušnými aktmi Únie.

4. Technická dokumentácia a korešpondencia súvisiace s postupom posudzovania zhody sa vypracúvajú v úradnom jazyku členského štátu, v ktorom je notifikovaná osoba usadená, alebo v jazyku, ktorý je pre túto osobu prijateľný.

5. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 50 s cieľom doplniť toto nariadenie o prvky, ktoré sa majú zahrnúť do technickej dokumentácie uvedenej v prílohe V, aby sa zohľadnil technologický vývoj, ako aj vývoj, ku ktorému dôjde v procese vykonávania tohto nariadenia.

Článok 24

Postupy posudzovania zhody produktov s digitálnymi prvkami

1. Výrobca vykonáva posudzovanie zhody produktu s digitálnymi prvkami a procesov zavedených výrobcom s cieľom určiť, či sú splnené základné požiadavky uvedené v prílohe I. Výrobca alebo splnomocnený zástupca výrobcu preukazuje zhodu so základnými požiadavkami použitím jedného z týchto postupov:

   a) postup vnútornej kontroly (na základe modulu A) stanovený v prílohe VI, alebo

   b) EÚ skúška typu (na základe modulu B) stanovená v prílohe VI, po ktorej nasleduje zhoda s EÚ typom založená na vnútornej kontrole výroby (na základe modulu C) stanovená v prílohe VI, alebo

   c) posudzovanie zhody založené na úplnom zabezpečení kvality (na základe modulu H) stanovené v prílohe VI.

2. Ak výrobca alebo splnomocnený zástupca výrobcu pri posudzovaní súladu kritického produktu s digitálnymi prvkami triedy I v zmysle v prílohy III a procesov zavedených jeho výrobcom so základnými požiadavkami stanovenými v prílohe I neuplatnil alebo len čiastočne uplatnil harmonizované normy, spoločné špecifikácie alebo európske systémy certifikácie kybernetickej bezpečnosti uvedené v článku 18, alebo ak takéto harmonizované normy, spoločné špecifikácie alebo európske systémy certifikácie kybernetickej bezpečnosti neexistujú, dotknutý produkt s digitálnymi prvkami a procesy zavedené výrobcom sa v súvislosti s týmito základnými požiadavkami podrobia jednému z týchto postupov:

   a) EÚ skúška typu (na základe modulu B) uvedená v prílohe VI, po ktorej nasleduje zhoda s EÚ typom založená na vnútornej kontrole výroby (na základe modulu C) stanovená v prílohe VI, alebo

   b) posudzovanie zhody založené na úplnom zabezpečení kvality (na základe modulu H) stanovené v prílohe VI.

3. Ak je produkt kritickým produktom s digitálnymi prvkami triedy II v zmysle prílohy III, výrobca alebo splnomocnený zástupca výrobcu preukazuje zhodu so základnými požiadavkami stanovenými v prílohe I použitím jedného z týchto postupov:

   a) EÚ skúška typu (na základe modulu B) uvedená v prílohe VI, po ktorej nasleduje zhoda s EÚ typom založená na vnútornej kontrole výroby (na základe modulu C) stanovená v prílohe VI, alebo

   b) posudzovanie zhody založené na úplnom zabezpečení kvality (na základe modulu H) stanovené v prílohe VI.

4. Výrobcovia produktov s digitálnymi prvkami, ktoré sú klasifikované ako systémy elektronických zdravotných záznamov v rozsahu pôsobnosti nariadenia [nariadenie o európskom priestore pre zdravotné údaje], preukazujú zhodu so základnými požiadavkami stanovenými v prílohe I k tomuto nariadeniu použitím príslušného postupu posudzovania zhody, ako sa vyžaduje v nariadení [kapitola III nariadenia o európskom priestore pre zdravotné údaje].

5. Notifikované osoby zohľadnia pri stanovovaní poplatkov za postupy posudzovania zhody špecifické záujmy a potreby malých a stredných podnikov (MSP) a uvedené poplatky na základe týchto osobitných záujmov a potrieb primerane znížia.

KAPITOLA IV

NOTIFIKÁCIA ORGÁNOV POSUDZOVANIA ZHODY

Článok 25

Notifikácia

Členské štáty notifikujú Komisii a ostatným členským štátom orgány posudzovania zhody, ktoré sú oprávnené vykonávať posudzovania zhody v súlade s týmto nariadením.

Článok 26

Notifikujúce orgány

1. Členské štáty určia notifikujúci orgán, ktorý je zodpovedný za stanovenie a vykonávanie postupov potrebných na posudzovanie a notifikáciu orgánov posudzovania zhody a za monitorovanie notifikovaných osôb vrátane súladu s článkom 31.

2. Členské štáty môžu rozhodnúť, že posudzovanie a monitorovanie uvedené v odseku 1 vykoná vnútroštátny akreditačný orgán v zmysle nariadenia (ES) č. 765/2008 a v súlade s ním.

Článok 27

Požiadavky týkajúce sa notifikujúcich orgánov

1. Notifikujúci orgán sa zriaďuje tak, aby nevznikali žiadne konflikty záujmov s orgánmi posudzovania zhody.

2. Notifikujúci orgán má takú organizačnú štruktúru a funguje takým spôsobom, aby bola zabezpečená objektivita a nestrannosť jeho činností.

3. Notifikujúci orgán má takú organizačnú štruktúru, aby každé rozhodnutie týkajúce sa notifikácie orgánu posudzovania zhody prijali odborne spôsobilé osoby, iné ako osoby, ktoré vykonali posúdenie.

4. Notifikujúci orgán neponúka ani neposkytuje žiadne činnosti, ktoré vykonávajú orgány posudzovania zhody, ani poradenské služby na komerčnom či konkurenčnom základe.

5. Notifikujúci orgán zabezpečuje dôvernosť ním získaných informácií.

6. Notifikujúci orgán má k dispozícii dostatočný počet odborne spôsobilých zamestnancov na riadne plnenie svojich úloh.

Článok 28

Informačná povinnosť notifikujúcich orgánov

1. Členské štáty informujú Komisiu o svojich postupoch posudzovania a notifikácie orgánov posudzovania zhody a monitorovania notifikovaných osôb a o všetkých zmenách, pokiaľ ide o tieto postupy.

2. Komisia tieto informácie zverejňuje.

Článok 29

Požiadavky týkajúce sa notifikovaných osôb

1. Na účely notifikácie musí orgán posudzovania zhody spĺňať požiadavky stanovené v odsekoch 2 až 12.

2. Orgán posudzovania zhody sa zriadi podľa vnútroštátnych právnych predpisov a má právnu subjektivitu.

3. Orgán posudzovania zhody je treťou stranou, nezávislou od organizácie alebo produktu, ktorý posudzuje.

   Za takýto orgán možno pod podmienkou, že je preukázaná jeho nezávislosť a nedochádza ku konfliktu záujmov, považovať subjekt, ktorý patrí do záujmového združenia alebo profesijného zväzu, ktoré zastupujú podniky zapojené do navrhovania, vývoja, výroby, obstarávania, montáže, používania alebo údržby produktov s digitálnymi prvkami, ktoré posudzuje.

4. Orgán posudzovania zhody, jeho vrcholový manažment a zamestnanci zodpovední za vykonávanie úloh posudzovania zhody nie sú dizajnéri, vývojári, výrobcovia, dodávatelia, subjekty vykonávajúce inštaláciu, nákupcovia, vlastníci, používatelia alebo subjekty vykonávajúce údržbu produktov s digitálnymi prvkami, ktoré posudzujú, ani splnomocnení zástupcovia žiadnej z týchto strán. Týmto sa nevylučuje použitie posudzovaných produktov, ktoré sú potrebné na výkon činností orgánu posudzovania zhody, ani použitie takýchto produktov na osobné účely.

   Orgán posudzovania zhody, jeho vrcholový manažment a zamestnanci zodpovední za vykonávanie úloh posudzovania zhody nie sú priamo zapojení do návrhu, vývoja, výroby, uvádzania na trh, inštalácie, používania alebo údržby týchto produktov, ani nezastupujú strany zapojené do týchto činností. Nepodieľajú sa na žiadnej činnosti, ktorá by mohla ovplyvniť ich nezávislý úsudok alebo bezúhonnosť vo vzťahu k činnostiam posudzovania zhody, na ktorých vykonávanie sú notifikované. Týka sa to najmä poradenských služieb.

   Orgány posudzovania zhody zabezpečia, aby činnosti ich pomocných orgánov alebo ich subdodávateľov neovplyvňovali dôvernosť, objektivitu a nestrannosť ich činností posudzovania zhody.

5. Orgány posudzovania zhody a ich zamestnanci vykonávajú činnosti posudzovania zhody na najvyššej úrovni odbornej integrity a nevyhnutnej technickej spôsobilosti v danej oblasti a nesmú podliehať žiadnym tlakom a stimulom, najmä finančným, ktoré by mohli ovplyvniť ich rozhodnutie alebo výsledky ich činností posudzovania

zhody, najmä zo strany osôb alebo skupín osôb, ktoré majú záujem na výsledku týchto činností.

6. Orgán posudzovania zhody je schopný vykonávať všetky úlohy posudzovania zhody uvedené v prílohe VI, v súvislosti s ktorými bol notifikovaný, bez ohľadu na to, či ide o úlohy vykonávané samotným orgánom posudzovania zhody, alebo v jeho mene a na jeho zodpovednosť.

   Orgán posudzovania zhody má vždy a pre každý postup posudzovania zhody a pre každý druh alebo kategóriu produktu s digitálnymi prvkami, v súvislosti s ktorými bol notifikovaný, k dispozícii:

   a) potrebný personál s technickými vedomosťami a dostatočnými a primeranými skúsenosťami na výkon úloh posudzovania zhody;

   b) potrebný opis postupov, v súlade s ktorými sa vykonáva posudzovanie zhody, na účely zaistenia transparentnosti a reprodukovateľnosti týchto postupov. Má zavedené príslušné politiky a postupy, v ktorých sa rozlišuje medzi úlohami, ktoré vykonáva ako notifikovaná osoba, a inými činnosťami;

   c) potrebné postupy na vykonávanie činností, ktoré náležitým spôsobom zohľadňujú veľkosť podniku, odvetvie, v ktorom podnik pôsobí, jeho štruktúru, stupeň zložitosti danej technológie produktu a hromadný či sériový charakter výrobného procesu.

   Má prostriedky potrebné na primerané plnenie technických a administratívnych úloh spojených s činnosťami posudzovania zhody a má prístup ku všetkým potrebným zariadeniam alebo vybaveniu.

7. Zamestnanci zodpovední za výkon činností posudzovania zhody majú:

   a) primerané technické a odborné vzdelanie vzťahujúce sa na všetky činnosti posudzovania zhody, v súvislosti s ktorými bol orgán posudzovania zhody notifikovaný;

   b) dostatočné vedomosti o požiadavkách týkajúcich sa nimi vykonávaných posudzovaní a primeranú právomoc vykonávať tieto posudzovania;

   c) primerané znalosti a pochopenie základných požiadaviek, uplatniteľných harmonizovaných noriem a príslušných ustanovení harmonizačných právnych predpisov Únie a ich vykonávacích aktov;

   d) schopnosť vypracúvať certifikáty, záznamy a správy preukazujúce, že sa posúdenie vykonalo.

8. Je potrebné zaručiť nestrannosť orgánov posudzovania zhody, ich vrcholového manažmentu a zamestnancov, ktorí vykonávajú posudzovanie.

   Odmeňovanie vrcholového manažmentu orgánu posudzovania zhody a jeho zamestnancov, ktorí vykonávajú posudzovanie, nezávisí od počtu vykonaných posúdení, ani od výsledkov týchto posúdení.

9. Orgány posudzovania zhody uzavrú poistenie zodpovednosti za škodu, pokiaľ túto zodpovednosť nenesie štát v súlade s vnútroštátnym právom, alebo pokiaľ nie je za posudzovanie zhody priamo zodpovedný samotný členský štát.

10. Zamestnanci orgánu posudzovania zhody sú povinní dodržiavať služobné tajomstvo, pokiaľ ide o všetky informácie získané pri vykonávaní ich úloh podľa prílohy VI alebo akéhokoľvek ustanovenia vnútroštátneho práva, ktorým sa táto príloha uvádza

do účinnosti, nie však vo vzťahu k orgánom dohľadu nad trhom členského štátu, v ktorom daný orgán vykonáva svoju činnosť. Vlastnícke práva sú chránené. Orgán posudzovania zhody má zdokumentované postupy, ktorými sa zaisťuje súlad s týmto odsekom.

11. Orgány posudzovania zhody sa zúčastňujú na príslušných normalizačných činnostiach a činnostiach koordinačnej skupiny notifikovanej osoby zriadenej podľa článku 40 alebo zabezpečia, aby ich zamestnanci, ktorí vykonávajú posudzovanie, boli o nich informovaní, a ako všeobecné usmernenie uplatňujú administratívne rozhodnutia a dokumenty, ktoré sú výsledkom práce tejto skupiny.

12. Orgány posudzovania zhody vykonávajú svoju činnosť v súlade so súborom konzistentných, spravodlivých a primeraných podmienok, pričom, pokiaľ ide o poplatky, zohľadňujú najmä záujmy MSP.

Článok 30

Predpoklad zhody notifikovaných osôb

Ak orgán posudzovania zhody preukáže svoju zhodu s kritériami stanovenými v príslušných harmonizovaných normách alebo ich častiach, na ktoré boli uverejnené odkazy v *Úradnom vestníku Európskej únie*, predpokladá sa, že spĺňa požiadavky stanovené v článku 29, pokiaľ sa na tieto požiadavky vzťahujú uplatniteľné harmonizované normy.

Článok 31

Pomocné orgány a subdodávatelia notifikovaných osôb

1. Ak notifikovaná osoba zadá osobitné úlohy spojené s posudzovaním zhody subdodávateľovi alebo využíva pomocný orgán, zaistí, aby subdodávateľ alebo pomocný orgán spĺňali požiadavky stanovené v článku 29, a informuje o tom notifikujúci orgán.

2. Notifikované osoby nesú plnú zodpovednosť za úlohy, ktoré vykonávajú subdodávatelia alebo pomocné orgány, bez ohľadu na to, kde sú tieto usadené.

3. Činnosti môžu byť vykonávané subdodávateľsky alebo pomocným orgánom len so súhlasom výrobcu.

4. Notifikované osoby uchovávajú k dispozícii pre notifikujúci orgán príslušnú dokumentáciu týkajúcu sa posúdenia kvalifikácie subdodávateľa alebo pomocného orgánu a práce, ktorú tento subdodávateľ alebo pomocný orgán vykonali podľa tohto nariadenia.

Článok 32

Žiadosť o notifikáciu

1. Orgán posudzovania zhody predkladá žiadosť o notifikáciu notifikujúcemu orgánu členského štátu, v ktorom je usadený.

2. Súčasťou žiadosti je opis činností posudzovania zhody, postupu alebo postupov posudzovania zhody a produktu alebo produktov, v súvislosti s ktorými orgán tvrdí, že je spôsobilý, ako aj osvedčenie o akreditácii, ak existuje, vydané vnútroštátnym

akreditačným orgánom, ktoré potvrdzuje, že orgán posudzovania zhody spĺňa požiadavky stanovené v článku 29.

3. Ak príslušný orgán posudzovania zhody nemôže poskytnúť osvedčenie o akreditácii, poskytne notifikujúcemu orgánu všetky listinné dôkazy potrebné na overenie, uznanie a pravidelné monitorovanie svojho súladu s požiadavkami stanovenými v článku 29.

Článok 33

Postup notifikácie

1. Notifikujúce orgány môžu notifikovať iba tie orgány posudzovania zhody, ktoré splnili požiadavky stanovené v článku 29.

2. Notifikujúci orgán notifikuje Komisii a ostatným členským štátom prostredníctvom informačného systému NANDO, ktorý vyvinula a spravuje Komisia.

3. V notifikácii sú zahrnuté všetky podrobnosti o činnostiach posudzovania zhody, modul alebo moduly posudzovania zhody, dotknutý produkt alebo dotknuté produkty a príslušné potvrdenie odbornej spôsobilosti.

4. Ak sa notifikácia nezakladá na osvedčení o akreditácii uvedenom v článku 32 ods. 2, notifikujúci orgán poskytne Komisii a ostatným členským štátom listinné dôkazy potvrdzujúce odbornú spôsobilosť orgánu posudzovania zhody a zavedené opatrenia s cieľom zaistiť, že tento orgán bude pravidelne monitorovaný a bude naďalej spĺňať požiadavky stanovené v článku 29.

5. Príslušný orgán môže vykonávať činnosti notifikovanej osoby iba v prípade, že Komisia ani ostatné členské štáty nevzniesli námietky, a to do dvoch týždňov od notifikácie, ak sa použije osvedčenie o akreditácii, alebo do dvoch mesiacov od notifikácie, ak sa akreditácia nepoužije.

   Iba takýto orgán sa pokladá za notifikovanú osobu na účely tohto nariadenia.

6. Komisii a ostatným členským štátom sa oznamujú všetky následné relevantné zmeny v notifikácii.

Článok 34

Identifikačné čísla a zoznamy notifikovaných osôb

1. Komisia pridelí notifikovanej osobe identifikačné číslo.

   Pridelí jej len jedno takéto číslo, aj keď je osoba notifikovaná podľa viacerých aktov Únie.

2. Komisia zverejní zoznam osôb notifikovaných podľa tohto nariadenia vrátane identifikačných čísiel, ktoré im boli pridelené, a činností, v súvislosti s ktorými boli notifikované.

   Komisia zabezpečuje aktualizáciu tohto zoznamu.

Článok 35

Zmeny v notifikáciách

1. Ak notifikujúci orgán zistí alebo je informovaný o tom, že notifikovaná osoba už nespĺňa požiadavky stanovené v článku 29 alebo že si neplní svoje povinnosti,

notifikujúci orgán podľa potreby obmedzí, pozastaví alebo zruší notifikáciu v závislosti od závažnosti nesplnenia týchto požiadaviek alebo neplnenia týchto povinností. Bezodkladne o tom informuje Komisiu a ostatné členské štáty.

2. V prípade obmedzenia, pozastavenia alebo zrušenia notifikácie, alebo ak notifikovaná osoba ukončila svoju činnosť, notifikujúci členský štát prijme primerané opatrenia na zaistenie toho, aby spisy tejto osoby buď spracovala iná notifikovaná osoba, alebo aby boli na požiadanie k dispozícii príslušným notifikujúcim orgánom a orgánom dohľadu nad trhom.

Článok 36

Spochybnenie odbornej spôsobilosti notifikovaných osôb

1. Komisia vyšetrí všetky prípady, v súvislosti s ktorými má pochybnosti alebo bola na pochybnosti upozornená, pokiaľ ide o odbornú spôsobilosť notifikovanej osoby alebo nepretržité plnenie požiadaviek a povinností, ktoré sa na notifikovanú osobu vzťahujú.

2. Notifikujúci členský štát poskytne Komisii na jej žiadosť všetky informácie v súvislosti s podkladmi pre notifikáciu alebo so zachovaním odbornej spôsobilosti dotknutej osoby.

3. Komisia zabezpečí dôverné zaobchádzanie so všetkými citlivými informáciami získanými počas jej vyšetrovania.

4. Ak Komisia zistí, že notifikovaná osoba nespĺňa alebo prestala spĺňať požiadavky na svoju notifikáciu, informuje o tom notifikujúci členský štát a požiada ho, aby prijal potrebné nápravné opatrenia vrátane zrušenia notifikácie, ak je to potrebné.

Článok 37

Povinnosti notifikovaných osôb, pokiaľ ide o výkon ich činností

1. Notifikované osoby vykonávajú posudzovanie zhody v súlade s postupmi posudzovania zhody stanovenými v článku 24 a prílohe VI.

2. Posudzovanie zhody sa vykonáva primeraným spôsobom tak, aby sa predišlo zbytočnému zaťaženiu hospodárskych subjektov. Orgány posudzovania zhody pri vykonávaní svojej činnosti náležite zohľadňujú veľkosť podniku, odvetvie, v ktorom podnik pôsobí, jeho štruktúru, stupeň zložitosti danej technológie produktu a hromadný či sériový charakter výrobného procesu.

3. Notifikovaná osoba však pri tom dbá na stupeň prísnosti a úroveň ochrany, ktoré sú potrebné vzhľadom na zabezpečenie súladu produktu s ustanoveniami nariadenia.

4. Ak notifikovaná osoba zistí, že výrobca nespĺňa požiadavky stanovené v prílohe I alebo zodpovedajúcich harmonizovaných normách alebo spoločných špecifikáciách uvedených v článku 19, požiada tohto výrobcu, aby prijal primerané nápravné opatrenia, a certifikát zhody nevydá.

5. Ak po vystavení certifikátu notifikovaná osoba v rámci monitorovania zhody zistí, že výrobok už nespĺňa požiadavky stanovené v tomto nariadení, požiada výrobcu, aby prijal primerané nápravné opatrenia, a ak to je potrebné, pozastaví platnosť certifikátu alebo ho odníme.

6. Ak sa neprijmú nápravné opatrenia alebo ak nemajú požadovaný účinok, notifikovaná osoba podľa potreby obmedzí rozsah, pozastaví platnosť alebo odníme všetky certifikáty.

Článok 38

Informačná povinnosť notifikovaných osôb

1. Notifikované osoby informujú notifikujúci orgán:

   a) o každom zamietnutí, obmedzení rozsahu, pozastavení platnosti alebo odňatí certifikátu;

   b) o akýchkoľvek okolnostiach, ktoré majú vplyv na rozsah a podmienky notifikácie;

   c) o každej žiadosti o informácie, ktorú dostali od orgánov dohľadu nad trhom v súvislosti s činnosťami posudzovania zhody;

   d) na požiadanie o činnostiach posudzovania zhody vykonaných v rozsahu ich notifikácie a o akejkoľvek inej vykonanej činnosti vrátane cezhraničných činností a zadávania činností subdodávateľom.

2. Notifikované osoby poskytnú iným osobám notifikovaným podľa tohto nariadenia, ktoré vykonávajú podobné činnosti posudzovania zhody vzťahujúce sa na rovnaké produkty, príslušné informácie o otázkach týkajúcich sa negatívnych a na požiadanie aj pozitívnych výsledkov posudzovania zhody.

Článok 39

Výmena skúseností

Komisia organizačne zabezpečí výmenu skúseností medzi vnútroštátnymi orgánmi členských štátov, ktoré sú zodpovedné za politiku notifikácie.

Článok 40

Koordinácia notifikovaných osôb

1. Komisia zabezpečuje zavedenie a riadne fungovanie primeranej koordinácie a spolupráce medzi notifikovanými osobami vo forme medziodvetvovej skupiny notifikovaných osôb.

2. Členské štáty zaistia, aby sa osoby, ktoré notifikovali, priamo alebo prostredníctvom určených zástupcov zúčastňovali na práci tejto skupiny.

KAPITOLA V

DOHĽAD NAD TRHOM A PRESADZOVANIE PRÁVA

Článok 41

Dohľad nad trhom a kontrola produktov s digitálnymi prvkami na trhu Únie

1. Na produkty s digitálnymi prvkami patriace do rozsahu pôsobnosti tohto nariadenia sa uplatňuje nariadenie (EÚ) 2019/1020.

2. Na účely zaistenia účinného vykonávania tohto nariadenia každý členský štát určí jeden alebo viac orgánov dohľadu nad trhom. Členské štáty môžu určiť existujúci alebo nový orgán, aby na účely tohto nariadenia konal ako orgán dohľadu nad trhom.

3. Orgány dohľadu nad trhom v relevantných prípadoch spolupracujú s vnútroštátnymi orgánmi pre certifikáciu kybernetickej bezpečnosti určenými podľa článku 58 nariadenia (EÚ) 2019/881 a pravidelne si vymieňajú informácie. Pokiaľ ide o dohľad nad vykonávaním oznamovacích povinností podľa článku 11 tohto nariadenia, určené orgány dohľadu nad trhom spolupracujú s agentúrou ENISA.

4. V relevantných prípadoch orgány dohľadu nad trhom spolupracujú s inými orgánmi dohľadu nad trhom určenými na základe iných harmonizačných právnych predpisov Únie pre iné produkty a pravidelne si vymieňajú informácie.

5. Orgány dohľadu nad trhom podľa potreby spolupracujú s orgánmi, ktoré vykonávajú dohľad nad právnymi predpismi Únie v oblasti ochrany osobných údajov. Takáto spolupráca zahŕňa informovanie týchto orgánov o každom zistení relevantnom z hľadiska plnenia ich právomocí, a to aj pri vydávaní usmernení a poskytovaní poradenstva podľa odseku 8 tohto článku, ak sa takéto usmernenia a poradenstvo týkajú spracúvania osobných údajov.

   Orgány, ktoré vykonávajú dohľad nad právnymi predpismi Únie v oblasti ochrany osobných údajov, majú právomoc požadovať akúkoľvek dokumentáciu vytvorenú alebo vedenú podľa tohto nariadenia a mať k nej prístup, ak je prístup k tejto dokumentácii potrebný na plnenie ich úloh. O každej takejto žiadosti informujú určené orgány dohľadu nad trhom dotknutého členského štátu.

6. Členské štáty zaistia, aby určené orgány dohľadu nad trhom mali na plnenie svojich úloh podľa tohto nariadenia k dispozícii primerané finančné a ľudské zdroje.

7. Komisia podporuje výmenu skúseností medzi určenými orgánmi dohľadu nad trhom.

8. Orgány dohľadu nad trhom môžu s podporou Komisie poskytovať hospodárskym subjektom usmernenia a poradenstvo v oblasti vykonávania tohto nariadenia.

9. Orgány dohľadu nad trhom každoročne podávajú Komisii správy o výsledkoch príslušných činností dohľadu nad trhom. Všetky informácie zistené v priebehu činností dohľadu nad trhom, ktoré by mohli mať potenciálny význam pre uplatňovanie práva Únie v oblasti hospodárskej súťaže, určené orgány dohľadu nad trhom bezodkladne oznámia Komisii a príslušným vnútroštátnym orgánom na ochranu hospodárskej súťaže.

10. V prípade produktov s digitálnymi prvkami v rozsahu pôsobnosti tohto nariadenia klasifikovaných ako vysokorizikové systémy umelej inteligencie podľa článku [článok 6] nariadenia [nariadenie o umelej inteligencii] sú orgány dohľadu nad trhom určené na účely nariadenia [nariadenie o umelej inteligencii] orgánmi zodpovednými za činnosti dohľadu nad trhom vyžadované podľa tohto nariadenia. Orgány dohľadu nad trhom určené podľa nariadenia [nariadenie o umelej inteligencii] spolupracujú podľa potreby s orgánmi dohľadu nad trhom určenými podľa tohto nariadenia a s agentúrou ENISA, pokiaľ ide o dohľad nad vykonávaním oznamovacích povinností podľa článku 11. Orgány dohľadu nad trhom určené podľa nariadenia [nariadenie o umelej inteligencii] najmä informujú orgány dohľadu nad trhom určené podľa tohto nariadenia o každom zistení, ktoré je relevantné z hľadiska plnenia ich úloh v súvislosti s vykonávaním tohto nariadenia.

11. Na jednotné uplatňovanie tohto nariadenia sa podľa článku 30 ods. 2 nariadenia (EÚ) 2019/1020 zriadi osobitná skupina pre administratívnu spoluprácu (ADCO). Skupinu ADCO tvoria zástupcovia určených orgánov dohľadu nad trhom a prípadne zástupcovia jednotných úradov pre spoluprácu.

Článok 42

Prístup k údajom a dokumentácii

Ak je potrebné posúdiť zhodu produktov s digitálnymi prvkami a procesov zavedených ich výrobcami so základnými požiadavkami stanovenými v prílohe I, na základe odôvodnenej žiadosti sa orgánom dohľadu nad trhom poskytne prístup k údajom požadovaným na posúdenie návrhu, vývoja, výroby a riešenia zraniteľností takýchto produktov vrátane súvisiacej internej dokumentácie príslušného hospodárskeho subjektu.

Článok 43

Postup na vnútroštátnej úrovni týkajúci sa produktov s digitálnymi prvkami, ktoré predstavujú významné kybernetickobezpečnostné riziko

1. Ak má orgán dohľadu nad trhom členského štátu dostatočné dôvody domnievať sa, že produkt s digitálnymi prvkami vrátane riešenia jeho zraniteľností predstavuje významné kybernetickobezpečnostné riziko, vykoná hodnotenie dotknutého produktu s digitálnymi prvkami, pokiaľ ide o jeho súlad so všetkými požiadavkami stanovenými v tomto nariadení. Príslušné hospodárske subjekty podľa potreby spolupracujú s orgánom dohľadu nad trhom.

   Ak v priebehu tohto hodnotenia orgán dohľadu nad trhom zistí, že produkt s digitálnymi prvkami nespĺňa požiadavky stanovené v tomto nariadení, bezodkladne požiada príslušný hospodársky subjekt, aby prijal všetky primerané nápravné opatrenia na uvedenie tohto produktu do súladu s uvedenými požiadavkami alebo aby produkt stiahol z trhu alebo od používateľov v primeranej lehote, ktorú môže orgán stanoviť a ktorá je úmerná charakteru rizika.

   Orgán dohľadu nad trhom o tom informuje príslušnú notifikovanú osobu. Na primerané nápravné opatrenia sa uplatňuje článok 18 nariadenia (EÚ) 2019/1020.

2. Ak sa orgán dohľadu nad trhom domnieva, že nesúlad sa neobmedzuje na územie jeho štátu, informuje Komisiu a ostatné členské štáty o výsledkoch hodnotenia a o opatreniach, ktorých prijatie požaduje od hospodárskeho subjektu.

3. Výrobca zaistí prijatie všetkých primeraných nápravných opatrení v súvislosti so všetkými dotknutými produktmi s digitálnymi prvkami, ktoré sprístupnil na trhu v celej Únii.

4. Ak výrobca produktu s digitálnymi prvkami v rámci lehoty uvedenej v odseku 1 druhom pododseku neprijme primerané nápravné opatrenia, orgán dohľadu nad trhom prijme všetky primerané predbežné opatrenia s cieľom zakázať alebo obmedziť sprístupnenie uvedeného produktu na svojom vnútroštátnom trhu, stiahnuť výrobok z daného trhu alebo od používateľa.

   O týchto opatreniach uvedený orgán bezodkladne informuje Komisiu a ostatné členské štáty.

5. Informácie uvedené v odseku 4 zahŕňajú všetky dostupné podrobné údaje, najmä údaje potrebné na identifikáciu nevyhovujúcich produktov s digitálnymi prvkami,

pôvod výrobku s digitálnymi prvkami, charakter údajného nesúladu a možné riziko, charakter a trvanie prijatých vnútroštátnych opatrení a stanoviská, ktoré predložil príslušný hospodársky subjekt. Orgán dohľadu nad trhom predovšetkým uvedie, či k nesúladu došlo v dôsledku jedného alebo viacerých z týchto dôvodov:

a) produkt alebo procesy zavedené výrobcom nespĺňajú základné požiadavky uvedené v prílohe I;

b) nedostatky v harmonizovaných normách, systémoch certifikácie kybernetickej bezpečnosti alebo spoločných špecifikáciách uvedených v článku 18.

6. Orgány dohľadu nad trhom členských štátov iné než orgán dohľadu nad trhom členského štátu, ktorý postup začal, bezodkladne oboznámia Komisiu a ostatné členské štáty so všetkými prijatými opatreniami a s akýmikoľvek dodatočnými informáciami týkajúcimi sa nesúladu dotknutého produktu, ktoré majú k dispozícii, a v prípade, že nesúhlasia s oznámeným vnútroštátnym opatrením, aj so svojimi námietkami.

7. Ak do troch mesiacov od prijatia informácií uvedených v odseku 4 žiadny členský štát ani Komisia nevznesú námietku, pokiaľ ide o predbežné opatrenie prijaté členským štátom, toto opatrenie sa považuje za opodstatnené. Týmto nie sú dotknuté procesné práva dotknutého hospodárskeho subjektu v súlade s článkom 18 nariadenia (EÚ) 2019/1020.

8. Orgány dohľadu nad trhom všetkých členských štátov zabezpečia, aby sa vo vzťahu k dotknutému výrobku bezodkladne prijali primerané reštriktívne opatrenia, ako je napríklad stiahnutie výrobku z ich trhu.

Článok 44

Ochranný postup Únie

1. Ak do troch mesiacov od doručenia oznámenia uvedeného v článku 43 ods. 4 členský štát vznesie námietky proti opatreniu prijatému iným členským štátom, alebo ak Komisia považuje toto opatrenie za také, ktoré je v rozpore s právnymi predpismi Únie, Komisia bezodkladne začne konzultácie s príslušným členským štátom a hospodárskym subjektom alebo hospodárskymi subjektmi a dané vnútroštátne opatrenie vyhodnotí. Na základe výsledkov tohto hodnotenia Komisia do deviatich mesiacov od oznámenia uvedeného v článku 43 ods. 4 rozhodne, či vnútroštátne opatrenie je alebo nie je opodstatnené, a toto rozhodnutie oznámi dotknutému členskému štátu.

2. Ak sa vnútroštátne opatrenie považuje za opodstatnené, všetky členské štáty prijmú opatrenia potrebné na zaistenie stiahnutia nevyhovujúceho produktu s digitálnymi prvkami zo svojho trhu a náležite o tom informujú Komisiu. Ak sa vnútroštátne opatrenie považuje za neopodstatnené, dotknutý členský štát toto opatrenie zruší.

3. Ak sa vnútroštátne opatrenie považuje za opodstatnené a nesúlad produktu s digitálnymi prvkami sa pripisuje nedostatkom v harmonizovaných normách, Komisia uplatní postup stanovený v článku 10 nariadenia (EÚ) č. 1025/2012.

4. Ak sa vnútroštátne opatrenie považuje za opodstatnené a nesúlad produktu s digitálnymi prvkami sa pripisuje nedostatkom v európskom systéme certifikácie kybernetickej bezpečnosti uvedenom v článku 18, Komisia zváži, či má zmeniť alebo zrušiť vykonávací akt uvedený v článku 18 ods. 4, v ktorom sa uvádza predpoklad zhody týkajúci sa tohto systému certifikácie.

5. Ak sa vnútroštátne opatrenie považuje za opodstatnené a nesúlad produktu s digitálnymi prvkami sa pripisuje nedostatkom v spoločných špecifikáciách uvedených v článku 19, Komisia zváži, či má zmeniť alebo zrušiť vykonávací akt uvedený v článku 19, ktorým sa stanovujú tieto spoločné špecifikácie.

Článok 45

Postup na úrovni EÚ týkajúci sa produktov s digitálnymi prvkami, ktoré predstavujú významné kybernetickobezpečnostné riziko

1. Ak má Komisia dostatočné dôvody domnievať sa, a to aj na základe informácií poskytnutých agentúrou ENISA, že produkt s digitálnymi prvkami, ktorý predstavuje významné kybernetickobezpečnostné riziko, nie je v súlade s požiadavkami stanovenými v tomto nariadení, môže požiadať príslušné orgány dohľadu nad trhom, aby vykonali hodnotenie súladu a riadili sa postupmi uvedenými v článku 43.

2. Za mimoriadnych okolností, ktoré odôvodňujú okamžitý zásah na zachovanie riadneho fungovania vnútorného trhu, a ak má Komisia dostatočné dôvody domnievať sa, že produkt uvedený v odseku 1 naďalej nie je v súlade s požiadavkami stanovenými v tomto nariadení a príslušné orgány dohľadu nad trhom neprijali žiadne účinné opatrenia, môže Komisia požiadať agentúru ENISA, aby vykonala hodnotenie súladu. Komisia o tom informuje príslušné orgány dohľadu nad trhom. Príslušné hospodárske subjekty spolupracujú s agentúrou ENISA podľa potreby.

3. Komisia môže na základe hodnotenia od agentúry ENISA rozhodnúť, že sú potrebné nápravné alebo reštriktívne opatrenia na úrovni EÚ. Na tento účel bezodkladne konzultuje s dotknutými členskými štátmi a príslušným hospodárskym subjektom alebo príslušnými hospodárskymi subjektmi.

4. Na základe konzultácie uvedenej v odseku 3 môže Komisia prijať vykonávacie akty s cieľom rozhodnúť o nápravných alebo reštriktívnych opatreniach na úrovni Únie, ako aj nariadiť stiahnutie z trhu alebo od používateľov v primeranej lehote úmernej charakteru rizika. Tieto vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 51 ods. 2.

5. Komisia bezodkladne oznámi rozhodnutie uvedené v odseku 4 príslušnému hospodárskemu subjektu alebo príslušným hospodárskym subjektom. Členské štáty vykonávajú akty uvedené v odseku 4 bezodkladne a náležite o tom informujú Komisiu.

6. Odseky 2 až 5 sú uplatniteľné počas trvania výnimočnej situácie, ktorá odôvodnila zásah Komisie, a dovtedy, kým sa príslušný produkt neuvedie do súladu s týmto nariadením.

Článok 46

Vyhovujúce produkty s digitálnymi prvkami, ktoré predstavujú významné kybernetickobezpečnostné riziko

1. Ak orgán dohľadu nad trhom členského štátu po vykonaní hodnotenia podľa článku 43 zistí, že hoci sú produkty s digitálnymi prvkami a procesy zavedené výrobcom v súlade s týmto nariadením, predstavujú významné kybernetickobezpečnostné riziko a okrem toho ohrozujú zdravie alebo bezpečnosť ľudí, súlad s povinnosťami podľa práva Únie alebo vnútroštátneho práva určenými na ochranu základných práv, dostupnosť, pravosť, integritu alebo dôvernosť služieb

ponúkaných prostredníctvom elektronického informačného systému základnými subjektmi druhu uvedeného v [prílohe I k smernici XXX/XXXX (NIS2)], alebo iné aspekty ochrany verejného záujmu, požiada príslušný hospodársky subjekt, aby prijal všetky primerané opatrenia s cieľom zaistiť, aby už dotknutý produkt s digitálnymi prvkami a procesy zavedené výrobcom pri uvedení na trh toto riziko nepredstavovali, alebo aby stiahol produkt s digitálnymi prvkami z trhu alebo od používateľa v primeranej lehote úmernej charakteru rizika.

2. Výrobca alebo iné príslušné hospodárske subjekty zaistia prijatie nápravných opatrení v súvislosti s dotknutými produktmi s digitálnymi prvkami, ktoré sprístupnili na trhu v celej Únii v lehote, ktorú stanoví orgán dohľadu nad trhom členského štátu uvedený v odseku 1.

3. Členský štát bezodkladne informuje Komisiu a ostatné členské štáty o každom opatrení prijatom podľa odseku 1. Tieto informácie zahŕňajú všetky dostupné podrobnosti, najmä údaje potrebné na identifikáciu dotknutých produktov s digitálnymi prvkami, pôvod a dodávateľský reťazec týchto produktov s digitálnymi prvkami, charakter možného rizika, charakter a trvanie prijatých vnútroštátnych opatrení.

4. Komisia začne bezodkladne konzultácie s členskými štátmi a príslušnými hospodárskymi subjektmi a vyhodnotí prijaté vnútroštátne opatrenia. Na základe výsledkov tohto hodnotenia Komisia rozhodne, či opatrenie je alebo nie je opodstatnené, a v prípade potreby navrhne primerané opatrenia.

5. Rozhodnutie Komisie je určené členským štátom.

6. Ak má Komisia dostatočné dôvody domnievať sa, a to aj na základe informácií poskytnutých agentúrou ENISA, že produkt s digitálnymi prvkami, hoci je v súlade s týmto nariadením, predstavuje riziká uvedené v odseku 1, môže požiadať príslušný orgán alebo orgány dohľadu nad trhom, aby vykonali hodnotenie súladu a riadili sa postupmi uvedenými v článku 43 a v odsekoch 1, 2 a 3 tohto článku.

7. Za mimoriadnych okolností, ktoré odôvodňujú okamžitý zásah na zachovanie riadneho fungovania vnútorného trhu, a ak má Komisia dostatočné dôvody domnievať sa, že produkt uvedený v odseku 6 naďalej predstavuje riziká uvedené v odseku 1 a príslušné orgány dohľadu nad trhom neprijali žiadne účinné opatrenia, môže Komisia požiadať agentúru ENISA, aby vykonala hodnotenie rizík, ktoré predstavuje tento produkt, a informuje o tom príslušné orgány dohľadu nad trhom. Príslušné hospodárske subjekty spolupracujú s agentúrou ENISA podľa potreby.

8. Komisia môže na základe hodnotenia od agentúry ENISA uvedeného v odseku 7 stanoviť, že sú potrebné nápravné alebo reštriktívne opatrenia na úrovni EÚ. Na tento účel bezodkladne konzultuje s dotknutými členskými štátmi a príslušným hospodárskym subjektom alebo príslušnými hospodárskymi subjektmi.

9. Na základe konzultácie uvedenej v odseku 8 môže Komisia prijať vykonávacie akty s cieľom rozhodnúť o nápravných alebo reštriktívnych opatreniach na úrovni Únie, ako aj nariadiť stiahnutie z trhu alebo od používateľov v primeranej lehote úmernej charakteru rizika. Tieto vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 51 ods. 2.

10. Komisia bezodkladne oznámi rozhodnutie uvedené v odseku 9 príslušnému hospodárskemu subjektu alebo príslušným hospodárskym subjektom. Členské štáty vykonávajú takéto akty bezodkladne a náležite o tom informujú Komisiu.

11. Odseky 6 až 10 sa uplatňujú počas trvania výnimočnej situácie, ktorá odôvodnila zásah Komisie, a dovtedy, kým príslušný produkt naďalej predstavuje riziká uvedené v odseku 1.

Článok 47

Formálny nesúlad

1. Orgán dohľadu nad trhom členského štátu požiada príslušného výrobcu o odstránenie predmetného nesúladu, ak dospeje k jednému z týchto zistení:

   a) označenie zhody bolo umiestnené v rozpore s článkami 21 a 22;

   b) označenie zhody nebolo umiestnené;

   c) EÚ vyhlásenie o zhode nebolo vyhotovené;

   d) EÚ vyhlásenie o zhode nebolo vyhotovené správne;

   e) nebolo umiestnené identifikačné číslo notifikovanej osoby zapojenej v relevantných prípadoch do postupu posudzovania zhody;

   f) technická dokumentácia buď nie je k dispozícii, alebo nie je úplná.

2. Ak nesúlad uvedený v odseku 1 pretrváva, príslušný členský štát prijme všetky primerané opatrenia na obmedzenie alebo zakázanie sprístupnenia produktu s digitálnymi prvkami na trhu, alebo zaistenie jeho stiahnutia od používateľa alebo z trhu.

Článok 48

Spoločné činnosti orgánov dohľadu nad trhom

1. Orgány dohľadu nad trhom sa môžu dohodnúť s inými príslušnými orgánmi na vykonávaní spoločných činností zameraných na zaistenie kybernetickej bezpečnosti a ochrany spotrebiteľov v súvislosti s konkrétnymi produktmi s digitálnymi prvkami, ktoré sú uvedené na trh alebo sprístupnené na trhu, najmä produktmi, v prípade ktorých sa často zistí, že predstavujú kybernetickobezpečnostné riziká.

2. Komisia alebo agentúra ENISA môžu navrhnúť spoločné činnosti na kontrolovanie dodržiavania súladu s týmto nariadením, ktoré majú vykonávať orgány dohľadu nad trhom na základe údajov alebo informácií vo viacerých členských štátoch o možnom nesúlade produktov patriacich do rozsahu pôsobnosti tohto nariadenia s požiadavkami stanovenými v tomto nariadení.

3. Orgány dohľadu nad trhom a v prípade potreby Komisia zaistia, aby dohoda o výkone spoločných činností neviedla k nekalej hospodárskej súťaži medzi hospodárskymi subjektmi a aby nemala negatívny vplyv na objektívnosť, nezávislosť a nestrannosť strán dohody.

4. Orgán dohľadu nad trhom môže využiť akékoľvek informácie vyplývajúce z činností vykonávaných v rámci akéhokoľvek vyšetrovania, ktoré vykonáva.

5. Dotknutý orgán dohľadu nad trhom a prípadne Komisia sprístupnia verejnosti dohodu o spoločných činnostiach vrátane mien zúčastnených strán.

Článok 49

Kontrolné akcie

1. Orgány dohľadu nad trhom sa môžu rozhodnúť, že vykonajú súbežné koordinované kontrolné akcie (ďalej len „kontrolné akcie“) týkajúce sa konkrétnych produktov s digitálnymi prvkami alebo ich kategórií s cieľom skontrolovať súlad s týmto nariadením alebo odhaliť jeho porušenia.

2. Pokiaľ sa zapojené orgány dohľadu nad trhom nedohodnú inak, kontrolné akcie koordinuje Komisia. Koordinátor kontrolnej akcie môže v prípade potreby zverejniť jej súhrnné výsledky.

3. Agentúra ENISA môže pri plnení svojich úloh identifikovať, a to aj na základe oznámení prijatých podľa článku 11 ods. 1 a 2, kategórie produktov, pre ktoré sa môžu organizovať kontrolné akcie. Návrh kontrolných akcií sa predkladá potenciálnemu koordinátorovi uvedenému v odseku 2 na posúdenie orgánmi dohľadu nad trhom.

4. Pri vykonávaní kontrolných akcií môžu zapojené orgány dohľadu nad trhom využívať vyšetrovacie právomoci stanovené v článkoch 41 až 47 a akékoľvek iné právomoci, ktoré im boli udelené na základe vnútroštátneho práva.

5. Orgány dohľadu nad trhom môžu vyzvať úradníkov Komisie a iné sprevádzajúce osoby poverené Komisiou, aby sa zúčastnili na kontrolných akciách.

KAPITOLA VI

DELEGOVANÉ PRÁVOMOCI A POSTUP VÝBORU

Článok 50

Vykonávanie delegovania právomoci

1. Komisii sa udeľuje právomoc prijímať delegované akty za podmienok stanovených v tomto článku.

2. Komisii sa udeľuje právomoc prijímať delegované akty uvedené v článku 2 ods. 4, článku 6 ods. 2, 3 a 5, článku 20 ods. 5 a článku 23 ods. 5.

3. Delegovanie právomoci uvedené v článku 2 ods. 4, článku 6 ods. 2, 3 a 5, článku 20 ods. 5 a článku 23 ods. 5 môže Európsky parlament alebo Rada kedykoľvek odvolať. Rozhodnutím o odvolaní sa ukončuje delegovanie právomoci, ktoré sa v ňom uvádza. Rozhodnutie nadobúda účinnosť dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie* alebo k neskoršiemu dátumu, ktorý je v ňom určený. Nie je ním dotknutá platnosť delegovaných aktov, ktoré už nadobudli účinnosť.

4. Komisia pred prijatím delegovaného aktu konzultuje s expertmi určenými jednotlivými členskými štátmi v súlade so zásadami stanovenými v Medziinštitucionálnej dohode z 13. apríla 2016 o lepšej tvorbe práva.

5. Komisia oznamuje delegovaný akt hneď po jeho prijatí súčasne Európskemu parlamentu a Rade.

6. Delegovaný akt prijatý podľa článku 2 ods. 4, článku 6 ods. 2, 3 a 5, článku 20 ods. 5 a článku 23 ods. 5 nadobudne účinnosť, len ak Európsky parlament alebo Rada voči nemu nevzniesli námietku v lehote dvoch mesiacov odo dňa oznámenia uvedeného aktu Európskemu parlamentu a Rade alebo ak pred uplynutím uvedenej lehoty Európsky parlament a Rada informovali Komisiu o svojom rozhodnutí nevzniesť

námietku. Na podnet Európskeho parlamentu alebo Rady sa táto lehota predĺži o dva mesiace.

Článok 51

Postup výboru

1. Komisii pomáha výbor. Tento výbor je výborom v zmysle nariadenia (EÚ) č. 182/2011.
2. Ak sa odkazuje na tento odsek, uplatňuje sa článok 5 nariadenia (EÚ) č. 182/2011.
3. Ak sa má stanovisko výboru získať písomným postupom, tento postup sa ukončí bez výsledku, ak tak v rámci lehoty na vydanie stanoviska rozhodne predseda výboru alebo ak o to požiada člen výboru.

KAPITOLA VII

DÔVERNOSŤ A SANKCIE

Článok 52

Dôvernosť

1. Všetky strany, ktoré sa zúčastňujú na uplatňovaní tohto nariadenia, musia dodržiavať dôvernosť informácií a údajov získaných pri vykonávaní svojich úloh a činností takým spôsobom, aby chránili najmä:
   a) práva duševného vlastníctva a dôverné obchodné informácie alebo obchodné tajomstvo fyzickej alebo právnickej osoby vrátane zdrojového kódu s výnimkou prípadov uvedených v článku 5 smernice Európskeho parlamentu a Rady 2016/943[24];
   b) účinné vykonávanie tohto nariadenia, najmä na účely inšpekcií, vyšetrovaní alebo auditov;
   c) verejné záujmy a záujmy národnej bezpečnosti;
   d) integritu trestného alebo správneho konania.
2. Bez toho, aby bol dotknutý odsek 1, sa informácie, ktoré sa na základe dôvernosti vymieňajú medzi orgánmi dohľadu nad trhom navzájom a medzi orgánmi dohľadu nad trhom a Komisiou, nezverejňujú bez predchádzajúceho súhlasu orgánu dohľadu nad trhom, od ktorého tieto informácie pochádzajú.
3. Odsekmi 1 a 2 nie sú dotknuté práva a povinnosti Komisie, členských štátov a notifikovaných osôb, pokiaľ ide o výmenu informácií a šírenie upozornení, ani povinnosti dotknutých osôb poskytovať informácie podľa trestného práva členských štátov.
4. Komisia a členské štáty si v prípade potreby môžu vymieňať citlivé informácie s príslušnými orgánmi tretích krajín, s ktorými uzavreli bilaterálne alebo multilaterálne dohody o zachovaní dôvernosti zaručujúce primeranú úroveň ochrany.

[24] Smernica Európskeho parlamentu a Rady (EÚ) 2016/943 z 8. júna 2016 o ochrane nesprístupneného know-how a obchodných informácií (obchodného tajomstva) (Ú. v. EÚ L 157, 15.6.2016, s. 1).

Článok 53

Sankcie

1. Členské štáty stanovia pravidlá ukladania sankcií uplatniteľných v prípade porušenia tohto nariadenia hospodárskymi subjektmi a prijmú všetky potrebné opatrenia na zabezpečenie ich presadzovania. Stanovené sankcie musia byť účinné, primerané a odrádzajúce.

2. Členské štáty o týchto pravidlách a opatreniach bezodkladne informujú Komisiu a bezodkladne jej oznámia každú ďalšiu zmenu, ktorá sa ich týka.

3. Za nesúlad so základnými požiadavkami na kybernetickú bezpečnosť stanovenými v prílohe I a s povinnosťami stanovenými v článkoch 10 a 11 sa ukladajú správne pokuty do výšky 15 000 000 EUR alebo, ak je porušiteľom podnik, do výšky 2,5 % jeho celkového ročného celosvetového obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia.

4. Za nesúlad s akýmikoľvek inými povinnosťami poľa tohto nariadenia sa ukladajú správne pokuty do výšky 10 000 000 EUR alebo, ak je porušiteľom podnik, do výšky 2 % jeho celkového ročného celosvetového obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia.

5. Za poskytnutie nesprávnych, neúplných alebo zavádzajúcich informácií v odpovedi na žiadosť notifikovaných osôb a orgánov dohľadu nad trhom sa ukladajú správne pokuty do výšky 5 000 000 EUR alebo, ak je porušiteľom podnik, do výšky 1 % jeho celkového ročného celosvetového obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia.

6. Pri rozhodovaní o výške správnej pokuty sa v každom jednotlivom prípade zohľadnia všetky relevantné okolnosti konkrétnej situácie a náležite sa vezme do úvahy:

   a) povaha, závažnosť a trvanie porušenia a jeho dôsledkov;

   b) či už tomu istému hospodárskemu subjektu uložili za podobné porušenie správne pokuty iné orgány dohľadu nad trhom;

   c) veľkosť a trhový podiel hospodárskeho subjektu, ktorý sa dopustil porušenia.

7. Orgány dohľadu nad trhom, ktoré uplatňujú správne pokuty, poskytujú tieto informácie orgánom dohľadu nad trhom ostatných členských štátov prostredníctvom informačného a komunikačného systému uvedeného v článku 34 nariadenia (EÚ) 2019/1020.

8. Každý členský štát stanoví pravidlá, či a v akom rozsahu sa môžu správne pokuty uložiť orgánom verejnej moci a subjektom zriadeným v danom členskom štáte.

9. V závislosti od právneho systému členských štátov sa pravidlá o správnych pokutách môžu uplatňovať tak, aby pokuty ukladali príslušné vnútroštátne súdy alebo iné orgány podľa právomocí stanovených na vnútroštátnej úrovni v daných členských štátoch. Uplatňovanie takýchto pravidiel v uvedených členských štátoch má rovnocenný účinok.

10. Správne pokuty sa môžu v závislosti od okolností každého jednotlivého prípadu uložiť spolu s akýmikoľvek inými nápravnými alebo reštriktívnymi opatreniami, ktoré uplatnia orgány dohľadu nad trhom za to isté porušenie.

KAPITOLA VIII

PRECHODNÉ A ZÁVEREČNÉ USTANOVENIA

Článok 54

Zmena nariadenia (EÚ) 2019/1020

V prílohe I k nariadeniu (EÚ) 2019/1020 sa dopĺňa tento bod:

„71. [Nariadenie XXX][akt o kybernetickej odolnosti].“

Článok 55

Prechodné ustanovenia

1. Certifikáty EÚ skúšky typu a rozhodnutia o schválení vydané v súvislosti s požiadavkami na kybernetickú bezpečnosť produktov s digitálnymi prvkami, na ktoré sa vzťahujú iné harmonizačné právne predpisy Únie, zostávajú v platnosti do [42 mesiacov od dátumu nadobudnutia účinnosti tohto nariadenia], pokiaľ ich platnosť neuplynie pred týmto dátumom alebo pokiaľ nie je v iných právnych predpisoch Únie uvedené inak, pričom v takom prípade zostávajú v platnosti tak, ako sa uvádza v daných právnych predpisoch Únie.
2. Na produkty s digitálnymi prvkami, ktoré boli uvedené na trh pred [dátum začatia uplatňovania tohto nariadenia uvedený v článku 57], sa vzťahujú požiadavky tohto nariadenia len vtedy, ak sú tieto produkty od uvedeného dátumu predmetom podstatnej úpravy svojho dizajnu alebo zamýšľaného účelu.
3. Odchylne od odseku 2 sa povinnosti stanovené v článku 11 uplatňujú na všetky produkty s digitálnymi prvkami v rozsahu pôsobnosti tohto nariadenia, ktoré boli uvedené na trh pred [dátum začatia uplatňovania tohto nariadenia uvedený v článku 57].

Článok 56

Hodnotenie a preskúmanie

Komisia do [36 mesiacov od dátumu začatia uplatňovania tohto nariadenia] a potom každé štyri roky predloží Európskemu parlamentu a Rade správu o hodnotení a preskúmaní tohto nariadenia. Tieto správy sa zverejnia.

Článok 57

Nadobudnutie účinnosti a uplatňovanie

Toto nariadenie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Uplatňuje sa od [24 mesiacov od dátumu nadobudnutia účinnosti tohto nariadenia]. Článok 11 sa však uplatňuje od [12 mesiacov od dátumu nadobudnutia účinnosti tohto nariadenia].

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli

Za Európsky parlament	*Za Radu*
predseda/predsedníčka	*predseda/predsedníčka*

LEGISLATÍVNY FINANČNÝ VÝKAZ

1. RÁMEC NÁVRHU/INICIATÍVY

1.1. Názov návrhu/iniciatívy

1.2. Príslušné oblasti politiky

1.3. Návrh/iniciatíva sa týka:

1.4. Ciele

1.4.1. Všeobecné ciele

1.4.2. Špecifické ciele

1.4.3. Očakávané výsledky a vplyv

1.4.4. Ukazovatele výkonnosti

1.5. Dôvody návrhu/iniciatívy

1.5.1. Požiadavky, ktoré sa majú splniť v krátkodobom alebo dlhodobom horizonte vrátane podrobného harmonogramu prvotnej fázy vykonávania iniciatívy

1.5.2. Prínos zapojenia Únie (môže byť výsledkom rôznych faktorov, napr. lepšej koordinácie, právnej istoty, väčšej účinnosti alebo komplementárnosti). Na účely tohto bodu je „prínos zapojenia Únie“ hodnota vyplývajúca zo zásahu Únie, ktorá dopĺňa hodnotu, ktorú by inak vytvorili len samotné členské štáty.

1.5.3. Poznatky získané z podobných skúseností v minulosti

1.5.4. Zlučiteľnosť s viacročným finančným rámcom a možná synergia s inými vhodnými nástrojmi

1.5.5. Posúdenie rôznych disponibilných možností financovania vrátane možnosti prerozdelenia

1.6. Trvanie a finančný vplyv návrhu/iniciatívy

1.7. Plánovaný spôsob riadenia

2. OPATRENIA V OBLASTI RIADENIA

2.1. Zásady monitorovania a predkladania správ

2.2. Systémy riadenia a kontroly

2.2.1. Opodstatnenie navrhovaných spôsobov riadenia, mechanizmov vykonávania financovania, spôsobov platby a stratégie kontroly

2.2.2. Informácie o zistených rizikách a systémoch vnútornej kontroly zavedených na ich zmierňovanie

2.2.3. Odhad a opodstatnenie nákladovej účinnosti kontrol (pomer medzi nákladmi na kontroly a hodnotou súvisiacich riadených finančných prostriedkov) a posúdenie očakávaných úrovní rizika chyby (pri platbe a uzavretí)

2.3. Opatrenia na predchádzanie podvodom a nezrovnalostiam

3. ODHADOVANÝ FINANČNÝ VPLYV NÁVRHU/INICIATÍVY

3.1. Príslušné okruhy viacročného finančného rámca a rozpočtové riadky výdavkov

3.2. Odhadovaný finančný vplyv návrhu na rozpočtové prostriedky

3.2.1. Zhrnutie odhadovaného vplyvu na operačné rozpočtové prostriedky

3.2.2. Odhadované výsledky financované z operačných rozpočtových prostriedkov

3.2.3. Zhrnutie odhadovaného vplyvu na administratívne rozpočtové prostriedky

3.2.4. Súlad s platným viacročným finančným rámcom

3.2.5. Príspevky od tretích strán

3.3. Odhadovaný vplyv na príjmy

LEGISLATÍVNY FINANČNÝ VÝKAZ

1. RÁMEC NÁVRHU/INICIATÍVY

1.1. Názov návrhu/iniciatívy

Návrh nariadenia o horizontálnych požiadavkách kybernetickej bezpečnosti produktov s digitálnymi prvkami (akt o kybernetickej odolnosti)

1.2. Príslušné oblasti politiky

Komunikačné siete, obsah a technológie

1.3. Návrh/iniciatíva sa týka:

× **novej akcie**

☐ **novej akcie, ktorá nadväzuje na pilotný projekt/prípravnú akciu**[37]

☐ **predĺženia trvania existujúcej akcie**

☐ **zlúčenia jednej alebo viacerých akcií do ďalšej/novej akcie alebo presmerovania jednej alebo viacerých akcií na ďalšiu/novú akciu**

1.4. Ciele

1.4.1. Všeobecné ciele

Návrh má dva hlavné ciele zamerané na zabezpečenie riadneho fungovania vnútorného trhu: 1. **vytvoriť podmienky pre vývoj bezpečných produktov s digitálnymi prvkami** tým, že sa zaistí, aby sa hardvérové a softvérové produkty uvádzali na trh s menším počtom zraniteľností a aby výrobcovia brali bezpečnosť vážne počas celého životného cyklu produktu a 2. **vytvoriť podmienky, ktoré používateľom umožnia zohľadniť kybernetickú bezpečnosť pri výbere a používaní produktov s digitálnymi prvkami**.

1.4.2. Špecifické ciele

V tomto návrhu boli stanovené **štyri špecifické ciele**: i) zaistiť, aby výrobcovia zlepšili bezpečnosť produktov s digitálnymi prvkami od fázy návrhu a vývoja počas celého životného cyklu; ii) zaistiť koherentný rámec kybernetickej bezpečnosti uľahčením dodržiavania pravidiel výrobcami hardvéru a softvéru; iii) zvýšiť transparentnosť bezpečnostných vlastností produktov s digitálnymi prvkami a iv) umožniť podnikom a spotrebiteľom bezpečné používanie produktov s digitálnymi prvkami.

Očakávané výsledky a vplyv

Uveďte, aký vplyv by mal mať návrh/iniciatíva na prijímateľov/cieľové skupiny.

Návrh by priniesol značné prínosy rôznym zainteresovaným stranám. V prípade podnikov by sa zabránilo rozdielnym bezpečnostným pravidlám pre produkty s digitálnymi prvkami a znížili by sa náklady na dodržiavanie príslušných právnych predpisov v oblasti kybernetickej bezpečnosti. Znížil by sa počet kybernetických bezpečnostných incidentov, náklady na ich riešenie incidentu a poškodenie dobrého mena. V prípade celej EÚ sa odhaduje, že iniciatíva by mohla viesť k zníženiu

[37] Podľa článku 58 ods. 2 písm. a) alebo b) nariadenia o rozpočtových pravidlách.

nákladov, ktoré z incidentov vznikajú podnikom, približne o 180 až 290 miliárd EUR ročne[38]. Viedla by k zvýšenému obratu vďaka využívaniu produktov s digitálnymi prvkami. Zlepšila by sa celková dobrá povesť spoločností, čo by podnietilo zvýšenie dopytu aj mimo EÚ. Uprednostňovaná možnosť by pre používateľov zvýšila transparentnosť bezpečnostných vlastností a uľahčila by používanie produktov s digitálnymi prvkami. Aj spotrebitelia a občania by mali prínos z lepšej ochrany svojich práv, ako je ochrana súkromia a ochrana osobných údajov.

Súčasne by sa podnikom, notifikovaným osobám a subjektom verejného sektora vrátane akreditačných orgánov a orgánov dohľadu nad trhom v dôsledku návrhu zvýšili náklady na dodržiavanie a presadzovanie predpisov. Vývojárom softvéru a výrobcom hardvéru sa návrhom zvýšia priame náklady na dodržiavanie predpisov vzhľadom na nové bezpečnostné požiadavky, posudzovanie zhody, dokumentáciu a oznamovacie povinnosti, vedúce k súhrnným nákladom na dodržiavanie predpisov až do výške približne 29 miliárd EUR pri odhadovanej trhovej hodnote obratu vo výške 1 485 miliárd EUR[39]. Používatelia vrátane komerčných používateľov, spotrebitelia a občania môžu čeliť vyšším cenám produktov s digitálnymi prvkami. Posudzovať by sa však mali so zreteľom na vyššie opísané značné prínosy.

1.4.3. Ukazovatele výkonnosti

Uveďte ukazovatele na monitorovanie pokroku a dosiahnutých výsledkov.

S cieľom vyskúšať, či výrobcovia zlepšujú bezpečnosť svojich produktov s digitálnymi prvkami od fázy návrhu a vývoja a počas celého životného cyklu týchto produktov, dali by sa vziať do úvahy viaceré ukazovatele. Mohlo by ísť o počet významných incidentov v Únii spôsobených zraniteľnosťami, podiel výrobcov hardvéru a softvéru, ktorí sledujú systematicky bezpečný vývoj životného cyklu, kvalitatívnu analýzu bezpečnosti produktov s digitálnymi prvkami, kvantitatívne a kvalitatívne posúdenie databáz zraniteľnosti, frekvenciu bezpečnostných záplat sprístupnených výrobcami alebo priemerný počet dní od objavenia zraniteľnosti do poskytnutia bezpečnostných záplat.

Ukazovateľom koherentného rámca kybernetickej bezpečnosti by mohol byť nedostatok cielených vnútroštátnych právnych predpisov v oblasti kybernetickej bezpečnosti zameraných na konkrétny produkt.

Ukazovateľom lepšej transparentnosti, pokiaľ ide o bezpečnostné vlastnosti produktov s digitálnymi prvkami, by mohol byť podiel produktov s digitálnymi prvkami, ktoré sa dodávajú s informáciami o bezpečnostných vlastnostiach. Podiel produktov s digitálnymi prvkami, ktoré sa dodávajú s pokynmi pre používateľov na bezpečné používanie, by sa navyše mohol použiť ako ukazovateľ toho, či majú organizácie a spotrebitelia možnosť používať produkty s digitálnymi prvkami bezpečne.

Čo sa týka monitorovania vplyvu regulácie, na tento účel by sa zvažovali určité ukazovatele, ktoré by posúdila Komisia, prípadne s podporou agentúry ENISA.

[38] Pozri [pracovný dokument útvarov Komisie o posúdení vplyvu, ktorý je sprievodným dokumentom k nariadeniu o horizontálnych požiadavkách kybernetickej bezpečnosti produktov s digitálnymi prvkami].

[39] Pozri [pracovný dokument útvarov Komisie o posúdení vplyvu, ktorý je sprievodným dokumentom k nariadeniu o horizontálnych požiadavkách kybernetickej bezpečnosti produktov s digitálnymi prvkami].

V závislosti od operačného cieľa, ktorý sa má dosiahnuť, niektoré monitorovacie ukazovatele, na základe ktorých by sa posudzoval úspech horizontálnych požiadaviek kybernetickej bezpečnosti, sú tieto:

Na posúdenie úrovne kybernetickej bezpečnosti produktov s digitálnymi prvkami:

– Štatistika a kvalitatívna analýza incidentov ovplyvňujúcich produkty s digitálnymi prvkami a spôsob, akým sa tieto riešili. Zhromažďovať a posudzovať by ich mohla Komisia s podporou agentúry ENISA.

– Záznamy o známych zraniteľnostiach a analýzy, ako sa tieto riešili. Takúto analýzu by mohla vykonať agentúra ENISA na základe európskej databázy zraniteľností zriadenej na základe [smernice XXX/XXXX (NIS2)].

– Prieskumy medzi výrobcami hardvéru a softvéru s cieľom monitorovať pokrok.

Na posúdenie úrovne informovanosti o bezpečnostných prvkoch, bezpečnostnej podpore, skončení životnosti a povinnej starostlivosti: výsledky prieskumu, ktorý má vykonať Komisia s podporou agentúry ENISA tak pre používateľov, ako aj podniky.

Na posúdenie vykonávania by sa Komisia zamerala na zabezpečenie toho, aby sa posudzovanie zhody vykonávalo účinne. Na tento účel sa vydá mandát na tvorbu normy s jej následnou realizáciou. Komisia takisto overí kapacitu notifikovaných osôb a prípadne aj certifikačných orgánov.

Pokiaľ ide o uplatňovanie, na základe správ členských štátov bude Komisia overovať, že sa národné iniciatívy netýkajú aspektov, na ktoré sa vzťahuje nariadenie.

1.5. Dôvody návrhu/iniciatívy

1.5.1. Požiadavky, ktoré sa majú splniť v krátkodobom alebo dlhodobom horizonte vrátane podrobného harmonogramu prvotnej fázy vykonávania iniciatívy

Nariadenie by malo byť v plnej miere uplatniteľné 24 mesiacov po nadobudnutí účinnosti. Prvky riadiacej štruktúry by však mali byť zavedené ešte predtým. Členské štáty musia mať najmä vymenované existujúce orgány a/alebo zriadené nové orgány, ktoré budú plniť úlohy stanovené v právnych predpisoch.

1.5.2. Prínos zapojenia Únie (môže byť výsledkom rôznych faktorov, napr. lepšej koordinácie, právnej istoty, väčšej účinnosti alebo komplementárnosti). Na účely tohto bodu je „prínos zapojenia Únie“ hodnota vyplývajúca zo zásahu Únie, ktorá dopĺňa hodnotu, ktorú by inak vytvorili len samotné členské štáty.

Z výrazného cezhraničného charakteru kybernetickej bezpečnosti a rastúceho počtu incidentov s účinkami, ktoré presahujú hranice, odvetvia a produkty, vyplýva, že ciele nemožno účinne dosiahnuť len na úrovni členských štátov. Vzhľadom na globálny charakter trhov s produktmi s digitálnymi prvkami čelia členské štáty na svojom území v prípade toho istého produktu s digitálnymi prvkami rovnakým rizikám. Vznikajúci rôznorodý rámec potenciálne odlišných vnútroštátnych pravidiel takisto prináša riziká, ktoré narúšajú otvorený a konkurencieschopný jednotný trh s produktmi s digitálnymi prvkami. Potrebné je preto spoločné opatrenie na úrovni EÚ, aby sa zvýšila úroveň dôvery medzi používateľmi a atraktívnosť produktov EÚ s digitálnymi prvkami. Aj vnútornému trhu by prospelo, keby sa zabezpečila právna istota a dosiahli rovnaké podmienky pre predajcov produktov s digitálnymi prvkami.

1.5.3. Poznatky získané z podobných skúseností v minulosti

Akt o kybernetickej odolnosti je prvým nariadením tohto druhu, ktorým sa zavádzajú požiadavky kybernetickej bezpečnosti pri uvádzaní produktov s digitálnymi prvkami na trh. Nadväzuje však na podmienky nového legislatívneho rámca a poznatky získané v procese vykonávania existujúcich harmonizačných právnych predpisov Únie týkajúcich sa rôznych produktov, najmä pokiaľ ide o prípravu vykonávania vrátane aspektov, ako je príprava harmonizovaných noriem.

1.5.4. Zlučiteľnosť s viacročným finančným rámcom a možná synergia s inými vhodnými nástrojmi

Nariadenie o horizontálnych požiadavkách kybernetickej bezpečnosti produktov s digitálnymi prvkami vymedzuje nové požiadavky kybernetickej bezpečnosti pre všetky produkty s digitálnymi prvkami uvádzané na trh EÚ, pričom prekračuje akékoľvek požiadavky stanovené existujúcimi právnymi predpismi. Návrh zároveň nadväzuje na existujúce ustanovenia právnych predpisov nového legislatívneho rámca. Preto by nadviazal na existujúce štruktúry a postupy nového legislatívneho rámca, ako sú spolupráca notifikovaných osôb a dohľad nad trhom, moduly posudzovania zhody, vývoj harmonizovaných noriem. Nový návrh takisto vychádza z niektorých štruktúr vyvinutých podľa iných právnych predpisov o kybernetickej bezpečnosti, ako sú smernica 2016/1148 (smernica NIS), resp. [smernica XXX/XXXX (NIS2)] alebo nariadenie 2019/881 (akt o kybernetickej bezpečnosti).

1.5.5. Posúdenie rôznych disponibilných možností financovania vrátane možnosti prerozdelenia

Riadenie oblastí činnosti pridelených agentúre ENISA sa zhoduje s jej existujúcim mandátom a všeobecnými úlohami. Tieto oblasti činnosti si môžu vyžadovať osobitné profily alebo nové úlohy, ale tie nemusia byť dôležité a dajú sa zvládnuť s existujúcimi zdrojmi agentúry ENISA a vyriešiť presunom alebo prepojením s rôznymi úlohami. Napríklad jedna z hlavných oblastí činnosti pridelených agentúre ENISA sa týka zhromažďovania a spracúvania oznámení výrobcov o zneužitých zraniteľnostiach produktov. V [smernici XXX/XXXX (NIS2)] sa už uložilo agentúre ENISA zriadiť európsku databázu zraniteľností, v ktorej možno dobrovoľne zverejniť a zaregistrovať verejne známe zraniteľnosti na účel umožňujúci používateľom prijať primerané zmierňujúce opatrenia. Zdroje pridelené na tento účel by sa mohli použiť aj na nové uvedené úlohy týkajúce sa oznámení o zraniteľnostiach produktov. Tým by sa mohlo zabezpečiť účinné využitie existujúcich zdrojov a vytvorila by sa aj potrebná synergia medzi takýmito úlohami, ktoré môžu lepšie formovať analýzy agentúry ENISA týkajúce sa kybernetickobezpečnostných rizík a hrozieb.

1.6. Trvanie a finančný vplyv návrhu/iniciatívy

☐ **obmedzené trvanie**

– ☐ v platnosti od [DD/MM]RRRR do [DD/MM]RRRR

– ☐ Finančný vplyv na viazané rozpočtové prostriedky od RRRR do RRRR a na platobné rozpočtové prostriedky od RRRR do RRRR.

× **neobmedzené trvanie**

– Počiatočná fáza sa začne vykonávať od roku 2025

– a potom bude implementácia pokračovať v plnom rozsahu.

1.7. Plánovaný spôsob riadenia[40]

☐ **Priame riadenie** na úrovni Komisie

– × prostredníctvom jej útvarov vrátane vlastných zamestnancov v delegáciách Únie;

– ☐ prostredníctvom výkonných agentúr

☐ **Zdieľané riadenie** s členskými štátmi

☐ **Nepriame riadenie**, pri ktorom sa plnením rozpočtu poveria:

– ☐ tretie krajiny alebo subjekty, ktoré tieto krajiny určili,

– ☐ medzinárodné organizácie a ich agentúry (uveďte),

– ☐ Európska investičná banka (EIB) a Európsky investičný fond,

– ☐ subjekty uvedené v článkoch 70 a 71 nariadenia o rozpočtových pravidlách,

– ☐ verejnoprávne subjekty,

– ☐ súkromnoprávne subjekty poverené vykonávaním verejnej služby v rozsahu, v akom sú im poskytnuté primerané finančné záruky,

– ☐ súkromnoprávne subjekty spravované právom členského štátu, ktoré sú poverené vykonávaním verejno-súkromného partnerstva a ktorým sú poskytnuté primerané finančné záruky,

– ☐ osoby poverené vykonávaním osobitných činností v oblasti SZBP podľa hlavy V Zmluvy o Európskej únii a určené v príslušnom základnom akte.

– *V prípade viacerých spôsobov riadenia uveďte v oddiele „Poznámky“ presnejšie vysvetlenie.*

Poznámky

Týmto nariadením sa agentúre ENISA ukladajú určité činnosti v súlade s jej existujúcim mandátom, a najmä s článkom 3 ods. 2 nariadenia 2019/881, v ktorom sa stanovuje, že agentúra ENISA plní úlohy, ktoré jej boli zverené v právnych aktoch Únie, v ktorých sa stanovujú opatrenia na aproximáciu zákonov, iných právnych predpisov a správnych opatrení členského štátu v oblasti kybernetickej bezpečnosti. Úlohou agentúry ENISA je najmä prijímať od výrobcov oznámenia o aktívne zneužívaných zraniteľnostiach obsiahnutých v ich produktoch s digitálnymi prvkami, ako aj o incidentoch, ktoré ovplyvnili bezpečnosť týchto

[40] Vysvetlenie spôsobov riadenia a odkazy na nariadenie o rozpočtových pravidlách sú k dispozícii na webovom sídle BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

produktov. Agentúra ENISA by mala tieto oznámenia postupovať buď príslušným jednotkám CSIRT, alebo príslušnému národnému miestu jednotného kontaktu určenému v súlade s článkom [článok X] smernice [smernica XXX/XXXX (NIS2)] a informovať orgány dohľadu nad trhom. Agentúra ENISA by na základe informácií, ktoré zhromažďuje, mala vypracovať každé dva roky technickú správu o vznikajúcich trendoch týkajúcich sa kybernetickobezpečnostných rizík produktov s digitálnymi prvkami a predložiť ju skupine pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti. Vzhľadom na odborné znalosti agentúry ENISA, zhromaždené informácie a analýzy hrozieb môže agentúra ENISA okrem toho podporiť proces vykonávania tohto nariadenia návrhom spoločných činností, ktoré by mali vykonávať národné orgány dohľadu nad trhom na základe údajov alebo informácií o možnom nesúlade produktov s digitálnymi prvkami s týmto nariadením vo viacerých členských štátoch, alebo identifikovať kategórie produktov, pri ktorých by sa mohli organizovať súbežné koordinované kontrolné opatrenia. Komisia môže požiadať agentúru ENISA, aby vykonala hodnotenie konkrétnych produktov za mimoriadnych okolností v súvislosti s produktmi s digitálnymi prvkami, ktoré predstavujú významné kybernetickobezpečnostné riziko, a za ktorých sa vyžaduje okamžitý zásah v záujme ochrany riadneho fungovania vnútorného trhu.

Na všetky tieto úlohy sa odhaduje potreba 4,5 ekvivalentu plného pracovného času z existujúcich zdrojov agentúry ENISA, už v nadväznosti na znalosti a prípravné práce, ktoré agentúra ENISA v súčasnosti vykonáva, okrem iného na podporu nadchádzajúceho vykonávania [smernice XXX/XXXX (NIS2)], na ktoré boli zdroje agentúry ENISA doplnené.

2. OPATRENIA V OBLASTI RIADENIA

2.1. Zásady monitorovania a predkladania správ

Uveďte frekvenciu a podmienky, ktoré sa vzťahujú na tieto opatrenia.

Komisia do 36 mesiacov od dátumu začiatku uplatňovania tohto nariadenia a potom každé štyri roky predloží Európskemu parlamentu a Rade správu o jeho vyhodnotení a preskúmaní. Tieto správy sa zverejnia.

2.2. Systémy riadenia a kontroly

2.2.1. Opodstatnenie navrhovaných spôsobov riadenia, mechanizmov vykonávania financovania, spôsobov platby a stratégie kontroly

Týmto nariadením sa ustanovuje nová politika, pokiaľ ide o harmonizované požiadavky kybernetickej bezpečnosti produktov s digitálnymi prvkami umiestňovaných na vnútorný trh počas celého ich životného cyklu Na právny akt nadviažu požiadavky Komisie voči európskym organizáciám pre normalizáciu, aby vypracovali normy.

Na tieto nové úlohy je potrebné vybaviť útvary Komisie primeranými zdrojmi. Odhaduje sa, že presadzovanie nového nariadenia si vyžiada 7 ekvivalentov plného pracovného času (z toho jeden VNE) na plnenie týchto úloh:

- pripraviť mandát na tvorbu normy a/alebo spoločné špecifikácie prostredníctvom vykonávacích aktov bez úspešného procesu normalizácie,
- vypracovať delegovaný akt [do 12 mesiacov od nadobudnutia účinnosti nariadenia], v ktorom sa vymedzujú kritické produkty s digitálnymi prvkami,
- potenciálna príprava delegovaných aktov na účely aktualizovania zoznamu kritických produktov triedy I a II; špecifikovania, či je potrebné obmedzenie alebo vylúčenie produktov s digitálnymi prvkami, na ktoré sa vzťahujú iné pravidlá Únie, ktorými sa stanovujú požiadavky na dosiahnutie rovnakej úrovne ochrany ako týmto nariadením; stanovenia povinnosti certifikácie určitých vysokokritických produktov s digitálnymi prvkami na základe kritérií stanovených v tomto nariadení; špecifikovania minimálneho obsahu EÚ vyhlásenia o zhode a doplnenia prvkov, ktoré sa majú zahrnúť do technickej dokumentácie,
- potenciálna príprava vykonávacích aktov týkajúcich sa formátu alebo prvkov oznamovacích povinností, softvérového kusovníka, spoločných špecifikácií alebo pripojenia označenia CE,
- potenciálna príprava okamžitého zásahu s uložením nápravných alebo reštriktívnych opatrení za mimoriadnych okolností s cieľom zachovať riadne fungovanie vnútorného trhu vrátane prípravy vykonávacieho aktu,
- organizácia a koordinácia notifikácií notifikovaných osôb členskými štátmi a koordinácia notifikovaných osôb,
- podpora koordinácie orgánov dohľadu nad trhom členských štátov.

2.2.2. Informácie o zistených rizikách a systémoch vnútornej kontroly zavedených na ich zmierňovanie

V záujme zabezpečenia, aby si notifikované osoby a orgány dohľadu nad trhom vymieňali informácie a riadne spolupracovali, je Komisia poverená ich koordináciou. Na získanie technických znalostí a poznatkov o trhu by sa vytvorila skupina odborníkov.

2.2.3. Odhad a opodstatnenie nákladovej účinnosti kontrol (pomer medzi nákladmi na kontroly a hodnotou súvisiacich riadených finančných prostriedkov) a posúdenie očakávaných úrovní rizika chyby (pri platbe a uzavretí)

2.3. Pokiaľ ide o výdavky na zasadnutia, vzhľadom na nízku hodnotu na jednu transakciu (napr. preplatenie cestovných nákladov delegátovi za zasadnutie), štandardné kontrolné postupy sa zdajú postačujúce. Opatrenia na predchádzanie podvodom a nezrovnalostiam

Uveďte existujúce alebo plánované preventívne a ochranné opatrenia, napr. zo stratégie na boj proti podvodom.

Existujúce opatrenia boja proti podvodom uplatniteľné na Komisiu sa budú vzťahovať na dodatočné rozpočtové prostriedky potrebné pre toto nariadenie.

3. ODHADOVANÝ FINANČNÝ VPLYV NÁVRHU/INICIATÍVY

3.1. Príslušné okruhy viacročného finančného rámca a rozpočtové riadky výdavkov

- Existujúce rozpočtové riadky

Schéma

- Požadované nové rozpočtové riadky

Neuvádza sa

3.2. Odhadovaný finančný vplyv návrhu na rozpočtové prostriedky

3.2.1. Zhrnutie odhadovaného vplyvu na operačné rozpočtové prostriedky

– ☑ Návrh/iniciatíva si nevyžaduje použitie operačných rozpočtových prostriedkov.

– ☐ Návrh/iniciatíva si vyžaduje použitie týchto operačných rozpočtových prostriedkov:

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Okruh viacročného finančného rámca	Číslo	

GR: <…….>			Rok **N**[41]	Rok **N + 1**	Rok **N + 2**	Rok **N + 3**	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)			**SPOLU**
• Operačné rozpočtové prostriedky										
Rozpočtový riadok[42]	Záväzky	(1a)								
	Platby	(2a)								
Rozpočtový riadok	Záväzky	(1b)								
	Platby	(2b)								
Administratívne rozpočtové prostriedky financované z finančného krytia na vykonávanie osobitných programov[43]										
Rozpočtový riadok		(3)								
Rozpočtové prostriedky pre GR <…….> SPOLU	Záväzky	= 1a + 1b + 3								
	Platby	= 2a + 2b								

41 Rok N je rokom, v ktorom sa návrh/iniciatíva začína vykonávať. Nahraďte „N“ očakávaným prvým rokom vykonávania (napríklad: 2021). To isté urobte aj pri nasledujúcich rokoch.

42 Podľa oficiálnej rozpočtovej nomenklatúry.

43 Technická a/alebo administratívna pomoc a výdavky na podporu vykonávania programov a/alebo akcií EÚ (pôvodné rozpočtové riadky „BA“), nepriamy výskum, priamy výskum.

		+ 3								

• Operačné rozpočtové prostriedky SPOLU	Záväzky	(4)								
	Platby	(5)								
• Administratívne rozpočtové prostriedky financované z finančného krytia na vykonávanie osobitných programov SPOLU		(6)								
Rozpočtové prostriedky OKRUHU <….> viacročného finančného rámca **SPOLU**	Záväzky	= 4 + 6								
	Platby	= 5 + 6								

Ak má návrh/iniciatíva vplyv na viaceré operačné okruhy, zopakujte oddiel uvedený vyššie:

• Operačné rozpočtové prostriedky SPOLU (všetky operačné okruhy)	Záväzky	(4)								
	Platby	(5)								
Administratívne rozpočtové prostriedky financované z finančného krytia na vykonávanie osobitných programov SPOLU (všetky operačné okruhy)		(6)								
Rozpočtové prostriedky OKRUHOV 1 až 6 viacročného finančného rámca **SPOLU** (referenčná suma)	Záväzky	= 4 + 6								
	Platby	= 5 + 6								

Okruh viacročného finančného rámca	**7**	„Administratívne výdavky“

Tento oddiel treba vyplniť s použitím rozpočtových údajov administratívnej povahy, ktoré sa najprv uvedú v prílohe k legislatívnemu finančnému výkazu (príloha V k interným pravidlám), ktorá sa na účely medziútvarovej konzultácie nahrá do aplikácie DECIDE.

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

		Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**SPOLU**
GR: CNECT						
• Ľudské zdroje		1,030	1,030	1,030	1,030	**4,120**
• Ostatné administratívne výdavky		**0,222**	**0,222**	**0,222**	**0,222**	**0,888**
GR CNECT **SPOLU**	Rozpočtové prostriedky	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

Rozpočtové prostriedky OKRUHU 7 viacročného finančného rámca **SPOLU**	(Záväzky spolu = Platby spolu)	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

		Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**SPOLU**
Rozpočtové prostriedky OKRUHOV 1 až 7 viacročného finančného rámca **SPOLU**	Záväzky	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**
	Platby	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

3.2.2. Odhadované výsledky financované z operačných rozpočtových prostriedkov

viazané rozpočtové prostriedky v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Uveďte ciele a výstupy			Rok **N**	Rok **N + 1**	Rok **N + 2**	Rok **N + 3**	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)	**SPOLU**
	VÝSTUPY							

⇩	Druh 44	Priemerné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet spolu	Náklady spolu
ŠPECIFICKÝ CIEĽ č. 1[45]…																		
– Výstup																		
– Výstup																		
– Výstup																		
Špecifický cieľ č. 1 medzisúčet																		
ŠPECIFICKÝ CIEĽ č. 2 …																		
– Výstup																		
Špecifický cieľ č. 2 medzisúčet																		
SPOLU																		

[44] Výstupy sú produkty, ktoré sa majú dodať, a služby, ktoré sa majú poskytnúť (napr. počet financovaných výmen študentov, vybudované cesty v km atď.).

[45] Ako je uvedené v bode 1.4.2. „Špecifické ciele…“

3.2.3. Zhrnutie odhadovaného vplyvu na administratívne rozpočtové prostriedky

– ☐ Návrh/iniciatíva si nevyžaduje použitie administratívnych rozpočtových prostriedkov

– ☑ Návrh/iniciatíva si vyžaduje použitie týchto administratívnych rozpočtových prostriedkov:

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	
OKRUH 7 viacročného finančného rámca					
Ľudské zdroje	1,030	1,030	1,030	1,030	**4,120**
Iné administratívne výdavky	0,222	0,222	0,222	0,222	**0,888**
Medzisúčet OKRUHU 7 viacročného finančného rámca	1,252	1,252	1,252	1,252	**5,008**

Mimo OKRUHU 7[46] **viacročného finančného rámca**					
Ľudské zdroje					
Ostatné administratívne výdavky					
Medzisúčet mimo OKRUHU 7 viacročného finančného rámca					

SPOLU	1,252	1,252	1,252	1,252	**5,008**

Rozpočtové prostriedky potrebné na ľudské zdroje a na ostatné administratívne výdavky budú pokryté rozpočtovými prostriedkami GR, ktoré už boli pridelené na riadenie akcie a/alebo boli prerozdelené v rámci GR, a v prípade potreby budú doplnené zdrojmi, ktoré sa môžu prideliť riadiacemu GR v rámci ročného postupu prideľovania zdrojov a v závislosti od rozpočtových obmedzení.

[46] Technická a/alebo administratívna pomoc a výdavky na podporu vykonávania programov a/alebo akcií EÚ (pôvodné rozpočtové riadky „BA“), nepriamy výskum, priamy výskum.

3.2.3.1. Odhadované potreby ľudských zdrojov

– ☐ Návrh/iniciatíva si nevyžaduje použitie ľudských zdrojov.

– ☑ Návrh/iniciatíva si vyžaduje použitie týchto ľudských zdrojov:

odhady sa vyjadrujú v jednotkách ekvivalentu plného pracovného času

		Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**
20 01 02 01 (ústredie a zastúpenia Komisie)		6	6	6	6
20 01 02 03 (delegácie)					
01 01 01 01 (nepriamy výskum)					
01 01 01 11 (priamy výskum)					
Iné rozpočtové riadky (uveďte)					
• Externí zamestnanci (v ekvivalente plného pracovného času: FTE)[47]					
20 02 01 (ZZ, VNE, DAZ z celkového finančného krytia)		1	1	1	1
20 02 03 (ZZ, MZ, VNE, DAZ a PED v delegáciách)					
XX 01 xx **yy zz** [48]	– ústredie				
	– delegácie				
01 01 01 02 (ZZ, VNE, DAZ, – nepriamy výskum)					
01 01 01 12 (ZZ, VNE, DAZ – priamy výskum)					
Iné rozpočtové riadky (uveďte)					
SPOLU		**7**	**7**	**7**	**7**

XX predstavuje príslušnú oblasť politiky alebo rozpočtovú hlavu.

Potreby ľudských zdrojov budú pokryté úradníkmi GR, ktorí už boli pridelení na riadenie akcie a/alebo boli interne prerozdelení v rámci GR, a v prípade potreby budú doplnené zdrojmi, ktoré sa môžu prideliť riadiacemu GR v rámci ročného postupu prideľovania zdrojov a v závislosti od rozpočtových obmedzení.

Opis úloh, ktoré sa majú vykonať:

Úradníci a dočasní zamestnanci 6 FTE x 157 000 EUR/rok = 942 000 EUR	Ako sa opisuje v bode 2.2.1: – pripraviť mandát na tvorbu normy a/alebo spoločné špecifikácie prostredníctvom vykonávacích aktov bez úspešného procesu normalizácie, – vypracovať delegovaný akt [do 12 mesiacov od nadobudnutia účinnosti nariadenia], v ktorom sa vymedzujú kritické produkty s digitálnymi prvkami, – potenciálna príprava delegovaných aktov na účely aktualizovania zoznamu kritických produktov triedy I a II; špecifikovania, či je potrebné obmedzenie alebo vylúčenie produktov s digitálnymi prvkami, na ktoré sa vzťahujú iné pravidlá Únie, ktorými sa stanovujú požiadavky na dosiahnutie rovnakej úrovne ochrany ako týmto nariadením; stanovenia povinnosti certifikácie určitých vysokokritických produktov s digitálnymi prvkami na základe kritérií stanovených v tomto nariadení; špecifikovania minimálneho obsahu EÚ vyhlásenia o zhode a doplnenia prvkov, ktoré sa majú zahrnúť do technickej dokumentácie, – potenciálna príprava vykonávacích aktov týkajúcich sa formátu alebo

[47] ZZ = zmluvný zamestnanec; MZ = miestny zamestnanec; VNE = vyslaný národný expert; DAZ = dočasný agentúrny zamestnanec; PED = pomocný expert v delegácii.

[48] Čiastkový strop pre externých zamestnancov financovaných z operačných rozpočtových prostriedkov (pôvodné rozpočtové riadky „BA“).

	prvkov oznamovacích povinností, softvérového kusovníka, spoločných špecifikácií alebo pripojenia označenia CE, – potenciálna príprava okamžitého zásahu s uložením nápravných alebo reštriktívnych opatrení za mimoriadnych okolností s cieľom zachovať riadne fungovanie vnútorného trhu vrátane prípravy vykonávacieho aktu, – organizácia a koordinácia notifikácií notifikovaných osôb členskými štátmi a koordinácia notifikovaných osôb, – podpora koordinácie orgánov dohľadu nad trhom členských štátov.
Externí zamestnanci 1 VNE x 88 000 EUR/rok	Ako sa opisuje v bode 2.2.1: – pripraviť mandát na tvorbu normy a/alebo spoločné špecifikácie prostredníctvom vykonávacích aktov bez úspešného procesu normalizácie, – vypracovať delegovaný akt [do 12 mesiacov od nadobudnutia účinnosti nariadenia], v ktorom sa vymedzujú kritické produkty s digitálnymi prvkami, – potenciálna príprava delegovaných aktov na účely aktualizovania zoznamu kritických produktov triedy I a II; špecifikovania, či je potrebné obmedzenie alebo vylúčenie produktov s digitálnymi prvkami, na ktoré sa vzťahujú iné pravidlá Únie, ktorými sa stanovujú požiadavky na dosiahnutie rovnakej úrovne ochrany ako týmto nariadením; stanovenia povinnosti certifikácie určitých vysokokritických produktov s digitálnymi prvkami na základe kritérií stanovených v tomto nariadení; špecifikovania minimálneho obsahu EÚ vyhlásenia o zhode a doplnenia prvkov, ktoré sa majú zahrnúť do technickej dokumentácie, – potenciálna príprava vykonávacích aktov týkajúcich sa formátu alebo prvkov oznamovacích povinností, softvérového kusovníka, spoločných špecifikácií alebo pripojenia označenia CE, – potenciálna príprava okamžitého zásahu s uložením nápravných alebo reštriktívnych opatrení za mimoriadnych okolností s cieľom zachovať riadne fungovanie vnútorného trhu vrátane prípravy vykonávacieho aktu, – organizácia a koordinácia notifikácií notifikovaných osôb členskými štátmi a koordinácia notifikovaných osôb, – podpora koordinácie orgánov dohľadu nad trhom členských štátov.

3.2.4. Súlad s platným viacročným finančným rámcom

Návrh/iniciatíva:

– x môže byť v plnej miere financovaná prerozdelením v medziach príslušného okruhu viacročného finančného rámca (VFR).

Nevyžaduje sa žiadne preprogramovanie.

– ☐ si vyžaduje použitie nepridelenej rezervy v rámci príslušného okruhu VFR a/alebo použitie osobitných nástrojov vymedzených v nariadení o VFR.

–

– ☐ si vyžaduje revíziu VFR.

–

3.2.5. Príspevky od tretích strán

Návrh/iniciatíva:

– x nezahŕňa spolufinancovanie tretími stranami.

– ☐ zahŕňa spolufinancovanie tretími stranami, ako je odhadnuté v nasledujúcej tabuľke:

rozpočtové prostriedky v mil. EUR (zaokrúhlené na 3 desatinné miesta)

	Rok **N**[49]	Rok **N + 1**	Rok **N + 2**	Rok **N + 3**	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)			Spolu
Uveďte spolufinancujúci subjekt								
Prostriedky zo spolufinancovania SPOLU								

[49] Rok N je rokom, v ktorom sa návrh/iniciatíva začína vykonávať. Nahraďte „N“ očakávaným prvým rokom vykonávania (napríklad: 2021). To isté urobte aj pri nasledujúcich rokoch.

3.3. Odhadovaný vplyv na príjmy

– ☐ Návrh/iniciatíva nemá finančný vplyv na príjmy.

– ☐ Návrh/iniciatíva má tento finančný vplyv na príjmy:

– ☐ vplyv na vlastné zdroje

– ☐ vplyv na iné príjmy

– uveďte, či sú príjmy pripísané rozpočtovým riadkom výdavkov☐

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Rozpočtový riadok príjmov:	Rozpočtové prostriedky k dispozícii v bežnom rozpočtovom roku	Vplyv návrhu/iniciatívy[50]						
		Rok **N**	Rok **N + 1**	Rok **N + 2**	Rok **N + 3**	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)		
Článok …….								

V prípade pripísaných príjmov uveďte ovplyvnené rozpočtové riadky výdavkov.

Ďalšie poznámky (napr. spôsob/vzorec použitý na výpočet vplyvu na príjmy alebo akékoľvek ďalšie informácie).

[50] Pokiaľ ide o tradičné vlastné zdroje (clá, odvody z produkcie cukru), uvedené sumy musia predstavovať čisté sumy, t. j. hrubé sumy po odčítaní 20 % na náklady na výber.