Úradný vestník
Európskej únie

SK
Séria L

2024/2847

20.11.2024

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2024/2847

z 23. októbra 2024

o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti)

(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]),

po porade s Výborom regiónov,

konajúc v súlade s riadnym legislatívnym postupom ([2]),

keďže:

(1) Kybernetická bezpečnosť je pre Úniu jednou z kľúčových výziev. Počet a rozmanitosť pripojených zariadení sa bude v nadchádzajúcich rokoch exponenciálne zvyšovať. Kybernetické útoky sú záležitosťou verejného záujmu, keďže majú zásadný vplyv nielen na hospodárstvo Únie, ale aj na demokraciu, ako aj na bezpečnosť a zdravie spotrebiteľov. Je preto potrebné posilniť prístup Únie ku kybernetickej bezpečnosti, riešiť kybernetickú odolnosť na úrovni Únie a 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 z hľadiska kybernetickej bezpečnosti alebo ich bezpečne používať.

(2) Cieľom tohto nariadenia je vytvoriť hraničné podmienky pre vývoj bezpečných produktov s digitálnymi prvkami, pričom treba zabezpečiť, 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, napríklad zlepšením transparentnosti, pokiaľ ide o obdobie podpory produktov s digitálnymi prvkami dostupných na trhu.

(3) Príslušné platné právne predpisy Únie 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 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 ([3]) a smernice Európskeho parlamentu a Rady (EÚ) 2022/2555 ([4]), však priamo neobsahujú povinné požiadavky bezpečnosti produktov s digitálnymi prvkami.

([1]) Ú. v. EÚ C 100, 16.3.2023, s. 101.
([2]) Pozícia Európskeho parlamentu z 12. marca 2024 (zatiaľ neuverejnená v úradnom vestníku) a rozhodnutie Rady z 10. októbra 2024.
([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]) Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) (Ú. v. EÚ L 333, 27.12.2022, s. 80).

(4) Aj keď sa existujúce právne predpisy Únie uplatňujú na určité produkty s digitálnymi prvkami, neexistuje 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 podnikom a organizáciám pri plnení mnohých požiadaviek a povinností v súvislosti s podobnými druhmi produktov. Kybernetická bezpečnosť týchto produktov má obzvlášť výrazný cezhraničný rozmer, keďže produkty s digitálnymi prvkami vyrobené v jednom členskom štáte alebo tretej krajine používajú často organizácie a spotrebitelia na celom vnútornom trhu. Preto treba regulovať túto oblasť na úrovni Únie s cieľom zabezpečiť harmonizovaný regulačný rámec a právnu istotu pre používateľov, organizácie a podniky vrátane mikropodnikov a malých a stredných podnikov v zmysle vymedzenia v prílohe k odporúčaniu Komisie 2003/361/ES ([5]). Regulačné prostredie Únie by sa malo harmonizovať zavedením horizontálnych požiadaviek kybernetickej bezpečnosti pre produkty s digitálnymi prvkami. Okrem toho by sa pre hospodárske subjekty a používateľov mala v celej Únii zabezpečiť právna istota a lepšia harmonizácia vnútorného trhu a proporcionalita pre mikropodniky a malé a stredné podniky, čím by sa vytvorili životaschopnejšie podmienky pre hospodárske subjekty, ktoré plánujú vstup na uvedený trh.

(5) Pokiaľ ide o mikropodniky a malé a stredné podniky, pri určovaní kategórie, do ktorej podnik patrí, by sa ustanovenia prílohy k odporúčaniu 2003/361/ES mali uplatňovať v celom rozsahu. Preto by sa pri výpočte počtu zamestnancov a finančných stropov na určenie kategórie podnikov mali uplatňovať aj ustanovenia článku 6 prílohy k odporúčaniu 2003/361/ES o stanovovaní údajov o podniku vzhľadom na osobitné typy podnikov, ako sú partnerské podniky alebo prepojené podniky.

(6) Komisia by pri uplatňovaní tohto nariadenia mala poskytnúť usmernenia na pomoc hospodárskym subjektom, najmä mikropodnikom a malým a stredným podnikom. Takéto usmernenia by sa mali okrem iného týkať rozsahu pôsobnosti tohto nariadenia, najmä spracúvania údajov na diaľku a jeho dôsledkov pre vývojárov slobodného softvéru a softvéru s otvoreným zdrojovým kódom, uplatňovania kritérií používaných na určenie období podpory pre produkty s digitálnymi prvkami, vzájomného pôsobenia medzi týmto nariadením a inými právnymi predpismi Únie a koncepcie podstatnej úpravy.

(7) Na úrovni Únie obsahujú rôzne programové a politické dokumenty, napríklad spoločné oznámenie Komisie a vysokého predstaviteľa Únie pre zahraničné veci a bezpečnostnú politiku zo 16. decembra 2020 s názvom „Stratégia kybernetickej bezpečnosti EÚ v digitálnej dekáde“, závery Rady z 2. decembra 2020 o kybernetickej bezpečnosti pripojených zariadení a z 23. mája 2022 o vývoji prístupu Európskej únie ku kybernetickej bezpečnosti a uznesenie Európskeho parlamentu z 10. júna 2021 o stratégii kybernetickej bezpečnosti EÚ v digitálnej dekáde ([6]), výzvy na zavedenie špecifických požiadaviek Únie týkajúcich sa kybernetickej bezpečnosti digitálnych alebo pripojených produktov, pričom viaceré tretie krajiny zavádzajú opatrenia na riešenie tohto problému z vlastnej iniciatívy. V záverečnej správe z Konferencie o budúcnosti Európy občania vyzvali na „silnejšiu úlohu EÚ v boji proti kybernetickobezpečnostným hrozbám“. Na to, aby Únia zohrávala vedúcu úlohu v oblasti kybernetickej bezpečnosti na medzinárodnej scéne, je dôležité zaviesť ambiciózny regulačný rámec.

(8) 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.

(9) 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 produkty s digitálnymi prvkami boli navrhnuté a vyvíjané v súlade so základnými požiadavkami kybernetickej bezpečnosti stanovenými v tomto nariadení. Táto povinnosť sa týka produktov, ktoré možno pripojiť fyzicky cez hardvérové rozhranie, ako aj produktov, ktoré sa pripájajú logicky, napríklad pomocou sieťových zásuviek, dátovodov, súborov, aplikačných programovacích rozhraní alebo iných druhov softvérového rozhrania. Keďže kybernetické hrozby môžu šíriť rôzne produkty s digitálnymi prvkami pred dosiahnutím určitého cieľa, napríklad zreťazením viacerých zneužití zraniteľnosti, výrobcovia by mali zaistiť kybernetickú bezpečnosť aj pre produkty s digitálnymi prvkami, ktoré sú k iným zariadeniam alebo sieťam pripojené iba nepriamo.

([5]) Odporúčanie Komisie 2003/361/ES zo 6. mája 2003 týkajúce sa vymedzenia pojmu mikropodniky, malé a stredné podniky (Ú. v. EÚ L 124, 20.5.2003, s. 36).

([6]) Ú. v. EÚ C 67, 8.2.2022, s. 81.

(10) Stanovením požiadaviek kybernetickej bezpečnosti na uvádzanie produktov s digitálnymi prvkami na trh sa má zlepšiť kybernetická bezpečnosť týchto produktov pre spotrebiteľov, ako aj pre podniky. Týmito požiadavkami sa takisto zabezpečí, aby sa v dodávateľských reťazcoch zohľadňovala kybernetická bezpečnosť, čím sa zvýši bezpečnosť konečných produktov s digitálnymi prvkami a ich komponentov. Toto zahŕňa aj požiadavky na uvedenie na trh pre spotrebný tovar s digitálnymi prvkami určený pre zraniteľných spotrebiteľov, ako sú napríklad hračky a elektronické systémy na monitorovanie detí. Spotrebné produkty s digitálnymi prvkami kategorizované v tomto nariadení ako dôležité produkty s digitálnymi prvkami predstavujú vyššie kybernetickobezpečnostné riziko tým, že vykonávajú funkciu, ktorá so sebou nesie významné riziko nepriaznivých účinkov z hľadiska intenzity a schopnosti poškodiť zdravie, bezpečnosť alebo ochranu používateľov takýchto produktov, a mali by podliehať prísnejšiemu postupu posudzovania zhody. Týka sa to takých produktov, ako sú inteligentné domáce produkty s bezpečnostnými funkciami vrátane inteligentných zámkov dverí, elektronických systémov na monitorovania detí a poplašných systémov, pripojených hračiek a osobných nositeľných zdravotníckych technológií. Okrem toho prísnejšie postupy posudzovania zhody, ktorým sa musia podrobiť iné produkty s digitálnymi prvkami kategorizované v tomto nariadení ako dôležité alebo kritické produkty s digitálnymi prvkami, prispejú k predchádzaniu potenciálnym nepriaznivým účinkom zneužívania zraniteľností na spotrebiteľov.

(11) Cieľom tohto nariadenia je zabezpečiť vysokú úroveň kybernetickej bezpečnosti produktov s digitálnymi prvkami a ich integrovaných riešení spracovania údajov na diaľku. Takéto riešenia spracovania údajov na diaľku by sa mali vymedziť ako spracovanie údajov na diaľku, pre ktoré je softvér určený a vyvinutý výrobcom produktu s digitálnymi prvkami alebo v jeho mene, a ktorého absencia zabráni produktu s digitálnymi prvkami plniť jednu zo svojich funkcií. Týmto prístupom sa zabezpečuje, aby boli takéto produkty primerane a v celom rozsahu zabezpečené ich výrobcami bez ohľadu na to, či sa údaje spracúvajú alebo uchovávajú lokálne na zariadení používateľa alebo na diaľku výrobcom. Zároveň patrí spracovanie alebo uchovávanie na diaľku do rozsahu pôsobnosti tohto nariadenia len vtedy, ak je potrebné na to, aby produkt s digitálnymi prvkami vykonával svoje funkcie. Takéto spracovanie alebo uchovávanie na diaľku zahŕňa situáciu, keď mobilná aplikácia vyžaduje prístup k aplikačnému programovaciemu rozhraniu alebo k databáze poskytovanej prostredníctvom služby, ktorú vyvinul výrobca. V takom prípade služba patrí do rozsahu pôsobnosti tohto nariadenia ako riešenie spracovania údajov na diaľku. Požiadavky na riešenia spracovania údajov na diaľku, ktoré patria do rozsahu pôsobnosti tohto nariadenia, preto nezahŕňajú technické, prevádzkové ani organizačné opatrenia zamerané na riadenie rizík pre bezpečnosť sietí a informačných systémov výrobcu ako celku.

(12) Cloudové riešenia predstavujú riešenia spracovania údajov na diaľku v zmysle tohto nariadenia len vtedy, ak spĺňajú vymedzenie stanovené v tomto nariadení. Napríklad cloudové funkcie poskytované výrobcom inteligentných domácich zariadení, ktoré používateľom umožňujú ovládať zariadenie na diaľku, patria do rozsahu pôsobnosti tohto nariadenia. Na druhej strane webové sídla, ktoré nepodporujú funkčnosť produktu s digitálnymi prvkami, ani cloudové služby navrhnuté a vyvinuté mimo zodpovednosti výrobcu produktu s digitálnymi prvkami nepatria do rozsahu pôsobnosti tohto nariadenia. Smernica (EÚ) 2022/2555 sa vzťahuje na cloudové služby a modely cloudových služieb, ako je softvér ako služba (SaaS), platforma ako služba (PaaS) a infraštruktúra ako služba (IaaS). Subjekty poskytujúce cloudové služby v Únii, ktoré sa považujú za stredné podniky podľa článku 2 prílohy k odporúčaniu 2003/361/ES alebo prekračujú limity pre stredné podniky stanovené v odseku 1 uvedeného článku, patria do rozsahu pôsobnosti uvedenej smernice.

(13) V súlade s cieľom tohto nariadenia odstrániť prekážky voľného pohybu produktov s digitálnymi prvkami by členské štáty v prípade záležitostí, na ktoré sa vzťahuje toto nariadenie, nemali brániť sprístupneniu produktov s digitálnymi prvkami, ktoré sú v súlade s týmto nariadením, na trhu. Preto členské štáty nemôžu v záležitostiach harmonizovaných týmto nariadením uložiť dodatočné požiadavky kybernetickej bezpečnosti na sprístupnenie produktov s digitálnymi prvkami na trhu. Každý verejný alebo súkromný subjekt však môže stanoviť dodatočné požiadavky k požiadavkám stanoveným v tomto nariadení na obstarávanie alebo používanie produktov s digitálnymi prvkami na ich osobitné účely, a preto sa môže rozhodnúť používať produkty s digitálnymi prvkami, ktoré spĺňajú prísnejšie alebo osobitnejšie požiadavky kybernetickej bezpečnosti, než sú požiadavky uplatniteľné na sprístupňovanie na trhu podľa tohto nariadenia. Bez toho, aby boli dotknuté smernice Európskeho parlamentu a Rady 2014/24/EÚ ([7]) a 2014/25/EÚ ([8]), pri obstarávaní produktov s digitálnymi prvkami, ktoré musia spĺňať základné požiadavky kybernetickej bezpečnosti stanovené v tomto nariadení vrátane požiadaviek na riešenie zraniteľností, by členské štáty mali zabezpečiť, aby sa takéto požiadavky zohľadnili v procese obstarávania a aby sa

([7]) Smernica Európskeho parlamentu a Rady 2014/24/EÚ z 26. februára 2014 o verejnom obstarávaní a o zrušení smernice 2004/18/ES (Ú. v. EÚ L 94, 28.3.2014, s. 65).

([8]) Smernica Európskeho parlamentu a Rady 2014/25/EÚ z 26. februára 2014 o obstarávaní vykonávanom subjektmi pôsobiacimi v odvetviach vodného hospodárstva, energetiky, dopravy a poštových služieb a o zrušení smernice 2004/17/ES (Ú. v. EÚ L 94, 28.3.2014, s. 243).

zohľadnila aj schopnosť výrobcov účinne uplatňovať opatrenia v oblasti kybernetickej bezpečnosti a riadiť kybernetické hrozby. Okrem toho sa v smernici (EÚ) 2022/2555 stanovujú opatrenia na riadenie kybernetickobezpečnostných rizík pre kľúčové a dôležité subjekty uvedené v článku 3 uvedenej smernice, ktoré by mohli zahŕňať bezpečnostné opatrenia dodávateľského reťazca, ktoré si vyžadujú, aby takéto subjekty používali produkty s digitálnymi prvkami, ktoré spĺňajú prísnejšie požiadavky kybernetickej bezpečnosti, než sú požiadavky stanovené v tomto nariadení. V súlade so smernicou (EÚ) 2022/2555 a v súlade s jej zásadou minimálnej harmonizácie môžu preto členské štáty uložiť dodatočné požiadavky kybernetickej bezpečnosti na používanie produktov informačných a komunikačných technológií kľúčovými alebo dôležitými subjektmi podľa uvedenej smernice s cieľom zabezpečiť vyššiu úroveň kybernetickej bezpečnosti za predpokladu, že takéto požiadavky sú v súlade s povinnosťami členských štátov stanovenými v práve Únie. Záležitosti, na ktoré sa toto nariadenie nevzťahuje, môžu zahŕňať netechnické faktory týkajúce sa produktov s digitálnymi prvkami a ich výrobcov. Členské štáty preto môžu stanoviť vnútroštátne opatrenia vrátane obmedzení týkajúcich sa produktov s digitálnymi prvkami alebo dodávateľov takýchto produktov, ktoré zohľadňujú netechnické faktory. Vnútroštátne opatrenia týkajúce sa takýchto faktorov musia byť v súlade s právom Únie.

(14) Týmto nariadením by nemala byť dotknutá zodpovednosť členských štátov za ochranu národnej bezpečnosti v súlade s právom Únie. Členské štáty by mali mať možnosť podrobiť produkty s digitálnymi prvkami, ktoré sa obstarávajú alebo používajú na účely národnej bezpečnosti alebo obrany, dodatočným opatreniam za predpokladu, že takéto opatrenia sú v súlade s povinnosťami členských štátov stanovenými v práve Únie.

(15) Toto nariadenie sa vzťahuje na hospodárske subjekty len v súvislosti s produktmi s digitálnymi prvkami, ktoré sú sprístupnené na trhu, a teda dodávanými na distribúciu alebo používanie na trhu Únie v rámci obchodnej činnosti. Dodávanie v rámci obchodnej činnosti môže byť charakterizované nielen účtovaním ceny za produkt s digitálnymi prvkami, ale aj účtovaním ceny za služby technickej podpory, ak nejde len o náhradu skutočných nákladov, so zámerom speňažiť, napríklad poskytnutím softvérovej platformy, prostredníctvom ktorej výrobca speňažuje iné služby, vyžadovaním použitia spracovania osobných údajov ako podmienky z iných dôvodov než výlučne na zlepšenie bezpečnosti, kompatibility alebo interoperability softvéru, alebo prijatím darov presahujúcich náklady spojené s návrhom, vývojom a poskytovaním produktu s digitálnymi prvkami. Prijímanie darov bez úmyslu dosiahnuť zisk by sa nemalo považovať za obchodnú činnosť.

(16) Produkty s digitálnymi prvkami dodávané ako súčasť poskytovanej služby, za ktorú sa účtuje poplatok výlučne na účely úhrady skutočných nákladov priamo súvisiacich s prevádzkou tejto služby, ako je to v prípade určitých produktov s digitálnymi prvkami poskytovaných subjektmi verejnej správy, by sa len na základe týchto dôvodov nemali na účely tohto nariadenia považovať za obchodnú činnosť. Okrem toho produkty s digitálnymi prvkami, ktoré vyvíja alebo upravuje subjekt verejnej správy výlučne na vlastné použitie, by sa nemali považovať za sprístupnené na trhu v zmysle tohto nariadenia.

(17) Softvér a údaje, ktoré sú voľne zdieľané, pričom používatelia môžu k nim alebo k ich upraveným verziám voľne pristupovať, používať ich, upravovať a ďalej rozosielať, môžu prispieť k výskumu a inováciám na trhu. S cieľom podporiť vývoj a zavádzanie slobodného softvéru a softvéru s otvoreným zdrojovým kódom, najmä zo strany mikropodnikov a malých a stredných podnikov vrátane startupov, jednotlivcov, neziskových organizácií a akademických výskumných organizácií, by sa pri uplatňovaní tohto nariadenia na produkty s digitálnymi prvkami, ktoré sa považujú za slobodný softvér a softvér s otvoreným zdrojovým kódom dodávaný na distribúciu alebo na použitie v rámci obchodnej činnosti, mala zohľadniť povaha rôznych modelov vývoja softvéru distribuovaného a vyvinutého s licenciou slobodného softvéru a softvéru s otvoreným zdrojovým kódom.

(18) Slobodný softvér a softvér s otvoreným zdrojovým kódom sa chápe ako softvér, ktorého zdrojový kód je otvorený a licencia naň poskytuje všetky práva na voľný prístup k nemu, jeho používanie, úpravy a redistribúciu. Slobodný softvér a softvér s otvoreným zdrojovým kódom sa vyvíja, udržiava a distribuuje voľne, a to aj prostredníctvom online platforiem. Vo vzťahu k hospodárskym subjektom, ktoré patria do rozsahu pôsobnosti tohto nariadenia, by do rozsahu pôsobnosti tohto nariadenia mal patriť len slobodný softvér a softvér s otvoreným zdrojovým kódom sprístupnený na trhu, a preto dodávaný na distribúciu alebo používanie v rámci obchodnej činnosti. Samotné okolnosti, za ktorých bol produkt s digitálnymi prvkami vyvinutý, alebo spôsob financovania vývoja by sa preto nemali zohľadňovať pri určovaní toho, či ide o činnosť obchodnej alebo neobchodnej povahy. Konkrétne na účely tohto nariadenia a vo vzťahu k hospodárskym subjektom, ktoré patria do jeho rozsahu pôsobnosti, by sa poskytovanie produktov s digitálnymi prvkami považovanými za slobodný softvér a softvér s otvoreným zdrojovým

kódom, ktoré ich výrobcovia nespeňažujú, nemalo považovať za obchodnú činnosť, aby sa zabezpečilo jasné rozlíšenie medzi fázou vývoja a fázou dodávky. Okrem toho by sa dodávka produktov s digitálnymi prvkami považovanými za komponenty slobodného softvéru a softvéru s otvoreným zdrojovým kódom určenými na integráciu inými výrobcami do ich vlastných produktov s digitálnymi prvkami, mala považovať za sprístupnenie na trhu len vtedy, ak komponent speňaží jeho pôvodný výrobca. Napríklad samotná skutočnosť, že softvérový produkt s otvoreným zdrojovým kódom s digitálnymi prvkami má finančnú podporu od výrobcov alebo že výrobcovia prispievajú k vývoju takéhoto produktu, by sama osebe nemala určovať, že ide o činnosť obchodnej povahy. Okrem toho samotné vydávanie pravidelných verzií by samo osebe nemalo viesť k záveru, že produkt s digitálnymi prvkami sa dodáva v rámci obchodnej činnosti. Napokon na účely tohto nariadenia by sa vývoj produktov s digitálnymi prvkami, ktoré neziskové organizácie označujú za slobodný softvér a softvér s otvoreným zdrojovým kódom, nemal považovať za obchodnú činnosť za predpokladu, že organizácia je zriadená tak, aby sa zabezpečilo, že všetky príjmy po odpočítaní nákladov sa použijú na dosiahnutie neziskových cieľov. Toto nariadenie sa nevzťahuje na fyzické alebo právnické osoby, ktoré prispievajú zdrojovým kódom k produktom s digitálnymi prvkami, ktoré sa považujú za slobodný softvér a softvér s otvoreným zdrojovým kódom, za ktoré nenesú zodpovednosť.

(19) Vzhľadom na význam mnohých produktov s digitálnymi prvkami, ktoré sa považujú za slobodný softvér a softvér s otvoreným zdrojovým kódom, pre kybernetickú bezpečnosť, ktoré sa zverejňujú, ale nesprístupňujú na trhu v zmysle tohto nariadenia, by právnické osoby, ktoré poskytujú trvalú podporu vývoju takýchto produktov určených na obchodné činnosti a ktoré zohrávajú hlavnú úlohu pri zabezpečovaní životaschopnosti týchto produktov (ďalej len „správcovia softvéru s otvoreným zdrojovým kódom“), mali podliehať miernemu a individuálne prispôsobenému regulačnému režimu. Medzi správcov softvéru s otvoreným zdrojovým kódom patria určité nadácie, ako aj subjekty, ktoré vyvíjajú a vydávajú slobodný softvér a softvér s otvoreným zdrojovým kódom v podnikateľskom prostredí, vrátane neziskových subjektov. Regulačný režim by mal zohľadňovať ich osobitnú povahu a zlučiteľnosť s druhom uložených povinností. Mal by sa vzťahovať len na produkty s digitálnymi prvkami, ktoré sa považujú za slobodný softvér a softvér s otvoreným zdrojovým kódom, ktorý je v konečnom dôsledku určený na obchodné činnosti, napríklad na integráciu do komerčných služieb alebo do speňažovaných produktov s digitálnymi prvkami. Na účely uvedeného regulačného režimu zahŕňa zámer integrácie do speňažovaných produktov s digitálnymi prvkami prípady, keď výrobcovia, ktorí komponent integrujú do vlastných produktov s digitálnymi prvkami, buď pravidelne prispievajú k vývoju tohto komponentu, alebo poskytujú pravidelnú finančnú pomoc na zabezpečenie kontinuity softvérového produktu. Poskytovanie trvalej podpory vývoju produktu s digitálnymi prvkami zahŕňa okrem iného hosting a riadenie platforiem spolupráce pri vývoji softvéru, hosting zdrojového kódu alebo softvéru, správu alebo riadenie produktov s digitálnymi prvkami, ktoré sa považujú za slobodný softvér a softvér s otvoreným zdrojovým kódom, ako aj riadenie vývoja takýchto produktov. Vzhľadom na to, že mierny a individuálne prispôsobený regulačný režim neukladá subjektom, ktoré pôsobia ako správcovia softvéru s otvoreným zdrojovým kódom, rovnaké povinnosti ako subjektom, ktoré pôsobia ako výrobcovia podľa tohto nariadenia, nemalo by im byť povolené umiestňovať označenie CE na produkty s digitálnymi prvkami, ktorých vývoj podporujú.

(20) Samotný hosting produktov s digitálnymi prvkami na otvorených úložiskách, a to aj prostredníctvom správcov balíkov alebo na platformách spolupráce, nie je ako taký sprístupňovaním produktu s digitálnymi prvkami na trhu. Poskytovatelia takýchto služieb by sa mali považovať za distribútorov len vtedy, ak sprístupňujú takýto softvér na trhu, a teda dodávajú ho na distribúciu alebo používanie na trhu Únie v rámci obchodnej činnosti.

(21) S cieľom podporiť a uľahčiť náležitú starostlivosť výrobcov, ktorí integrujú komponenty slobodného softvéru a softvéru s otvoreným zdrojovým kódom, na ktoré sa nevzťahujú základné požiadavky kybernetickej bezpečnosti stanovené v tomto nariadení, do svojich produktov s digitálnymi prvkami by Komisia mala mať možnosť zaviesť programy dobrovoľného osvedčovania bezpečnosti, a to buď delegovaným aktom, ktorým sa doplní toto nariadenie, alebo požiadaním o európsku schému certifikácie kybernetickej bezpečnosti podľa článku 48 nariadenia (EÚ) 2019/881, v ktorej sa zohľadnia osobitosti modelov vývoja slobodného softvéru a softvéru s otvoreným zdrojovým kódom. Programy osvedčovania bezpečnosti by mali byť koncipované tak, aby osvedčenie bezpečnosti mohli iniciovať alebo financovať nielen fyzické alebo právnické osoby, ktoré vyvíjajú alebo prispievajú k vývoju produktu s digitálnymi prvkami, ktoré sa považujú za slobodný softvér a softvér s otvoreným zdrojovým kódom, ale aj tretie strany, ako sú výrobcovia, ktorí takéto produkty integrujú do vlastných produktov s digitálnymi prvkami, používatelia alebo orgány verejnej správy Únie a členských štátov.

(22) Vzhľadom na verejné ciele tohto nariadenia v oblasti kybernetickej bezpečnosti a s cieľom zlepšiť situačnú informovanosť členských štátov o závislosti Únie od softvérových komponentov, a najmä od potenciálne slobodných softvérových komponentov a softvérových komponentov s otvoreným zdrojovým kódom, by špecializovaná skupina pre administratívnu spoluprácu (ďalej len „ADCO“) zriadená týmto nariadením mala mať možnosť rozhodnúť o spoločnom posúdení závislosti Únie. Orgány dohľadu nad trhom by mali mať možnosť požiadať výrobcov kategórií produktov s digitálnymi prvkami stanovených skupinou ADCO o predloženie zoznamov softvéru, ktoré zostavili podľa tohto nariadenia. S cieľom chrániť dôvernosť zoznamov softvéru by orgány dohľadu nad trhom mali skupine ADCO anonymne a súhrnne predkladať relevantné informácie o závislostiach.

(23) Účinnosť vykonávania tohto nariadenia bude závisieť aj od dostupnosti zodpovedajúcich kybernetickobezpečnostných zručností. Na úrovni Únie sa v rôznych programových a politických dokumentoch vrátane oznámenia Komisie z 18. apríla 2023 s názvom „Riešenie nedostatku odborníkov v oblasti kybernetickej bezpečnosti s cieľom posilniť konkurencieschopnosť, rast a odolnosť EÚ“ a v záveroch Rady z 22. mája 2023 o politike EÚ v oblasti kybernetickej obrany uznal nedostatok zručností v oblasti kybernetickej bezpečnosti v Únii a potreba prioritne riešiť takéto výzvy vo verejnom aj súkromnom sektore. S cieľom zaistiť účinné vykonávanie tohto nariadenia by členské štáty mali zabezpečiť, aby boli k dispozícii primerané zdroje na vhodné personálne obsadenie orgánov dohľadu nad trhom a orgánov posudzovania zhody na vykonávanie ich úloh stanovených v tomto nariadení. Uvedené opatrenia by mali posilniť mobilitu pracovnej sily v oblasti kybernetickej bezpečnosti a s nimi súvisiace kariérne možnosti. Mali by tiež prispieť k zvýšeniu odolnosti a inkluzívnosti pracovnej sily v oblasti kybernetickej bezpečnosti, a to aj z hľadiska rodovej rovnosti. Členské štáty by preto mali prijať opatrenia s cieľom zabezpečiť, aby tieto úlohy vykonávali primerane vyškolení odborníci s potrebnými zručnosťami v oblasti kybernetickej bezpečnosti. Podobne by výrobcovia mali zabezpečiť, aby ich zamestnanci mali potrebné zručnosti na plnenie svojich povinností stanovených v tomto nariadení. Členské štáty a Komisia by v súlade so svojimi výsadami a právomocami a osobitnými úlohami, ktoré im boli zverené týmto nariadením, mali prijať opatrenia na podporu výrobcov, a najmä mikropodnikov a malých a stredných podnikov vrátane startupov, a to aj v oblastiach, ako je rozvoj zručností, na účely plnenia ich povinností stanovených v tomto nariadení. Keďže v smernici (EÚ) 2022/2555 sa od členských štátov vyžaduje, aby v rámci svojich národných stratégií kybernetickej bezpečnosti prijali politiky na podporu a rozvoj odbornej prípravy v oblasti kybernetickej bezpečnosti a zručností v oblasti kybernetickej bezpečnosti, členské štáty môžu pri prijímaní takýchto stratégií zvážiť aj riešenie potrieb zručností v oblasti kybernetickej bezpečnosti vyplývajúcich z tohto nariadenia vrátane tých, ktoré sa týkajú rekvalifikácie a zvyšovania úrovne zručností.

(24) Pre fungovanie kritickej infraštruktúry a pre spoločnosť ako celok je bezpečný internet nevyhnutný. Cieľom smernice (EÚ) 2022/2555 je zaistiť vysokú úroveň kybernetickej bezpečnosti služieb poskytovaných kľúčovými a dôležitými subjektmi uvedenými v článku 3 uvedenej smernice, vrátane poskytovateľov digitálnej infraštruktúry, ktorí podporujú základné funkcie otvoreného internetu, zabezpečujú prístup na internet a poskytujú 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 (EÚ) 2022/2555 poskytovateľmi digitálnej infraštruktúry tým, že sa zabezpečí, aby sa produkty s digitálnymi prvkami, ktoré používajú na poskytovanie svojich služieb, vyvíjali bezpečne a aby mali prístup k včasným bezpečnostným aktualizáciám takýchto produktov.

(25) V nariadení Európskeho parlamentu a Rady (EÚ) 2017/745 ([9]) sú stanovené pravidlá pre zdravotnícke pomôcky a v nariadení Európskeho parlamentu a Rady (EÚ) 2017/746 ([10]) sú stanovené pravidlá pre diagnostické zdravotnícke pomôcky in vitro. V uvedených nariadeniach sa riešia kybernetickobezpečnostné riziká a uplatňujú sa v nich osobitné prístupy, ktorým sa venuje aj toto nariadenie. Presnejšie sa v nariadeniach (EÚ) 2017/745 a (EÚ) 2017/746 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 pri uplatnení zásad riadenia 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 kybernetickobezpečnostné požiadavky stanovené v prílohe I k uvedeným nariadeniam. Produkty s digitálnymi prvkami, na ktoré sa uplatňuje jedno z uvedených nariadení, by preto nemali podliehať tomuto nariadeniu.

(26) Produkty s digitálnymi prvkami vyvinuté alebo upravené výlučne na účely národnej bezpečnosti alebo na obranné účely, alebo produkty špecificky navrhnuté na spracovanie utajovaných skutočností nepatria do rozsahu pôsobnosti tohto nariadenia. Členské štáty sa vyzývajú, aby zabezpečili rovnakú alebo vyššiu úroveň ochrany týchto produktov v porovnaní s produktmi, ktoré patria do rozsahu pôsobnosti tohto nariadenia.

([9]) 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).

([10]) 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).

(27) V nariadení Európskeho parlamentu a Rady (EÚ) 2019/2144 ([11]) 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, najmä predpisom OSN č. 155 – Jednotné ustanovenia na účely schvaľovania vozidiel vzhľadom na kybernetickú bezpečnosť a systém riadenia kybernetickej bezpečnosti ([12]), a stanovujú sa osobitné postupy posudzovania zhody. V oblasti letectva je hlavným cieľom nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1139 ([13]) dosiahnutie a udržanie vysokej a jednotnej úrovne bezpečnosti civilného letectva v Únii. Vytvára sa ním rámec pre základné požiadavky letovej spôsobilosti výrobkov, súčastí a zariadení vrátane softvéru leteckej techniky, ktorý zahŕňa povinnosti ochrany pred ohrozením bezpečnosti informácií. Postupom certifikácie podľa nariadenia (EÚ) 2018/1139 sa zaisťuje úroveň záruky, ktorá je cieľom tohto nariadenia. Produkty s digitálnymi prvkami, na ktoré sa uplatňuje nariadenie (EÚ) 2019/2144 a produkty certifikované v súlade s nariadením (EÚ) 2018/1139, by preto nemali podliehať základným požiadavkám kybernetickej bezpečnosti a postupom posudzovania zhody stanoveným v tomto nariadení.

(28) Týmto nariadením sa stanovujú horizontálne pravidlá kybernetickej bezpečnosti, ktoré nie sú špecifické pre jednotlivé odvetvia alebo určité produkty s digitálnymi prvkami. Mohli by sa však zaviesť špecifické pravidlá Únie pre dané odvetvie alebo produkt a v nich by sa stanovili požiadavky na riešenie všetkých alebo niektorých rizík, na ktoré sa vzťahujú základné požiadavky kybernetickej bezpečnosti stanovené v tomto nariadení. V takýchto prípadoch možno uplatňovanie tohto nariadenia na produkty s digitálnymi prvkami upravených v iných pravidlách Únie, ktorými sa stanovujú požiadavky na riešenie všetkých alebo niektorých rizík, ktorých sa týkajú základné požiadavky kybernetickej bezpečnosti stanovené v tomto nariadení, obmedziť alebo vylúčiť, ak sa takéto obmedzenie alebo vylúčenie zhoduje s celkovým regulačným rámcom uplatňovaným na tieto produkty a ak sa odvetvovými pravidlami dosiahne aspoň rovnaká úroveň ochrany ako úroveň stanovená týmto nariadením. Komisia by mala byť splnomocnená prijímať delegované akty s cieľom doplniť 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.

(29) S cieľom zabezpečiť možnosť účinnej opravy produktov s digitálnymi prvkami sprístupnených na trhu a predĺženie ich životnosti by sa mala udeliť výnimka pre náhradné diely. Táto výnimka by mala platiť pre náhradné diely, ktorých účelom je oprava pôvodných produktov sprístupnených pred dátumom začatia uplatňovania tohto nariadenia, ako aj pre náhradné diely, ktoré už prešli postupom posudzovania zhody podľa tohto nariadenia.

(30) V delegovanom nariadení Komisie (EÚ) 2022/30 ([14]) sa stanovuje, že niekoľko základných požiadaviek stanovených v článku 3 ods. 3 písm. d), e) a f) smernice Európskeho parlamentu a Rady 2014/53/EÚ ([15]), ktoré sa týkajú poškodenia siete a zneužitia sieťových zdrojov, osobných údajov a súkromia a podvodov, sa uplatňuje na rádiové zariadenia. Vo vykonávacom rozhodnutí Komisie C(2022)5637 z 5. augusta 2022 o mandáte na tvorbu noriem adresovanom Európskemu výboru pre normalizáciu a Európskemu výboru pre normalizáciu v elektrotechnike sa stanovujú požiadavky na vypracovanie konkrétnych noriem s ďalším špecifikovaním spôsobu, akým by sa tieto základné požiadavky mali riešiť. Základné požiadavky kybernetickej bezpečnosti stanovené v tomto nariadení obsahujú všetky prvky základných požiadaviek uvedených v článku 3 ods. 3 písm. d), e) a f) smernice 2014/53/EÚ.

([11]) 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).

([12]) Ú. v. EÚ L 82, 9.3.2021, s. 30.

([13]) 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).

([14]) Delegované nariadenie Komisie (EÚ) 2022/30 z 29. októbra 2021, ktorým sa dopĺňa smernica Európskeho parlamentu a Rady 2014/53/EÚ, pokiaľ ide o uplatňovanie základných požiadaviek uvedených v článku 3 ods. 3 písm. d), e) a f) uvedenej smernice (Ú. v. EÚ L 7, 12.1.2022, s. 6).

([15]) Smernica Európskeho parlamentu a Rady 2014/53/EÚ zo 16. apríla 2014 o harmonizácii právnych predpisov členských štátov týkajúcich sa sprístupňovania rádiových zariadení na trhu, ktorou sa zrušuje smernica 1999/5/ES (Ú. v. EÚ L 153, 22.5.2014, s. 62).

Okrem toho sú základné požiadavky kybernetickej bezpečnosti stanovené v tomto nariadení 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 C(2022) 5637. Počas prechodného obdobia na uplatňovanie tohto nariadenia by Komisia mala poskytnúť usmernenia výrobcom, na ktorých sa vzťahuje toto nariadenie a na ktorých sa vzťahuje aj delegované nariadenie (EÚ) 2022/30, s cieľom uľahčiť preukazovanie súladu s týmito dvoma nariadeniami.

(31) Smernica Európskeho parlamentu a Rady (EÚ) 2024/2853 ([16]) dopĺňa toto nariadenie. Uvedenou smernicou sa stanovujú pravidlá zodpovednosti za chybné produkty, aby poškodené osoby mohli uplatniť nárok na náhradu, keď im škodu spôsobili chybné produkty. Ustanovuje zásadu, že výrobca produktu zodpovedá za škody spôsobené nedostatočnou bezpečnosťou svojho produktu 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.

(32) Týmto nariadením by nemalo byť dotknuté nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 ([17]), a to ani ustanovenia týkajúce sa zavedenia 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, ako aj certifikácie kybernetickej bezpečnosti prostredníctvom spolupráce medzi Komisiou, európskymi normalizačnými organizáciami, Agentúrou Európskej únie pre kybernetickú bezpečnosť (ďalej len „ENISA“), Európskym výborom pre ochranu údajov, ktorý bol zriadený nariadením (EÚ) 2016/679, a národnými dozornými orgánmi pre ochranu údajov. Vzniknúť by 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 určené podľa tohto nariadenia mali spolupracovať s orgánmi, ktoré vykonávajú dohľad nad uplatňovaním práva Únie v oblasti ochrany údajov. Tie by mali mať prístup aj k informáciám, ktoré sú dôležité pre plnenie ich úloh.

(33) Poskytovatelia európskych peňaženiek digitálnej identity uvedení v článku 5a ods. 2 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 ([18]) by v rozsahu, v akom ich produkty patria do rozsahu pôsobnosti tohto nariadenia, mali spĺňať základné horizontálne požiadavky kybernetickej bezpečnosti stanovené v tomto nariadení, ako aj osobitné bezpečnostné požiadavky stanovené v článku 5a nariadenia (EÚ) č. 910/2014. V záujme uľahčenia dodržiavania predpisov by poskytovatelia peňaženiek mali byť schopní preukázať súlad európskych peňaženiek digitálnej identity s požiadavkami stanovenými v tomto nariadení a v nariadení (EÚ) č. 910/2014 certifikáciou svojich produktov v rámci európskej schémy certifikácie kybernetickej bezpečnosti zavedenej podľa nariadenia (EÚ) 2019/881, pre ktorý Komisia prostredníctvom delegovaných aktov špecifikovala predpoklad zhody s týmto nariadením, pokiaľ sa certifikát alebo jeho časti vzťahujú na uvedené požiadavky.

(34) Pri integrácii komponentov získaných od tretích strán do produktov s digitálnymi prvkami vo fáze návrhu a vývoja by výrobcovia s cieľom zabezpečiť, aby sa produkty navrhovali, vyvíjali a vyrábali v súlade so základnými požiadavkami kybernetickej bezpečnosti stanovenými v tomto nariadení, mali uplatňovať náležitú starostlivosť, pokiaľ ide o tieto komponenty vrátane komponentov so slobodným softvérom a softvérom s otvoreným zdrojovým

([16]) Smernica Európskeho parlamentu a Rady (EÚ) 2024/2853 z 23. októbra 2024 o zodpovednosti za chybné výrobky a o zrušení smernice Rady 85/374/EHS (Ú. v. EÚ L, 2024/2853, 18.11.2024, ELI: http://data.europa.eu/eli/dir/2024/2853/oj).

([17]) 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).

([18]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (Ú. v. EÚ L 257, 28.8.2014, s. 73).

kódom, ktoré neboli sprístupnené na trhu. Primeraná úroveň náležitej starostlivosti závisí od povahy a úrovne kybernetickobezpečnostného rizika spojeného s daným komponentom a na tento účel by mala zahŕňať jedno alebo viaceré z týchto opatrení: podľa potreby overenie, či výrobca komponentu preukázal zhodu s týmto nariadením, a to aj kontrolou toho, či komponent už má označenie CE; overenie, či je komponent pravidelne aktualizovaný na účely bezpečnosti, napríklad kontrolou histórie jeho bezpečnostných aktualizácií; overenie, či komponent neobsahuje zraniteľnosti zaznamenané v európskej databáze zraniteľností zriadenej podľa článku 12 ods. 2 smernice (EÚ) 2022/2555 alebo v iných verejne prístupných databázach zraniteľností; alebo vykonanie dodatočných bezpečnostných testov. Povinnosti riešiť zraniteľnosti stanovené v tomto nariadení, ktoré sú výrobcovia povinní dodržiavať pri uvádzaní produktu s digitálnymi prvkami na trh a počas obdobia podpory, sa vzťahujú na produkty s digitálnymi prvkami v ich celistvosti, ako aj na všetky integrované komponenty. Ak pri vykonávaní náležitej starostlivosti výrobca produktu s digitálnymi prvkami zistí zraniteľnosť komponentu, a to aj komponentu, ktorý obsahuje slobodný softvér a softvér s otvoreným zdrojovým kódom, mal by informovať osobu alebo subjekt, ktorý komponent vyrába alebo poskytuje jeho údržbu, riešiť a napraviť zraniteľnosť a prípadne poskytnúť tejto osobe alebo subjektu používanú bezpečnostnú nápravu.

(35) Ihneď po prechodnom období na uplatňovanie tohto nariadenia výrobca produktu s digitálnymi prvkami, ktorý integruje jeden alebo viacero komponentov od tretích strán, na ktoré sa takisto vzťahuje toto nariadenie, nemusí byť schopný v rámci svojej povinnosti náležitej starostlivosti overiť, či výrobcovia týchto komponentov preukázali zhodu s týmto nariadením, napríklad overením toho, či tieto komponenty už majú označenie CE. Môže ísť o prípad, keď komponenty boli integrované skôr, ako sa toto nariadenie začne uplatňovať na výrobcov týchto komponentov. V tom prípade by mal výrobca, ktorý takéto komponenty integruje, uplatňovať náležitú starostlivosť inými prostriedkami.

(36) Produkty s digitálnymi prvkami by mali niesť označenie CE, ktorým sa viditeľne, čitateľne a nezmazateľne preukazuje zhoda s týmto nariadením, aby im bol umožnený voľný pohyb v rámci vnútorného trhu. Členské štáty by nemali vytvárať neodôvodnené prekážky uvedeniu na trh produktov s digitálnymi prvkami, ktoré spĺňajú požiadavky stanovené v tomto nariadení a majú označenie CE. Okrem toho by členské štáty na obchodných veľtrhoch, výstavách a predvádzaniach alebo podobných podujatiach nemali brániť ukážkam alebo používaniu produktu s digitálnymi prvkami, ktorý nie je v súlade s týmto nariadením, vrátane jeho prototypov, za predpokladu, že produkt je prezentovaný s viditeľným označením, ktoré jasne uvádza, že produkt nie je v súlade s týmto nariadením a že nesmie byť sprístupnený na trhu, kým sa nedosiahne súlad.

(37) S cieľom zabezpečiť, aby výrobcovia mohli uvoľňovať softvér na účely testovania pred podrobením svojich produktov s digitálnymi prvkami posudzovaniu zhody, by členské štáty nemali brániť sprístupneniu nedokončeného softvéru, ako sú alfa verzie, beta verzie alebo kandidáti na finálnu verziu, pokiaľ sa nedokončený softvér sprístupňuje iba na čas potrebný na jeho 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 stanovuje 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.

(38) 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 kybernetickej bezpečnosti. Tieto základné požiadavky kybernetickej bezpečnosti vrátane požiadaviek na riadenie zraniteľnosti sa uplatňujú na každý jednotlivý produkt s digitálnymi prvkami pri jeho uvedení na trh bez ohľadu na to, či sa produkt s digitálnymi prvkami vyrába ako samostatná jednotka alebo v sérii. Napríklad v prípade typu produktu by každý jednotlivý produkt s digitálnymi prvkami mal mať všetky dostupné bezpečnostné opravy alebo aktualizácie na riešenie relevantných bezpečnostných problémov pri uvedení na trh. Ak sa produkty s digitálnymi prvkami následne fyzicky alebo digitálne upravia spôsobom, s ktorým výrobca pri prvom posúdení rizika nepočítal a z ktorého môže vyplynúť, že už nespĺňajú príslušné základné požiadavky kybernetickej bezpečnosti, úprava by sa mala považovať za podstatnú. Napríklad opravy by sa mohli klásť na rovnakú úroveň ako činnosti údržby za predpokladu, že by sa nimi produkt s digitálnymi prvkami, ktorý už bol uvedený na trh, neupravil takým spôsobom, ktorý by mohol ovplyvniť spĺňanie uplatniteľných požiadaviek alebo ktorým by sa mohol zmeniť zamýšľaný účel, na ktoré sa produkt posudzoval.

(39) Rovnako ako v prípade fyzických opráv alebo úprav by sa produkt s digitálnymi prvkami mal považovať za podstatne upravený zmenou softvéru, ak sa aktualizáciou softvéru mení zamýšľaný účel daného produktu a tieto zmeny výrobca nepredpokladal v počiatočnom posúdení rizika, alebo ak sa povaha nebezpečenstva zmenila alebo sa

zvýšila úroveň kybernetickobezpečnostného rizika v dôsledku aktualizácie softvéru a aktualizovaná verzia produktu sa sprístupňuje na trhu. Ak bezpečnostná aktualizácia, ktorá je navrhnutá na zníženie úrovne kybernetickobezpečnostného rizika produktu s digitálnymi prvkami, nemení zamýšľaný účel produktu s digitálnymi prvkami, nepovažuje sa za podstatnú úpravu. Zvyčajne to zahŕňa situácie, keď si bezpečnostná aktualizácia vyžaduje len malé úpravy zdrojového kódu. Mohlo by ísť napríklad o prípad, keď bezpečnostná aktualizácia rieši známu zraniteľnosť, a to aj úpravou funkcií alebo výkonnosti produktu s digitálnymi prvkami výlučne s cieľom znížiť úroveň kybernetickobezpečnostného rizika. Podobne menšia aktualizácia funkcie, ako je vizuálne zlepšenie alebo pridanie nových piktogramov alebo jazykov do používateľského rozhrania, by sa vo všeobecnosti nemala považovať za podstatnú úpravu. Naopak ak aktualizácia prvku mení pôvodné zamýšľané funkcie alebo typ, či výkonnosť produktu s digitálnymi prvkami a spĺňa vyššie uvedené kritériá, mala by sa považovať za podstatnú úpravu, keďže pridanie nových prvkov zvyčajne vedie k širšej ploche útoku, čím sa kybernetickobezpečnostné riziko zvyšuje. Mohlo by ísť napríklad o prípad, keď sa do aplikácie pridá nový vstupný prvok, ktorý od výrobcu vyžaduje, aby zabezpečil primeranú validáciu vstupov. Pri posudzovaní toho, či sa aktualizácia prvku považuje za podstatnú úpravu, nie je relevantné, či sa poskytuje ako samostatná aktualizácia alebo v kombinácii s bezpečnostnou aktualizáciou. Komisia by mala vydať usmernenia o tom, ako určiť, čo predstavuje podstatnú úpravu.

(40) Vzhľadom na cyklický charakter vývoja softvéru by výrobcovia, ktorí uviedli na trh nové verzie softvérového produktu v dôsledku následnej podstatnej úpravy tohto produktu, mali mať možnosť poskytovať bezpečnostné aktualizácie počas obdobia podpory len pre verziu softvérového produktu, ktorú uviedli na trh naposledy. Mali by mať možnosť tak urobiť, len ak používatelia príslušných predchádzajúcich verzií produktu majú bezplatný prístup k verzii produktu, ktorá bola naposledy uvedená na trh, a nevznikajú im dodatočné náklady na prispôsobenie hardvérového alebo softvérového prostredia, v ktorom produkt prevádzkujú. Mohlo by ísť napríklad o prípad, keď si modernizácia operačného systému pre stolové počítače nevyžaduje nový hardvér, napríklad rýchlejší centrálny procesor alebo väčšiu pamäť. Výrobca by však mal počas obdobia podpory naďalej spĺňať ďalšie požiadavky na riešenie zraniteľností, ako je politika koordinovaného zverejňovania zraniteľností alebo opatrenia na uľahčenie výmeny informácií o potenciálnych zraniteľnostiach pre všetky následné podstatne upravené verzie softvérového produktu uvedeného na trh. Výrobcovia by mali mať možnosť poskytovať menšie bezpečnostné alebo funkčné aktualizácie, ktoré nepredstavujú podstatnú úpravu, len pre poslednú verziu alebo čiastkovú verziu softvérového produktu, ktorý nebol podstatne upravený. Ak zároveň hardvérový produkt, napríklad smartfón, nie je kompatibilný s najnovšou verziou operačného systému, s ktorým bol pôvodne dodaný, výrobca by mal naďalej poskytovať bezpečnostné aktualizácie aspoň pre poslednú kompatibilnú verziu operačného systému počas obdobia podpory.

(41) V súlade so všeobecne zaužívaným pojmom podstatnej úpravy pri produktoch regulovaných harmonizačnými právnymi predpismi Únie je vždy, keď dôjde k podstatnej úprave, ktorá môže ovplyvniť súlad produktu s digitálnymi prvkami 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 mala oznámiť zmena, ktorá by mohla viesť k podstatnej úprave.

(42) Ak produkt s digitálnymi prvkami podlieha „renovovaniu“, „údržbe“ a „oprave“ v zmysle vymedzenia v článku 2 bodoch 18, 19 a 20 nariadenia Európskeho parlamentu a Rady (EÚ) 2024/1781 ([19]), nemusí to nevyhnutne viesť k podstatnej úprave produktu, napríklad ak sa zamýšľaný účel a funkcie nezmenia a neovplyvnená zostane aj úroveň rizika. Modernizácia produktu s digitálnymi prvkami výrobcom by mohla viesť k zmenám v návrhu a vývoji tohto produktu, a preto by mohla mať vplyv na jeho zamýšľaný účel a súlad s požiadavkami stanovenými v tomto nariadení.

(43) Produkty s digitálnymi prvkami by sa mali považovať za dôležité, ak môže byť nepriaznivý účinok zneužitia potenciálnych zraniteľností produktu závažný okrem iného z dôvodu funkcie súvisiacej s kybernetickou bezpečnosťou alebo funkcie, ktorá predstavuje významné riziko nepriaznivých účinkov z hľadiska jeho intenzity a schopnosti narušiť, ovládať alebo spôsobiť poškodenie veľkého počtu iných produktov s digitálnymi prvkami alebo zdravia, bezpečnosti alebo ochrany jeho používateľov pri priamej manipulácii, ako je funkcia centrálneho systému vrátane riadenia siete, kontroly konfigurácie, virtualizácie alebo spracovania osobných údajov. Zraniteľnosti produktov s digitálnymi prvkami, ktoré majú funkciu súvisiacu s kybernetickou bezpečnosťou, napríklad správcovia spúšťania, môžu viesť k šíreniu bezpečnostných problémov v celom dodávateľskom reťazci. Závažnosť dosahu

([19]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1781 z 13. júna 2024, ktorým sa zriaďuje rámec na stanovenie požiadaviek na ekodizajn udržateľných výrobkov, mení smernica (EÚ) 2020/1828 a nariadenie (EÚ) 2023/1542 a zrušuje smernica 2009/125/ES (Ú. v. EÚ L, 2024/1781, 28.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1781/oj).

incidentu sa môže zvýšiť aj vtedy, keď produkt primárne vykonáva funkciu centrálneho systému vrátane správy siete, kontroly konfigurácie, virtualizácie alebo spracovania osobných údajov.

(44) Určité kategórie produktov s digitálnymi prvkami by mali podliehať prísnejším postupom posudzovania zhody pri súčasnom zachovaní primeraného prístupu. Na tento účel by sa mali dôležité produkty s digitálnymi prvkami rozdeliť do dvoch tried podľa úrovne kybernetickobezpečnostného rizika spojeného s týmito kategóriami produktov. Incident zahŕňajúci dôležité produkty s digitálnymi prvkami, ktoré patria do triedy II, by mohol viesť k väčším nepriaznivým účinkom ako incident zahŕňajúci dôležité produkty s digitálnymi prvkami, ktoré patria do triedy I, napríklad z dôvodu povahy ich funkcie súvisiacej s kybernetickou bezpečnosťou alebo výkonu inej funkcie, ktorá so sebou prináša významné riziko nepriaznivých účinkov. So zreteľom na takéto významnejšie nepriaznivé účinky by produkty s digitálnymi prvkami, ktoré patria do triedy II, mohli plniť funkciu súvisiacu s kybernetickou bezpečnosťou alebo inú funkciu, ktorá so sebou prináša významné riziko nepriaznivých účinkov, ktoré je vyššie ako v prípade produktov patriacich do triedy I, alebo by mohli spĺňať obe uvedené kritériá. Dôležité produkty s digitálnymi prvkami, ktoré patria do triedy II, by preto mali podliehať prísnejšiemu postupu posudzovania zhody.

(45) Dôležité produkty s digitálnymi prvkami uvedené v tomto nariadení by sa mali chápať ako produkty, ktoré majú základnú funkciu kategórie dôležitých produktov s digitálnymi prvkami, ktorá je stanovená v tomto nariadení. V tomto nariadení sa napríklad stanovujú kategórie dôležitých produktov s digitálnymi prvkami, ktoré sú podľa ich základnej funkcie vymedzené ako firewally alebo systémy detekcie alebo prevencie narušení v triede II. Preto sú firewally a systémy detekcie alebo prevencie narušení predmetom povinného posudzovania zhody treťou stranou. Neplatí to v prípade iných produktov s digitálnymi prvkami, ktoré nie sú kategorizované ako dôležité produkty s digitálnymi prvkami, ktoré môžu zahŕňať firewally alebo systémy detekcie alebo prevencie narušení. Komisia by mala prijať vykonávací akt s cieľom spresniť technický opis kategórií dôležitých produktov s digitálnymi prvkami, ktoré patria do tried I a II, ako sa stanovuje v tomto nariadení.

(46) Kategórie kritických produktov s digitálnymi prvkami stanovené v tomto nariadení majú funkciu súvisiacu s kybernetickou bezpečnosťou a vykonávajú funkciu, ktorá nesie významné riziko nepriaznivých účinkov, pokiaľ ide o ich intenzitu a schopnosť narušiť, ovládať alebo spôsobiť poškodenie veľkého počtu iných produktov s digitálnymi prvkami prostredníctvom priamej manipulácie. Okrem toho sa tieto kategórie produktov s digitálnymi prvkami považujú za kritické závislosti pre kľúčové subjekty uvedené v článku 3 ods. 1 smernice (EÚ) 2022/2555. Kategórie kritických produktov s digitálnymi prvkami uvedené v prílohe k tomuto nariadeniu vzhľadom na svoju kritickosť už vo veľkej miere využívajú rôzne formy certifikácie a vzťahuje sa na ne aj európska schéma certifikácie kybernetickej bezpečnosti založená na spoločných kritériách (ďalej len „EUCC“) stanovená vo vykonávacom nariadení Komisie (EÚ) 2024/482 ([20]). S cieľom zabezpečiť spoločnú primeranú ochranu kybernetickej bezpečnosti kritických produktov s digitálnymi prvkami v Únii by preto mohlo byť vhodné a primerané, aby sa takéto kategórie produktov prostredníctvom delegovaného aktu podrobili povinnej európskej certifikácii kybernetickej bezpečnosti, ak už existuje príslušná európska schéma certifikácie kybernetickej bezpečnosti, ktorá sa na tieto produkty vzťahuje, a Komisia vykonala posúdenie potenciálneho vplyvu plánovanej povinnej certifikácie na trh. V tomto posúdení by sa mala vziať do úvahy strana ponuky aj dopytu vrátane toho, či existuje dostatočný dopyt po dotknutých produktoch s digitálnymi prvkami z členských štátov aj používateľov na to, aby sa vyžadovala európska certifikácia kybernetickej bezpečnosti, ako aj účely, na ktoré sa majú produkty s digitálnymi prvkami používať, vrátane kritickej závislosti kľúčových subjektov uvedených v článku 3 ods. 1 smernice (EÚ) 2022/2555 od nich. V posúdení by sa mali analyzovať aj potenciálne účinky povinnej certifikácie na dostupnosť týchto produktov na vnútornom trhu a schopnosti a pripravenosť členských štátov vykonávať príslušné európske schémy certifikácie kybernetickej bezpečnosti.

(47) V delegovaných aktoch vyžadujúcich povinnú európsku certifikáciu kybernetickej bezpečnosti by sa mali určiť produkty s digitálnymi prvkami, ktoré majú základnú funkciu kategórie kritických produktov s digitálnymi prvkami podľa tohto nariadenia a ktoré majú podliehať povinnej certifikácii, ako aj požadovanú úroveň záruky, ktorá by mala byť aspoň „významná“. Požadovaná úroveň záruky by mala byť primeraná úrovni kybernetickobezpečnostného rizika spojeného s produktom s digitálnymi prvkami. Ak má napríklad produkt s digitálnymi prvkami základnú

([20]) Vykonávacie nariadenie Komisie (EÚ) 2024/482 z 31. januára 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881, pokiaľ ide o prijatie európskeho systému certifikácie kybernetickej bezpečnosti založeného na spoločných kritériách (EUCC) (Ú. v. EÚ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

funkciu kategórie kritických produktov s digitálnymi prvkami podľa tohto nariadenia a je určený na použitie v citlivom alebo kritickom prostredí, ako sú produkty určené na používanie kľúčovými subjektmi uvedenými v článku 3 ods. 1 smernice (EÚ) 2022/2555, môže sa vyžadovať najvyššiu úroveň záruky.

(48) S cieľom zabezpečiť v Únii spoločnú primeranú kybernetickobezpečnostnú ochranu produktov s digitálnymi prvkami, ktoré majú základnú funkciu kategórie kritických produktov s digitálnymi prvkami podľa tohto nariadenia, Komisia by mala byť tiež splnomocnená prijímať delegované akty s cieľom zmeniť toto nariadenie doplnením alebo zrušením kategórií kritických produktov s digitálnymi prvkami, v prípade ktorých by sa od výrobcov mohlo vyžadovať, aby získali európsky certifikát kybernetickej bezpečnosti v rámci európskej schémy certifikácie kybernetickej bezpečnosti podľa nariadenia (EÚ) 2019/881 na preukázanie súladu s týmto nariadením. Do týchto kategórií sa môže doplniť nová kategória kritických produktov s digitálnymi prvkami, ak kľúčové subjekty uvedené v článku 3 ods. 1 smernice (EÚ) 2022/2555 od nich kriticky závisia, alebo ak sú ovplyvnené incidentmi alebo obsahujú zneužívané zraniteľnosti, čo by mohlo viesť k narušeniam kritických dodávateľských reťazcov. Pri posudzovaní potreby doplniť alebo zrušiť kategórie kritických produktov s digitálnymi prvkami prostredníctvom delegovaného aktu by Komisia mala mať možnosť zohľadniť, či členské štáty na vnútroštátnej úrovni identifikovali produkty s digitálnymi prvkami, ktoré zohrávajú kľúčovú úlohu z hľadiska odolnosti kľúčových subjektov uvedených v článku 3 ods. 1 smernice (EÚ) 2022/2555 a ktoré čoraz viac čelia kybernetickým útokom v dodávateľskom reťazci s možnými vážnymi rušivými účinkami. Komisia by okrem toho mala byť schopná zohľadniť výsledok koordinovaného posúdenia bezpečnostných rizík kritických dodávateľských reťazcov na úrovni Únie, ktoré sa vykonáva v súlade s článkom 22 smernice (EÚ) 2022/2555.

(49) Pri príprave opatrení na vykonávanie tohto nariadenia by Komisia mala zabezpečiť štruktúrované a pravidelné konzultácie so širokou škálou príslušných zainteresovaných strán. Malo by to tak byť najmä v prípade, keď Komisia usúdi, že sú potrebné potenciálne aktualizácie zoznamov kategórií dôležitých alebo kritických produktov s digitálnymi prvkami, keď by sa malo konzultovať s príslušnými výrobcami a mali by sa zohľadniť ich názory s cieľom analyzovať kybernetickobezpečnostné riziká, ako aj vyváženosť nákladov a prínosov označenia takýchto kategórií produktov za dôležité alebo kritické.

(50) V tomto nariadení sa rieši kybernetickobezpečnostné riziká cieleným spôsobom. Produkty s digitálnymi prvkami by však mohli predstavovať ďalšie bezpečnostné riziká, ktoré vždy nesúvisia s kybernetickou bezpečnosťou, ale môžu byť dôsledkom narušenia bezpečnosti. Tieto riziká by mali byť naďalej regulované inými príslušnými harmonizačnými právnymi predpismi Únie, než je toto nariadenie. Ak sa neuplatňujú žiadne iné harmonizačné právne predpisy Únie, než je toto nariadenie, malo by sa uplatňovať nariadenie Európskeho parlamentu a Rady (EÚ) 2023/988 ([21]). Preto vzhľadom na cielenú povahu tohto nariadenia by sa odchylne od článku 2 ods. 1 tretieho pododseku písm. b) nariadenia (EÚ) 2023/988 mala kapitola III oddiel 1, kapitoly V a VII a kapitoly IX až XI nariadenia (EÚ) 2023/988 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 stanovené v iných harmonizačných právnych predpisoch Únie, než je toto nariadenie, v zmysle článku 3 bodu 27 nariadenia (EÚ) 2023/988.

(51) Produkty s digitálnymi prvkami klasifikované ako vysokorizikové systémy umelej inteligencie (ďalej len „vysokorizikové systémy AI“) podľa článku 6 nariadenia Európskeho parlamentu a Rady (EÚ) 2024/1689 ([22]), ktoré patria do rozsahu pôsobnosti tohto nariadenia, by mali vyhovovať základným požiadavkám kybernetickej bezpečnosti stanoveným v tomto nariadení. Ak tieto vysokorizikové systémy AI spĺňajú základné požiadavky kybernetickej bezpečnosti stanovené v tomto nariadení, mali by sa považovať za systémy, ktoré spĺňajú požiadavky kybernetickej bezpečnosti stanovené v článku 15 nariadenia (EÚ) 2024/1689, pokiaľ sa na tieto požiadavky vzťahuje EÚ vyhlásenie o zhode alebo jeho časti vydané podľa tohto nariadenia. Na tento účel by posúdenie kybernetickobezpečnostných rizík spojených s produktom s digitálnymi prvkami klasifikovaným ako vysokorizikový systém AI podľa nariadenia (EÚ) 2024/1689, ktoré sa má zohľadniť vo fáze plánovania, navrhovania, vývoja, výroby, dodávky a údržby takéhoto produktu, ako sa vyžaduje podľa tohto nariadenia, malo zohľadňovať riziká pre kybernetickú odolnosť systému umelej inteligencie, pokiaľ ide o pokusy neoprávnených tretích strán zmeniť jeho

([21]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/988 z 10. mája 2023 o všeobecnej bezpečnosti výrobkov, ktorým sa mení nariadenie Európskeho parlamentu a Rady (EÚ) č. 1025/2012 a smernica Európskeho parlamentu a Rady (EÚ) 2020/1828 a zrušuje smernica Európskeho parlamentu a Rady 2001/95/ES a smernica Rady 87/357/EHS (Ú. v. EÚ L 135, 23.5.2023, s. 1).

([22]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii) (Ú. v. EÚ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

používanie, správanie alebo výkonnosť vrátane zraniteľností súvisiacich s umelou inteligenciou, ako sú otravy údajov alebo nepriateľské útoky, ako aj relevantné riziká pre základné práva v súlade s nariadením (EÚ) 2024/1689. Pokiaľ ide o postupy posudzovania zhody týkajúce sa základných požiadaviek kybernetickej bezpečnosti pre na produkt s digitálnymi prvkami, ktorý spadá do rozsahu pôsobnosti tohto nariadenia a ktorý je klasifikovaný ako vysokorizikový systém AI, namiesto príslušných ustanovení tohto nariadenia by sa mal spravidla uplatňovať článok 43 nariadenia (EÚ) 2024/1689. Toto pravidlo by však nemalo viesť k zníženiu potrebnej úrovne záruky pre dôležité alebo kritické produkty s digitálnymi prvkami, ako sú uvedené v tomto nariadení. Odchylne od tohto pravidla by preto vysokorizikové systémy AI, ktoré patria do rozsahu pôsobnosti nariadenia (EÚ) 2024/1689 a zároveň sú tiež dôležitými alebo kritickými produktmi s digitálnymi prvkami, ako sú uvedené v tomto nariadení, a na ktoré sa uplatňuje postup posudzovania zhody na základe vnútornej kontroly uvedený v prílohe VI k nariadeniu (EÚ) 2024/1689, mali podliehať postupom posudzovania zhody podľa tohto nariadenia, pokiaľ ide o základné požiadavky kybernetickej bezpečnosti stanovené v tomto nariadení. V takom prípade by sa na všetky ostatné aspekty, na ktoré sa vzťahuje nariadenie (EÚ) 2024/1689, mali uplatňovať príslušné ustanovenia o posudzovaní zhody na základe vnútornej kontroly uvedené v prílohe VI k uvedenému nariadeniu.

(52) S cieľom zlepšiť bezpečnosť produktov s digitálnymi prvkami uvádzaných na vnútorný trh je potrebné stanoviť základné požiadavky kybernetickej bezpečnosti uplatniteľné na takéto produkty. Týmito základnými požiadavkami kybernetickej bezpečnosti by nemalo byť dotknuté koordinované posudzovanie bezpečnostných rizík kritických dodávateľských reťazcov na úrovni Únie stanovené v článku 22 smernice (EÚ) 2022/2555, pri ktorom sa zohľadňujú technické a v relevantnom prípade aj netechnické faktory rizík, ako je neprimeraný vplyv tretej krajiny na dodávateľov. Okrem toho by nimi 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 Komisie (EÚ) 2019/534 ([23]), v koordinovanom posúdení rizík na úrovni EÚ, pokiaľ ide o kybernetickú bezpečnosť sietí 5G, a v súbore nástrojov EÚ pre kybernetickú bezpečnosť 5G, ktoré schválila skupina pre spoluprácu zriadená podľa článku 14 smernice (EÚ) 2022/2555.

(53) Výrobcovia produktov patriacich do rozsahu pôsobnosti nariadenia Európskeho parlamentu a Rady (EÚ) 2023/1230 ([24]), ktoré sú zároveň produktmi s digitálnymi prvkami v zmysle vymedzenia v tomto nariadení, by mali spĺňať základné požiadavky kybernetickej bezpečnosti stanovené v tomto nariadení, ako aj základné požiadavky na bezpečnosť a ochranu zdravia stanovené v nariadení (EÚ) 2023/1230. Základnými požiadavkami kybernetickej bezpečnosti stanovenými v tomto nariadení a určitými základnými požiadavkami stanovenými v nariadení (EÚ) 2023/1230 sa môžu riešiť podobné kybernetickobezpečnostné riziká. Dodržiavanie základných požiadaviek kybernetickej bezpečnosti stanovených v tomto nariadení by preto mohlo uľahčiť dodržiavanie základných požiadaviek na určité kybernetickobezpečnostné riziká stanovené v nariadení (EÚ) 2023/1230, a to najmä požiadaviek na ochranu pred zneužitím a bezpečnosť a spoľahlivosť ovládacích systémov stanovených v oddieloch 1.1.9 a 1.2.1 prílohy III k uvedenému nariadeniu. Takéto synergie musí výrobca preukázať, napríklad uplatnením harmonizovaných noriem alebo iných technických špecifikácií, ktoré sa vzťahujú na príslušné základné požiadavky kybernetickej bezpečnosti, ak sú k dispozícii, na základe posúdenia rizík, ktoré sa vzťahuje na uvedené kybernetickobezpečnostné riziká. Výrobca by sa mal riadiť aj uplatniteľnými postupmi posudzovania zhody stanovenými v tomto nariadení a v nariadení (EÚ) 2023/1230. Komisia a európske normalizačné organizácie by v rámci prípravných prác na podporu vykonávania tohto nariadenia a nariadenia (EÚ) 2023/1230 a súvisiacich normalizačných postupov mali podporovať konzistentnosť spôsobu posudzovania kybernetickobezpečnostných rizík a toho, ako majú byť tieto riziká pokryté harmonizovanými normami, pokiaľ ide o príslušné základné požiadavky. Komisia a európske normalizačné organizácie by mali toto nariadenie zohľadniť najmä pri príprave a vypracovaní harmonizovaných noriem s cieľom uľahčiť vykonávanie nariadenia (EÚ) 2023/1230, najmä pokiaľ ide o aspekty kybernetickej bezpečnosti súvisiace s ochranou pred zneužitím a bezpečnosťou a spoľahlivosťou ovládacích systémov stanovených v oddieloch 1.1.9 a 1.2.1 prílohy III k uvedenému nariadeniu. Komisia by mala poskytnúť usmernenia na podporu výrobcov, na ktorých sa vzťahuje toto nariadenie a tiež aj nariadenie (EÚ) 2023/1230, najmä s cieľom uľahčiť preukazovanie dodržiavania príslušných základných požiadaviek stanovených v tomto nariadení a v nariadení (EÚ) 2023/1230.

(54) S cieľom zaistiť, aby boli produkty s digitálnymi prvkami zabezpečené tak v čase ich uvedenia na trh, ako aj počas ich očakávaného obdobia používania je potrebné stanoviť základné požiadavky kybernetickej bezpečnosti na riešenie zraniteľností a základné požiadavky kybernetickej bezpečnosti týkajúce sa vlastností produktov s digitálnymi prvkami. Hoci by výrobcovia mali splniť všetky základné požiadavky kybernetickej bezpečnosti týkajúce sa riešenia

([23]) Odporúčanie Komisie (EÚ) 2019/534 z 26. marca 2019 Kybernetická bezpečnosť sietí 5G (Ú. v. EÚ L 88, 29.3.2019, s. 42).
([24]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1230 zo 14. júna 2023 o strojových zariadeniach a o zrušení smernice Európskeho parlamentu a Rady 2006/42/ES a smernice Rady 73/361/EHS (Ú. v. EÚ L 165, 29.6.2023, s. 1).

zraniteľností počas celého obdobia podpory, mali by určiť, ktoré ďalšie základné požiadavky kybernetickej bezpečnosti týkajúce sa vlastností produktu sú relevantné pre príslušný druh produktu s digitálnymi prvkami. Na tento účel by výrobcovia mali vykonať posúdenie kybernetickobezpečnostných rizík spojených s produktom s digitálnymi prvkami s cieľom identifikovať príslušné riziká a relevantné základné požiadavky kybernetickej bezpečnosti, aby mohli sprístupňovať svoje produkty s digitálnymi prvkami bez známych zneužiteľných zraniteľností, ktoré by mohli mať vplyv na bezpečnosť týchto produktov, a primerane uplatňovať vhodné harmonizované normy, spoločné špecifikácie alebo európske či medzinárodné normy.

(55) Ak na produkt s digitálnymi prvkami nemožno uplatniť určité základné požiadavky kybernetickej bezpečnosti, výrobca by mal v posúdení kybernetickobezpečnostného rizika priloženého k technickej dokumentácii uviesť jasné odôvodnenie. Môže ísť o prípady, keď je základná požiadavka kybernetickej bezpečnosti nezlučiteľná s povahou produktu s digitálnymi prvkami. Napríklad zamýšľaný účel produktu s digitálnymi prvkami môže vyžadovať, aby výrobca dodržiaval všeobecne uznávané normy interoperability, aj keď sa jeho bezpečnostné prvky už nepovažujú za najmodernejšie. Podobne sa v iných právnych predpisoch Únie vyžaduje, aby výrobcovia uplatňovali osobitné požiadavky na interoperabilitu. Ak sa základná požiadavka kybernetickej bezpečnosti na produkt s digitálnymi prvkami nevzťahuje, ale výrobca v súvislosti s touto základnou požiadavkou kybernetickej bezpečnosti identifikoval kybernetickobezpečnostné riziká, mal by prijať opatrenia na riešenie týchto rizík inými prostriedkami, napríklad obmedzením zamýšľaného účelu produktu na dôveryhodné prostredia alebo informovaním používateľov o týchto rizikách.

(56) Jedným z najdôležitejších opatrení, ktoré majú používatelia prijať na ochranu svojich produktov s digitálnymi prvkami pred kybernetickými útokmi, je čo najskôr nainštalovať najnovšie dostupné bezpečnostné aktualizácie. Výrobcovia by preto mali navrhovať svoje produkty a zavádzať postupy tak, aby zabezpečili, že produkty s digitálnymi prvkami zahŕňajú funkcie, ktoré umožňujú automatické oznamovanie, distribúciu, sťahovanie a inštaláciu bezpečnostných aktualizácií, najmä v prípade spotrebných produktov. Mali by tiež umožniť v poslednom kroku súhlas so stiahnutím a inštaláciou bezpečnostných aktualizácií. Používatelia by mali mať ponechanú možnosť deaktivovať automatické aktualizácie jasným a ľahko použiteľným mechanizmom a so zrozumiteľným návodom na vypnutie aktualizácie. Požiadavky týkajúce sa automatických aktualizácií stanovené v prílohe k tomuto nariadeniu sa neuplatňujú na produkty s digitálnymi prvkami, ktoré sú primárne určené na integráciu ako komponenty do iných produktov. Nevzťahujú sa ani na produkty s digitálnymi prvkami, v prípade ktorých používatelia dôvodne neočakávajú automatické aktualizácie vrátane produktov s digitálnymi prvkami, ktoré sa majú používať v profesionálnych sieťach informačných a komunikačných technológií, a najmä v kritickom a priemyselnom prostredí, v ktorom by automatická aktualizácia mohla spôsobiť zasahovanie do prevádzky. Bez ohľadu na to, či je produkt s digitálnymi prvkami navrhnutý tak, aby prijímal automatické aktualizácie alebo nie, jeho výrobca by mal používateľov informovať o zraniteľnostiach a bezodkladne poskytnúť bezpečnostné aktualizácie. Ak má produkt s digitálnymi prvkami používateľské rozhranie alebo podobné technické prostriedky umožňujúce priamu interakciu s používateľmi, výrobca by mal takéto funkcie využiť na informovanie používateľov o tom, že ich produkt s digitálnymi prvkami dosiahol koniec obdobia podpory. Oznámenia by sa mali obmedziť na to, čo je potrebné na zabezpečenie účinného prijímania týchto informácií, a nemali by mať negatívny vplyv na skúsenosti používateľov s produktom s digitálnymi prvkami.

(57) S cieľom zlepšiť transparentnosť procesov riešenia zraniteľností a zabezpečiť, aby používatelia neboli povinní inštalovať nové aktualizácie funkcií výlučne na účely prijímania najnovších bezpečnostných aktualizácií, by výrobcovia mali zabezpečiť, ak je to technicky možné, aby sa nové bezpečnostné aktualizácie poskytovali oddelene od aktualizácií funkcií.

(58) V spoločnom oznámení Komisie a vysokého predstaviteľa Únie pre zahraničné veci a bezpečnostnú politiku z 20. júna 2023 s názvom „Európska stratégia hospodárskej bezpečnosti“ sa uvádza, že Únia musí maximalizovať prínosy svojej hospodárskej otvorenosti a zároveň minimalizovať riziká vyplývajúce z hospodárskej závislosti od vysokorizikových predajcov, a to prostredníctvom spoločného strategického rámca pre hospodársku bezpečnosť Únie. Závislosť od vysokorizikových dodávateľov produktov s digitálnymi prvkami môže predstavovať strategické riziko, ktoré sa musí riešiť na úrovni Únie, najmä ak sú produkty s digitálnymi prvkami určené na použitie pre kľúčové subjekty uvedené v článku 3 ods. 1 smernice (EÚ) 2022/2555. Takéto riziká môžu byť spojené nielen s jurisdikciou vzťahujúcou sa na výrobcu, charakteristikami jeho vlastníckej štruktúry a kontrolnými prepojeniami na vládu tretej krajiny, v ktorej je usadený, najmä ak daná tretia krajina vykonáva priemyselnú špionáž alebo nezodpovedné štátne zásahy v kybernetickom priestore a jej právne predpisy umožňujú svojvoľný prístup k akémukoľvek druhu operácií alebo k údajom podnikov, a to vrátane citlivých obchodných údajov, a môže ukladať povinnosti na spravodajské účely bez demokratického systému bŕzd a protiváh, mechanizmov dohľadu, riadneho procesu alebo práva odvolať sa na nezávislý súd alebo tribunál. Pri určovaní závažnosti kybernetickobezpečnostného rizika v zmysle tohto nariadenia by Komisia a orgány dohľadu nad trhom v rámci svojich povinností stanovených v tomto nariadení mali zohľadniť aj netechnické rizikové faktory, najmä tie, ktoré boli identifikované na základe

koordinovaných posúdení bezpečnostných rizík kritických dodávateľských reťazcov na úrovni Únie, ktoré sa vykonávajú v súlade s článkom 22 smernice (EÚ) 2022/2555.

(59) Na účely zaistenia bezpečnosti produktov s digitálnymi prvkami po ich uvedení na trh by výrobcovia mali určiť obdobie podpory, ktoré by malo zodpovedať času predpokladaného používania produktu s digitálnymi prvkami. Pri určovaní obdobia podpory by mal výrobca zohľadniť najmä primerané očakávania používateľov, povahu produktu, ako aj príslušné právo Únie určujúce životnosť produktov s digitálnymi prvkami. Výrobcovia by mali mať možnosť zohľadniť aj iné relevantné faktory. Kritériá by sa mali uplatňovať spôsobom, ktorý pri určovaní obdobia podpory zabezpečí proporcionalitu. Výrobca by mal na požiadanie poskytnúť orgánom dohľadu nad trhom informácie, ktoré sa zohľadnili pri určovaní obdobia podpory produktu s digitálnymi prvkami.

(60) Obdobie podpory, počas ktorého výrobca zabezpečuje účinné riešenie zraniteľností, by nemalo byť kratšie ako päť rokov, pokiaľ životnosť produktu s digitálnymi prvkami nie je kratšia ako päť rokov, pričom v takom prípade by mal výrobca zabezpečiť riešenie zraniteľností počas tejto životnosti. Ak sa dôvodne očakáva, že produkt s digitálnymi prvkami sa bude používať dlhšie ako päť rokov, ako je to často v prípade hardvérových komponentov, ako sú základné dosky alebo mikroprocesory, sieťových zariadení, ako sú smerovače, modemy alebo prepínače, ako aj softvéru, ako sú operačné systémy alebo nástroje na editovanie videí, výrobcovia by mali zabezpečiť dlhšie obdobia podpory. Najmä produkty s digitálnymi prvkami určené na použitie v priemyselnom prostredí, ako sú priemyselné riadiace systémy, sa často používajú počas výrazne dlhšieho obdobia. Výrobca by mal mať možnosť vymedziť obdobie podpory kratšie ako päť rokov, len ak je to odôvodnené povahou dotknutého produktu s digitálnymi prvkami a ak sa očakáva, že tento produkt sa bude používať menej ako päť rokov, pričom v takom prípade by obdobie podpory malo zodpovedať očakávanému času používania. Napríklad životnosť aplikácie na sledovanie kontaktov určenej na použitie počas pandémie by mohla byť obmedzená na trvanie pandémie. Okrem toho niektoré softvérové aplikácie môžu byť pre svoju povahu sprístupnené len s predplatným, najmä ak sa aplikácia stane pre používateľa nedostupnou, a teda po skončení predplatného sa už nepoužíva.

(61) S cieľom zabezpečiť, aby sa zraniteľnosti mohli riešiť po skončení obdobia podpory, keď sa obdobie podpory produktov s digitálnymi prvkami skončí, výrobcovia by mali zvážiť poskytnutie zdrojového kódu takýchto produktov s digitálnymi prvkami buď iným podnikom, ktoré sa zaviažu predĺžiť poskytovanie služieb riešenia zraniteľností, alebo verejnosti. Ak výrobcovia poskytnú zdrojový kód iným podnikom, mali by byť schopní chrániť vlastníctvo produktu s digitálnymi prvkami a zabrániť poskytovaniu zdrojového kódu verejnosti, napríklad prostredníctvom zmluvných ustanovení.

(62) S cieľom zabezpečiť, aby výrobcovia v celej Únii určili podobné obdobia podpory pre porovnateľné produkty s digitálnymi prvkami, skupina ADCO by mala zverejňovať štatistiky o priemerných obdobiach podpory určených výrobcami pre kategórie produktov s digitálnymi prvkami a vydať usmernenia, v ktorých sa uvedú vhodné obdobia podpory pre takéto kategórie. Okrem toho s cieľom zabezpečiť harmonizovaný prístup na celom vnútornom trhu by Komisia mala mať možnosť prijímať delegované akty, v ktorých stanoví minimálne obdobia podpory pre konkrétne kategórie produktov, ak z údajov poskytnutých orgánmi dohľadu nad trhom vyplýva, že obdobia podpory určené výrobcami buď systematicky nie sú v súlade s kritériami na určenie období podpory stanovenými v tomto nariadení, alebo že výrobcovia v rôznych členských štátoch neodôvodnene určujú odlišné obdobia podpory.

(63) Výrobcovia by mali zriadiť jednotné kontaktné miesto, ktoré používateľom umožní jednoduchú komunikáciu s nimi, a to aj na účely oznamovania a prijímania informácií o zraniteľnosti produktu s digitálnym prvkom. Mali by zabezpečiť jednoduchý prístup používateľov k jednotnému kontaktnému miestu, jasne uviesť jeho dostupnosť a tieto informácie aktualizovať. Ak sa výrobcovia rozhodnú ponúkať automatizované nástroje, napríklad chatboty, mali by uviesť aj telefónne číslo alebo iné digitálne kontaktné prostriedky, ako je e-mailová adresa alebo kontaktný formulár. Jednotné kontaktné miesto by nemalo využívať výlučne automatizované nástroje.

(64) Výrobcovia by mali svoje produkty s digitálnymi prvkami sprístupniť na trhu so štandardne zabezpečenou konfiguráciou a používateľom bezplatne poskytovať bezpečnostné aktualizácie. Výrobcovia by mali mať možnosť odchýliť sa od základných požiadaviek kybernetickej bezpečnosti len v súvislosti s produktmi na mieru, ktoré sú namontované na konkrétny účel pre konkrétneho komerčného používateľa, a ak výrobca aj používateľ výslovne súhlasili s iným súborom zmluvných podmienok.

(65) Výrobcovia by mali súčasne prostredníctvom jednotnej oznamovacej platformy informovať jednotku pre riešenie počítačových bezpečnostných incidentov (ďalej len „CSIRT“) určenú za koordinátora, ako aj agentúru ENISA o aktívne zneužívaných zraniteľnostiach v produktoch s digitálnymi prvkami, ako aj o závažných incidentoch, ktoré majú vplyv na bezpečnosť týchto produktov. Tieto oznámenia by sa mali podávať prostredníctvom koncového bodu na elektronické oznamovanie jednotky CSIRT určenej za koordinátora a mali by byť súčasne prístupné agentúre ENISA.

(66) Výrobcovia by mali oznamovať aktívne zneužívané zraniteľnosti s cieľom zabezpečiť, aby jednotky CSIRT určené za koordinátorov a agentúra ENISA mali primeraný prehľad o takýchto zraniteľnostiach a aby im boli poskytnuté informácie potrebné na plnenie ich úloh stanovených v smernici (EÚ) 2022/2555 a zvýšenie celkovej úrovne kybernetickej bezpečnosti kľúčových a dôležitých subjektov uvedených v článku 3 uvedenej smernice, ako aj zabezpečenie účinného fungovania orgánov dohľadu nad trhom. 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. Agentúra ENISA by mala po dohode s výrobcom zverejniť pevné zraniteľnosti v európskej databáze zraniteľností zriadenej podľa článku 12 ods. 2 smernice (EÚ) 2022/2555. Európska databáza zraniteľností bude pomáhať výrobcom pri zisťovaní známych zneužiteľných zraniteľností v ich produktoch, aby sa zabezpečilo, že sa na trhu budú sprístupňovať bezpečné produkty.

(67) Výrobcovia by takisto mali oznámiť jednotke CSIRT určenej za koordinátora a agentúre ENISA každý závažný incident, ktorý má vplyv na bezpečnosť produktu s digitálnymi prvkami. S cieľom zaistiť používateľom možnosť rýchlo reagovať na závažné incidenty, ktoré majú vplyv na bezpečnosť ich produktov s digitálnymi prvkami, by výrobcovia mali informovať svojich používateľov aj o akomkoľvek takomto incidente a v relevantnom prípade 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 kybernetickobezpečnostnými rizikami.

(68) Aktívne zneužívané zraniteľnosti sa týkajú prípadov, keď výrobca zistí, že narušenie bezpečnosti ovplyvňujúce jeho používateľov alebo akékoľvek iné fyzické alebo právnické osoby bolo spôsobené tým, že škodlivý subjekt využil chybu v jednom z produktov s digitálnymi prvkami, ktoré výrobca sprístupnil na trhu. Príkladmi takýchto zraniteľností by mohli byť nedostatky v identifikačných a autentifikačných funkciách produktu. Zraniteľnosti, ktoré sa zistia bez zlého úmyslu na účely testovania, skúmania, opravy alebo zverejnenia v dobrej viere s cieľom podporiť bezpečnosť alebo ochranu vlastníka systému a jeho používateľov, by nemali podliehať povinnému oznamovaniu. Závažné incidenty, ktoré majú vplyv na bezpečnosť produktu s digitálnymi prvkami, sa na druhej strane týkajú situácií, keď kybernetickobezpečnostný incident ovplyvňuje postupy vývoja, výroby alebo údržby výrobcu takým spôsobom, že by mohol viesť k zvýšenému kybernetickobezpečnostnému riziku pre používateľov alebo iné osoby. Takýto závažný incident by mohol zahŕňať situáciu, keď útočník úspešne vloží škodlivý kód do kanála, prostredníctvom ktorého výrobca poskytuje bezpečnostné aktualizácie používateľom.

(69) S cieľom zabezpečiť rýchle rozposielanie oznámení všetkým príslušným jednotkám CSIRT určeným za koordinátorov a s cieľom umožniť výrobcom predložiť jediné oznámenie v každej fáze postupu oznamovania by agentúra ENISA mala zriadiť jednotnú oznamovaciu platformu s vnútroštátnymi koncovými bodmi na elektronické oznamovanie. Agentúra ENISA by mala riadiť každodennú prevádzku tejto jednotnej oznamovacej platformy a vykonávať jej údržbu. Jednotky CSIRT určené za koordinátorov by mali informovať svoje príslušné orgány dohľadu nad trhom o oznámených zraniteľnostiach alebo incidentoch. Jednotná oznamovacia platforma by mala byť navrhnutá tak, aby zabezpečovala dôvernosť oznámení, najmä pokiaľ ide o zraniteľnosti, pre ktoré ešte nie je k dispozícii bezpečnostná aktualizácia. Agentúra ENISA by okrem toho mala zaviesť postupy na bezpečné a dôverné zaobchádzanie s informáciami. Agentúra ENISA by na základe informácií, ktoré zhromažďuje, mala každé dva roky vypracovať technickú správu o nových trendoch v oblasti kybernetickobezpečnostných rizík produktov s digitálnymi prvkami a predložiť ju skupine pre spoluprácu zriadenej podľa článku 14 smernice (EÚ) 2022/2555.

(70) Za výnimočných okolností, a najmä na žiadosť výrobcu, by jednotka CSIRT určená za koordinátora, ktorej bolo oznámenie pôvodne doručené, mala mať možnosť rozhodnúť o odložení jeho rozosielania ostatným príslušným jednotkám CSIRT určeným za koordinátorov prostredníctvom jednotnej oznamovacej platformy, ak to možno odôvodniť dôvodmi súvisiacimi s kybernetickou bezpečnosťou a na nevyhnutne potrebné obdobie. Jednotka CSIRT určená za koordinátora by mala bezodkladne informovať agentúru ENISA o svojom rozhodnutí odložiť rozosielanie informácií, o dôvodoch takéhoto rozhodnutia, ako aj o tom, kedy má v úmysle rozoslanie vykonať. Komisia by mala prostredníctvom delegovaného aktu špecifikovať podmienky, za ktorých by sa mohli uplatňovať dôvody súvisiace s kybernetickou bezpečnosťou, a pri príprave návrhu delegovaného aktu by mala spolupracovať so sieťou jednotiek CSIRT zriadenou podľa článku 15 smernice (EÚ) 2022/2555 a agentúrou ENISA. K príkladom dôvodov súvisiacich s kybernetickou bezpečnosťou patrí prebiehajúci koordinovaný postup zverejňovania zraniteľností alebo situácie, keď má výrobca čoskoro poskytnúť zmierňujúce opatrenie a kybernetickobezpečnostné riziká okamžitého rozoslania informácií prostredníctvom jednotnej oznamovacej platformy prevažujú nad jeho prínosmi. Ak o to

jednotka CSIRT určená za koordinátora požiada, agentúra ENISA by jej mala byť schopná poskytnúť podporu pri uplatňovaní dôvodov súvisiacich s kybernetickou bezpečnosťou v súvislosti s odloženým rozoslaním oznámenia na základe informácií, ktoré agentúra ENISA prijala od tejto jednotky CSIRT o rozhodnutí pozastaviť oznámenie z uvedených dôvodov kybernetickej bezpečnosti. Okrem toho by sa agentúre ENISA za obzvlášť výnimočných okolností nemali doručovať všetky podrobnosti oznámenia o aktívne zneužívanej zraniteľnosti súčasne. Ide o prípad, keď výrobca vo svojom oznámení uvedie, že oznámenú zraniteľnosť aktívne zneužíva škodlivý subjekt a že podľa dostupných informácií nebola zneužitá v žiadnom inom členskom štáte okrem členského štátu jednotky CSIRT určenej za koordinátora, ktorej výrobca zraniteľnosť oznámil, pričom akýmkoľvek ďalším okamžitým rozoslaním oznámenej zraniteľnosti by sa pravdepodobne poskytli informácie, ktorých zverejnenie by bolo v rozpore so základnými záujmami daného členského štátu, alebo keď oznámená zraniteľnosť predstavuje bezprostredné vysoké kybernetickobezpečnostné riziko vyplývajúce z ďalšieho rozosielania. V takýchto prípadoch agentúra ENISA zároveň získa prístup len k informáciám o tom, že výrobca podal oznámenie, k všeobecným informáciám o dotknutom produkte s digitálnymi prvkami, k informáciám o všeobecnej povahe zneužitia a k informáciám o tom, že výrobca uviedol dané bezpečnostné dôvody, a že sa preto neposkytuje úplný obsah oznámenia. Úplné oznámenie by sa následne malo sprístupniť agentúre ENISA a ostatným príslušným jednotkám CSIRT určeným za koordinátorov, keď jednotka CSIRT určená za koordinátora, ktorej bolo oznámenie pôvodne doručené, zistí, že tieto bezpečnostné dôvody, ktoré zodpovedajú mimoriadne výnimočným okolnostiam stanoveným v tomto nariadení, zanikli. Ak sa agentúra ENISA na základe dostupných informácií domnieva, že existuje systémové riziko ovplyvňujúce bezpečnosť na vnútornom trhu, odporučí jednotke CSIRT, ktorej bolo oznámenie doručené, aby rozoslala úplné oznámenie ostatným jednotkám CSIRT určeným za koordinátorov a samotnej agentúre ENISA.

(71) Keď výrobcovia oznámia aktívne zneužívanú zraniteľnosť alebo závažný incident, ktorý má vplyv na bezpečnosť produktu s digitálnymi prvkami, mali by uviesť, do akej miery považujú oznámené informácie za citlivé. Jednotka CSIRT určená za koordinátora, ktorej je oznámenie doručené ako prvej, by mala tieto informácie zohľadniť pri posudzovaní toho, či oznámenie vedie k výnimočným okolnostiam, ktoré by mohli byť dôvodom pre odložené rozoslanie oznámenia ostatným príslušným jednotkám CSIRT určeným za koordinátorov na základe opodstatnených dôvodov súvisiacich s kybernetickou bezpečnosťou. Tieto informácie by mala zohľadniť aj pri posudzovaní toho, či oznámenie aktívne zneužívanej zraniteľnosti vedie k mimoriadne výnimočným okolnostiam, ktoré odôvodňujú, že úplné oznámenie nie je súčasne sprístupnené agentúre ENISA. Jednotky CSIRT určené za koordinátorov by napokon mali byť schopné zohľadniť tieto informácie pri určovaní vhodných opatrení na zmiernenie rizík vyplývajúcich z takýchto zraniteľností a incidentov.

(72) S cieľom zjednodušiť oznamovanie informácií požadovaných podľa tohto nariadenia a vzhľadom na ďalšie doplňujúce požiadavky na oznamovanie stanovené v právnych predpisoch Únie, ako je nariadenie (EÚ) 2016/679, nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 ([25]), smernica Európskeho parlamentu a Rady 2002/58/ES ([26]) a smernica (EÚ) 2022/2555, ako aj znížiť administratívnu záťaž subjektov sa členské štáty vyzývajú, aby zvážili zriadenie národných jednotných kontaktných miest pre takéto požiadavky na oznamovanie. Používanie takéhoto národného jednotného kontaktného miesta na oznamovanie bezpečnostných incidentov podľa nariadenia (EÚ) 2016/679 a smernice 2002/58/ES by nemalo mať vplyv na uplatňovanie ustanovení nariadenia (EÚ) 2016/679 a smernice 2002/58/ES, najmä nie na uplatňovanie ustanovení o nezávislosti orgánov v nich uvedených. Pri zriaďovaní jednotnej oznamovacej platformy uvedenej v tomto nariadení by agentúra ENISA mala zohľadniť možnosť začlenenia vnútroštátnych koncových bodov na elektronické oznamovanie uvedených v tomto nariadení do národných jednotných kontaktných miest, ktoré môžu prijímať aj iné oznámenia požadované podľa práva Únie.

(73) Pri zriaďovaní jednotnej oznamovacej platformy uvedenej v tomto nariadení a s cieľom využiť predchádzajúce skúsenosti by agentúra ENISA mala konzultovať s inými inštitúciami alebo agentúrami Únie, ktoré spravujú platformy alebo databázy podľa prísnych bezpečnostných požiadaviek, ako je Agentúra Európskej únie na prevádzkové riadenie rozsiahlych informačných systémov v priestore slobody, bezpečnosti a spravodlivosti (eu-LISA). Agentúra ENISA by mala uskutočniť analýzu možnej doplnkovosti s európskou databázou zraniteľností zriadenou podľa článku 12 ods. 2 smernice (EÚ) 2022/2555.

(74) Výrobcovia a iné fyzické a právnické osoby by mali mať možnosť dobrovoľne oznámiť jednotke CSIRT určenej za koordinátora alebo agentúre ENISA každú zraniteľnosť produktu s digitálnymi prvkami, kybernetické hrozby, ktoré

([25]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011 (Ú. v. EÚ L 333, 27.12.2022, s. 1).

([26]) Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (Ú. v. ES L 201, 31.7.2002, s. 37).

by mohli ovplyvniť rizikový profil produktu s digitálnymi prvkami, akýkoľvek incident, ktorý má vplyv na bezpečnosť produktu s digitálnymi prvkami, ako aj situácie, ktoré takmer viedli k takémuto incidentu.

(75) Členské štáty by sa mali v súlade s vnútroštátnym právom snažiť v čo najväčšej miere riešiť výzvy, ktorým čelia výskumní pracovníci zaoberajúci sa zraniteľnosťami, vrátane ich možnej trestnej zodpovednosti. Keďže fyzické a právnické osoby, ktoré skúmajú zraniteľnosti, by v niektorých členských štátoch mohli byť vystavené trestnej a občianskoprávnej zodpovednosti, členským štátom sa odporúča prijať usmernenia, aby výskumní pracovníci v oblasti bezpečnosti informácií neboli za svoju činnosť stíhaní a dostali výnimku z občianskoprávnej zodpovednosti.

(76) Výrobcovia produktov s digitálnymi prvkami by mali zaviesť koordinované politiky zverejňovania informácií o zraniteľnosti s cieľom uľahčiť oznamovanie zraniteľností jednotlivcami alebo subjektmi, a to buď priamo výrobcovi alebo nepriamo a na požiadanie anonymne prostredníctvom jednotiek CSIRT určených za koordinátorov na účely koordinovaného zverejňovania informácií o zraniteľnosti v súlade s článkom 12 ods. 1 smernice (EÚ) 2022/2555. V politike výrobcov týkajúcej sa koordinovaného zverejňovania informácií o zraniteľnosti by sa mal špecifikovať štruktúrovaný proces, pomocou 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. Okrem toho by výrobcovia mali zvážiť aj zverejňovanie svojich bezpečnostných politík v strojovo čitateľnom formáte. Keďže 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 zraniteľnosti programy na stimulovanie oznamovania zraniteľností tým, že zaistia, aby jednotlivci alebo subjekty dostali uznanie a odmenu za svoje úsilie. Ide o tzv. „programy odmeňovania za nájdenie chýb“.

(77) Výrobcovia by na uľahčenie analýzy zraniteľnosti mali identifikovať a zdokumentovať komponenty obsiahnuté v produktoch s digitálnymi prvkami, a to aj vypracovaním zoznamu softvéru. Zoznam softvéru môže tým, ktorí vyrábajú, kupujú a prevádzkujú softvér, poskytnúť informácie pre lepšie pochopenie dodávateľského reťazca, čo má viacero prínosov, konkrétne pomáha výrobcom a používateľom sledovať známe novovzniknuté zraniteľnosti a kybernetickobezpečnostné riziká. Pre výrobcov má osobitný význam zabezpečiť, aby ich produkty s digitálnymi prvkami neobsahovali zraniteľné komponenty vyvinuté tretími stranami. Výrobcovia by nemali byť povinní zverejňovať zoznam softvéru.

(78) V rámci nových komplexných obchodných modelov spojených s online predajom môže subjekt pôsobiaci online poskytovať rôzne služby. Podľa povahy služieb poskytovaných v súvislosti s daným produktom s digitálnymi prvkami môže ten istý subjekt patriť do rôznych kategórií obchodných modelov alebo hospodárskych subjektov. Ak subjekt poskytuje len online sprostredkovateľské služby pre produkt s digitálnymi prvkami a je len prevádzkovateľom online trhoviska v zmysle vymedzenia v článku 3 bode 14 nariadenia (EÚ) 2023/988, nepovažuje sa za hospodársky subjekt v zmysle tohto nariadenia. Ak je ten istý subjekt prevádzkovateľom online trhoviska a koná aj ako hospodársky subjekt v zmysle vymedzenia v tomto nariadení, pokiaľ ide o predaj produktov s digitálnymi prvkami, mali by sa naň vzťahovať povinnosti podľa tohto nariadenia pre daný typ hospodárskeho subjektu. Ak napríklad prevádzkovateľ online trhoviska aj distribuuje produkt s digitálnymi prvkami, v súvislosti s predajom tohto produktu by sa považoval za distribútora. Podobne ak by daný subjekt predával svoje vlastné značkové produkty s digitálnymi prvkami, považoval by sa za výrobcu, a preto by musel spĺňať požiadavky uplatniteľné na výrobcov. Niektoré subjekty sa takisto môžu považovať za poskytovateľov logistických služieb v zmysle vymedzenia v článku 3 bode 11 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/1020 ([27]), ak takéto služby ponúkajú. Takéto prípady by sa mali posudzovať individuálne. Vzhľadom na významnú úlohu, ktorú online trhy zohrávajú pri umožňovaní elektronického obchodu, by sa mali usilovať o spoluprácu s orgánmi dohľadu nad trhom členských štátov s cieľom pomôcť zabezpečiť, aby produkty s digitálnymi prvkami zakúpené prostredníctvom online trhov boli v súlade s požiadavkami kybernetickej bezpečnosti stanovenými v tomto nariadení.

(79) 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 kybernetickej bezpečnosti stanovené v tomto nariadení premietnuté do podrobných

([27]) 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).

technických špecifikácií a ktoré sú prijaté v súlade s nariadením Európskeho parlamentu a Rady (EÚ) č. 1025/2012 ([28]). V uvedenom nariadení sa stanovuje postup týkajúci sa námietok voči harmonizovaným normám, keď tieto normy nespĺňajú v plnej miere požiadavky stanovené v tomto nariadení. Procesom normalizácie by sa malo zabezpečiť vyvážené zastúpenie záujmov a účinná účasť zainteresovaných strán občianskej spoločnosti vrátane organizácií spotrebiteľov. Na uľahčenie vývoja harmonizovaných noriem a vykonávanie tohto nariadenia, ako aj uľahčenie dodržiavania predpisov zo strany podnikov, najmä mikropodnikov a malých a stredných podnikov, ako aj podnikov s globálnym pôsobením by sa mali zohľadniť aj medzinárodné normy, ktoré sú v súlade s úrovňou ochrany kybernetickej bezpečnosti, ktorá je predmetom základných požiadaviek kybernetickej bezpečnosti stanovených v tomto nariadení.

(80) Včasné vypracovanie harmonizovaných noriem počas prechodného obdobia na uplatňovanie tohto nariadenia a ich dostupnosť pred dátumom začatia uplatňovania tohto nariadenia budú mimoriadne dôležité pre jeho účinné vykonávanie. To sa týka najmä dôležitých produktov s digitálnymi prvkami, ktoré patria do triedy I. Dostupnosť harmonizovaných noriem umožní výrobcom takýchto produktov vykonávať posudzovanie zhody postupom vnútornej kontroly, a môže preto zabrániť prekážkam a oneskoreniam v činnosti orgánov posudzovania zhody.

(81) Nariadením (EÚ) 2019/881 sa stanovuje dobrovoľný európsky rámec certifikácie kybernetickej bezpečnosti pre produkty informačných a komunikačných technológií, procesy informačných a komunikačných technológií a služby informačných a komunikačných technológií. Európske schémy certifikácie kybernetickej bezpečnosti poskytujú používateľom spoločný rámec dôvery na používanie produktov s digitálnymi prvkami, ktoré patria do rozsahu pôsobnosti tohto nariadenia. Týmto nariadením by sa mala následne 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 európskej schémy kybernetickej bezpečnosti podľa nariadenia (EÚ) 2019/881, ktorá bola Komisiou identifikovaná vo vykonávacom akte, sú v súlade so základnými požiadavkami kybernetickej bezpečnosti stanovenými v tomto nariadení, pokiaľ sa európsky certifikát kybernetickej bezpečnosti alebo vyhlásenie o zhode alebo ich časti na tieto požiadavky vzťahujú. Potreba nových európskych schém certifikácie kybernetickej bezpečnosti pre produkty s digitálnymi prvkami by sa mala posúdiť na základe tohto nariadenia, a to aj pri príprave priebežného pracovného programu Únie v súlade s nariadením (EÚ) 2019/881. Ak je potrebná nová schéma vzťahujúca sa na produkty s digitálnymi prvkami, a to aj s cieľom uľahčiť súlad s týmto nariadením, Komisia môže požiadať agentúru ENISA, aby pripravila kandidátske schémy v súlade s článkom 48 nariadenia (EÚ) 2019/881. Takéto budúce európske schémy certifikácie kybernetickej bezpečnosti vzťahujúce sa na produkty s digitálnymi prvkami by mali zohľadňovať základné požiadavky kybernetickej bezpečnosti a postupy posudzovania zhody stanovené v tomto nariadení a uľahčovať dodržanie súladu s týmto nariadením. V prípade európskych schém certifikácie kybernetickej bezpečnosti, ktoré nadobudnú účinnosť pred nadobudnutím účinnosti tohto nariadenia, môžu byť potrebné ďalšie špecifikácie podrobných aspektov uplatňovania predpokladu zhody. Komisia by mala mať právomoc prostredníctvom delegovaných aktov špecifikovať, za akých podmienok sa môžu európske schémy certifikácie kybernetickej bezpečnosti používať na preukázanie zhody so základnými požiadavkami kybernetickej bezpečnosti stanovenými v tomto nariadení. Okrem toho s cieľom predísť neprimeranému administratívnemu zaťaženiu by výrobcovia nemali mať povinnosť vykonať posúdenie zhody treťou stranou, ako to stanovuje toto nariadenie pri zodpovedajúcich požiadavkách, ak bol v rámci takýchto európskych schém certifikácie kybernetickej bezpečnosti vydaný certifikát kybernetickej bezpečnosti aspoň na úrovni záruky „významná“.

(82) Po nadobudnutí účinnosti vykonávacieho nariadenia (EÚ) 2024/482, ktoré sa týka produktov, ktoré patria do pôsobnosti tohto nariadenia, ako sú hardvérové bezpečnostné moduly a mikroprocesory, by Komisia mala mať možnosť prostredníctvom delegovaného aktu špecifikovať, ako sa v EUCC zabezpečí predpoklad zhody so základnými požiadavkami kybernetickej bezpečnosti stanovenými v tomto nariadení alebo s ich časťami. Okrem toho môže takýto delegovaný akt špecifikovať, akým spôsobom certifikát vydaný v rámci EUCC ruší povinnosť výrobcov dať vykonať posúdenie tretej strane, ako sa vyžaduje podľa tohto nariadenia pri zodpovedajúcich požiadavkách.

(83) Súčasný európsky normalizačný rámec, ktorý je založený na zásadách nového prístupu stanovených v uznesení Rady zo 7. mája 1985 o novom prístupe k technickej harmonizácii a normám a na nariadení (EÚ) č. 1025/2012, predstavuje štandardný rámec pre vypracovanie noriem, ktoré stanovujú predpoklad zhody s príslušnými základnými požiadavkami kybernetickej bezpečnosti stanovenými v tomto nariadení. Európske normy by mali byť trhovo orientované a mali by zohľadňovať verejný záujem, ako aj politické ciele jasne uvedené v žiadosti Komisie adresovanej jednej alebo viacerým európskym normalizačným organizáciám o vypracovanie harmonizovaných noriem v stanovenej lehote a mali by byť založené na konsenze. Ak však neexistujú príslušné odkazy na harmonizované normy, Komisia by mala môcť prijať vykonávacie akty stanovujúce spoločné špecifikácie pre

([28]) 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).

základné požiadavky kybernetickej bezpečnosti stanovené v tomto nariadení za predpokladu, že pritom náležite zohľadní úlohu a funkcie európskych normalizačných organizácií ako výnimočné núdzové riešenie na uľahčenie povinnosti výrobcu dosiahnuť súlad s uvedenými základnými požiadavkami kybernetickej bezpečnosti, keď je normalizačný proces zablokovaný alebo keď pri zavádzaní vhodných harmonizovaných noriem dochádza k oneskoreniam. Ak je takéto oneskorenie spôsobené technickou zložitosťou príslušnej normy, Komisia by to mala zvážiť pred tým, ako zváži stanovenie spoločných špecifikácií.

(84) S cieľom čo najefektívnejšie stanoviť spoločné špecifikácie, ktoré sa vzťahujú na základné požiadavky kybernetickej bezpečnosti stanovené v tomto nariadení, by Komisia mala do tohto procesu zapojiť príslušné zainteresované strany.

(85) „Primeraná lehota“ súvislosti s uverejnením odkazu na harmonizované normy v *Úradnom vestníku Európskej únie* v súlade s nariadením (EÚ) č. 1025/2012 je lehota, počas ktorej sa očakáva uverejnenie odkazu na normu, jej korigenda alebo jej zmeny v *Úradnom vestníku Európskej únie* a ktorá by nemala presiahnuť jeden rok po lehote na vypracovanie európskej normy stanovenej v súlade s nariadením (EÚ) č. 1025/2012.

(86) Na uľahčenie posudzovania zhody so základnými požiadavkami kybernetickej bezpečnosti 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.

(87) Uplatňovanie harmonizovaných noriem, spoločných špecifikácií alebo európskych schém certifikácie kybernetickej bezpečnosti prijatých podľa nariadenia (EÚ) 2019/881, v ktorých sa stanovuje predpoklad zhody v súvislosti so základnými požiadavkami kybernetickej bezpečnosti uplatniteľnými na produkty s digitálnymi prvkami, uľahčí posudzovanie zhody výrobcami. Ak sa výrobca rozhodne neuplatňovať takéto prostriedky na určité požiadavky, musí vo svojej technickej dokumentácii uviesť, akým iným spôsobom dosahuje súlad. Okrem toho by uplatňovanie harmonizovaných noriem, spoločných špecifikácií alebo európskych schém certifikácie kybernetickej bezpečnosti prijatých podľa nariadenia (EÚ) 2019/881, v ktorých sa stanovuje predpoklad zhody zo strany výrobcov, uľahčilo kontrolu súladu produktov s digitálnymi prvkami, ktorú vykonávajú orgány dohľadu nad trhom. Výrobcom produktov s digitálnymi prvkami sa preto odporúča, aby uplatňovali takéto harmonizované normy, spoločné špecifikácie alebo európske schémy certifikácie kybernetickej bezpečnosti.

(88) 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 kybernetickej bezpečnosti stanovenými v tomto nariadení a v relevantnom prípade iných relevantných harmonizačných právnych predpisoch Únie, ktoré sa vzťahujú na produkt s digitálnymi prvkami. Od výrobcov sa môže vypracovanie EÚ vyhlásenia o zhode vyžadovať aj v iných právnych aktoch 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 právnymi aktmi Únie. V záujme zníženia administratívnej záťaže hospodárskych subjektov by sa malo umožniť, aby toto jediné EÚ vyhlásenie o zhode tvoril súbor pozostávajúci z príslušných jednotlivých vyhlásení o zhode.

(89) Označenie CE, ktorým sa preukazuje zhoda výrobku, je viditeľným výsledkom celého postupu posudzovania zhody v širokom zmysle. Všeobecné zásady, ktorými sa riadi označenie CE, sú uvedené v nariadení Európskeho parlamentu a Rady (ES) č. 765/2008 ([29]). 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 súlad produktov s digitálnymi prvkami s požiadavkami stanovenými v tomto nariadení.

(90) S cieľom umožniť hospodárskym subjektom preukázať zhodu so základnými požiadavkami kybernetickej bezpečnosti 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

([29]) 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).

zhody. Rozhodnutím Európskeho parlamentu a Rady č. 768/2008/ES ([30]) sa stanovujú moduly pre postupy posudzovania zhody úmerne k úrovni možného rizika a úrovni požadovanej bezpečnosti. S cieľom zaistiť súlad medzi odvetviami a vyhnúť sa ad hoc variantom by postupy posudzovania zhody vhodné na overovanie zhody produktov s digitálnymi prvkami so základnými požiadavkami kybernetickej bezpečnosti stanovenými v tomto nariadení mali byť 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 s digitálnymi prvkami.

(91) Posudzovanie zhody produktov s digitálnymi prvkami, ktoré nie sú v tomto nariadení uvedené ako dôležité alebo kritické produkty s digitálnymi prvkami, môže výrobca vykonávať na vlastnú zodpovednosť postupom vnútornej kontroly podľa modulu A rozhodnutia č. 768/2008/ES v súlade s týmto nariadením. Platí to aj v prípadoch, keď sa výrobca rozhodne úplne alebo čiastočne neuplatňovať platnú harmonizovanú normu, spoločnú špecifikáciu alebo európsku schému certifikácie kybernetickej bezpečnosti. Výrobca si zachováva flexibilitu pri výbere prísnejšieho postupu posudzovania zhody za účasti tretej strany. Pri postupe posudzovania zhody na základe vnútornej kontroly výrobca na vlastnú zodpovednosť zabezpečuje a vyhlasuje, že produkt s digitálnymi prvkami a procesy výrobcu spĺňajú uplatniteľné základné požiadavky kybernetickej bezpečnosti stanovené v tomto nariadení. Ak dôležitý produkt s digitálnymi prvkami patrí do triedy I, vyžaduje sa dodatočné uistenie na preukázanie zhody so základnými požiadavkami kybernetickej bezpečnosti stanovenými v tomto nariadení. Výrobca by mal uplatniť harmonizované normy, spoločné špecifikácie alebo európske schémy certifikácie kybernetickej bezpečnosti prijaté 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 európske schémy certifikácie kybernetickej bezpečnosti, mal by podstúpiť posudzovanie zhody so zapojením tretej strany (podľa modulov B a C alebo modulu H). Pri zohľadnení administratívneho zaťaženia výrobcov a toho, 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 dôležitých produktov s digitálnymi prvkami zvolené postupy posudzovania zhody podľa modulov B a C alebo modulu H rozhodnutia č. 768/2008/ES. Výrobca, ktorý vykonáva posudzovanie zhody treťou stranou, si môže vybrať postup, ktorý najlepšie vyhovuje jeho procesom návrhu a výroby. Vzhľadom na ešte väčšie kybernetickobezpečnostné riziko spojené s používaním dôležitých produktov s digitálnymi prvkami, ktoré patria do triedy II by sa na posudzovaní zhody mala vždy zúčastňovať tretia strana, a to aj vtedy, keď je produkt úplne alebo čiastočne v súlade s harmonizovanými normami, spoločnými špecifikáciami alebo európskymi schémami certifikácie kybernetickej bezpečnosti. Výrobcovia dôležitých produktov s digitálnymi prvkami, ktoré sa považujú za slobodný softvér a softvér s otvoreným zdrojovým kódom, by mali mať možnosť uplatniť postup vnútornej kontroly podľa modulu A za predpokladu, že technickú dokumentáciu zverejnia.

(92) Kým pri vytváraní hmotných produktov s digitálnymi prvkami sa od výrobcov obvykle vyžaduje značné úsilie vo fáze 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 kybernetickej bezpečnosti stanovenými v tomto nariadení vo fáze návrhu, vývoja a výroby.

(93) Pokiaľ ide o mikropodniky a malé podniky, s cieľom zabezpečiť proporcionalitu je vhodné zmierniť administratívne náklady bez toho, aby bola dotknutá úroveň ochrany kybernetickej bezpečnosti produktov s digitálnymi prvkami, ktoré patria do rozsahu pôsobnosti tohto nariadenia, alebo rovnaké podmienky pre výrobcov. Preto je vhodné, aby Komisia vypracovala zjednodušený formulár technickej dokumentácie pre potreby mikropodnikov a malých podnikov. Zjednodušený formulár technickej dokumentácie prijatý Komisiou by mal zahŕňať všetky uplatniteľné prvky súvisiace s technickou dokumentáciou stanovenou v tomto nariadení a špecifikovať, ako môže mikropodnik alebo malý podnik v stručnej forme poskytnúť požadované prvky, ako je opis návrhu, vývoja a výroby produktu s digitálnymi prvkami. Formulár tak prispeje k zmierneniu administratívnej záťaže spojenej s dodržiavaním predpisov tým, že dotknutým podnikom poskytne právnu istotu, pokiaľ ide o rozsah a podrobnosti informácií, ktoré sa majú poskytnúť. Mikropodniky a malé podniky by mali mať možnosť rozhodnúť sa, že uplatniteľné prvky súvisiace s technickou dokumentáciou odovzdajú v neskrátenej forme a nepoužijú zjednodušený technický formulár, ktorý majú k dispozícii.

([30]) 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).

(94) V záujme podpory a ochrany inovácií je dôležité, aby sa osobitne zohľadnili záujmy výrobcov, ktorí sú mikropodnikmi alebo malými či strednými podnikmi, najmä mikropodnikov a malých podnikov vrátane startupov. Na tento účel by členské štáty mohli vyvinúť iniciatívy zamerané na výrobcov, ktorí sú mikropodnikmi alebo malými podnikmi, a to aj v oblasti odbornej prípravy, zvyšovania informovanosti, komunikácie, testovania a činností posudzovania zhody tretími stranami, ako aj vytvárania experimentálnych prostredí. Náklady na preklady súvisiace s povinnou dokumentáciou, ako je technická dokumentácia a informácie a návody pre používateľov požadované podľa tohto nariadenia, a komunikácia s orgánmi môžu predstavovať značné výdavky pre výrobcov, a to najmä pre malých výrobcov. Členské štáty by preto mali môcť zvážiť, aby jedným z jazykov, ktoré určia a akceptujú na účely príslušnej dokumentácie výrobcov a komunikácie s nimi, bol jazyk, ktorému vo všeobecnosti rozumie čo najväčší počet používateľov.

(95) S cieľom zabezpečiť bezproblémové uplatňovanie tohto nariadenia by členské štáty mali pred dátumom začatia jeho uplatňovania zabezpečiť, aby bol v Únii dostatočný počet notifikovaných osôb na výkon posudzovania zhody treťou stranou. Komisia by v tomto úsilí mala pomáhať členským štátom a iným relevantným subjektom, aby sa predišlo problémovým miestam a prekážkam pri vstupe výrobcov na trh. Cielené činnosti odbornej prípravy pod vedením členských štátov, prípadne aj s podporou Komisie, môžu prispieť k dostupnosti kvalifikovaných odborníkov, a to aj na podporu činností notifikovaných osôb podľa tohto nariadenia. Okrem toho by sa vzhľadom na náklady, ktoré môže predstavovať posudzovanie zhody treťou stranou, mali zvážiť iniciatívy financovania na úrovni Únie a na vnútroštátnej úrovni, ktorých cieľom je zmierniť takéto náklady pre mikropodniky a malé podniky.

(96) S cieľom zabezpečiť proporcionalitu by orgány posudzovania zhody mali pri určovaní poplatkov za postupy posudzovania zhody zohľadňovať osobitné záujmy a potreby mikropodnikov a malých a stredných podnikov vrátane startupov. Orgány posudzovania zhody by predovšetkým mali uplatňovať príslušný postup preskúmania a skúšky stanovené v tomto nariadení len v prípade potreby a podľa prístupu založeného na riziku.

(97) Cieľom experimentálnych regulačných prostredí by mala byť podpora inovácií a konkurencieschopnosti podnikov vytvorením kontrolovaných testovacích prostredí pred uvedením produktov s digitálnymi prvkami na trh. Experimentálne regulačné prostredia by mali prispieť k zlepšeniu právnej istoty pre všetkých aktérov, ktorí patria do rozsahu pôsobnosti tohto nariadenia, a uľahčiť a urýchliť prístup produktov s digitálnymi prvkami na trh Únie, najmä ak ich poskytujú mikropodniky a malé podniky vrátane startupov.

(98) 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.

(99) 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 mal byť doplnený systémom akreditácie 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.

(100) Orgány posudzovania zhody, ktoré boli akreditované a notifikované podľa právnych predpisov Únie, ktorými sa stanovujú požiadavky podobné požiadavkám stanoveným v tomto nariadení, ako napríklad orgán posudzovania zhody, ktorý bol notifikovaný pre európsku schému certifikácie kybernetickej bezpečnosti prijatú podľa nariadenia (EÚ) 2019/881 alebo notifikovaný podľa delegovaného nariadenia (EÚ) 2022/30, by sa mali znovu posúdiť a notifikovať podľa tohto nariadenia. Príslušné orgány však môžu vymedziť synergie akýchkoľvek duplicitných požiadaviek s cieľom zabrániť zbytočnej finančnej a administratívnej záťaži a zabezpečiť bezproblémový a včasný proces notifikácie.

(101) Transparentnú akreditáciu stanovenú v nariadení (ES) č. 765/2008, ktorou sa zabezpečuje potrebná úroveň dôvery v certifikáty zhody, by mali vnútroštátne orgány verejnej moci 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.

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

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

(104) Keďže notifikované osoby môžu ponúkať svoje služby v celej Únii, je vhodné poskytnúť iným členským štátom a Komisii možnosť vzniesť v súvislosti s notifikovanými osobami námietky. Je preto dôležité stanoviť lehotu, počas ktorej bude možné objasniť všetky pochybnosti alebo obavy, pokiaľ ide o spôsobilosť orgánov posudzovania zhody skôr, než začnú pôsobiť ako notifikované osoby.

(105) 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 primeranou koordináciou a spoluprácou medzi notifikovanými osobami.

(106) Dohľad nad trhom predstavuje nevyhnutný nástroj zaisťovania správneho a jednotného uplatňovania práva Únie. Je preto vhodné zaviesť právny rámec, v ktorom sa môže dohľad nad trhom vykonávať primeraným spôsobom. Na produkty s digitálnymi prvkami, ktoré patria do pôsobnosti tohto nariadenia, sa uplatňujú pravidlá pre dohľad nad trhom Únie a kontrolu produktov vstupujúcich na trh Únie stanovené v nariadení (EÚ) 2019/1020.

(107) Orgán dohľadu nad trhom vykonáva v súlade s nariadením (EÚ) 2019/1020 dohľad nad trhom na území členského štátu, ktorý ho vymenuje. Toto nariadenie by členským štátom nemalo brániť vo výbere príslušných orgánov na vykonávanie úloh dohľadu nad trhom. Každý členský štát by mal na svojom území určiť jeden orgán alebo viac orgánov dohľadu nad trhom. Členské štáty by mali mať možnosť určiť ktorýkoľvek existujúci alebo nový orgán, aby konal ako orgán dohľadu nad trhom, a to vrátane príslušných orgánov určených alebo zriadených podľa článku 8 smernice (EÚ) 2022/2555, vnútroštátnych orgánov pre certifikáciu kybernetickej bezpečnosti určených podľa článku 58 nariadenia (EÚ) 2019/881 alebo orgánov dohľadu nad trhom určených na účely smernice 2014/53/EÚ. Hospodárske subjekty by mali v plnej miere spolupracovať s orgánmi dohľadu nad trhom a s ďalšími príslušnými orgánmi. Každý členský štát by mal o svojich orgánoch dohľadu nad trhom a oblasti pôsobnosti každého z týchto orgánov informovať Komisiu a ostatné členské štáty a mal by zaistiť potrebné zdroje a zručnosti na vykonávanie úloh dohľadu nad trhom v súvislosti s týmto nariadením. Podľa článku 10 ods. 2 a 3 nariadenia (EÚ) 2019/1020 by mal každý členský štát určiť jednotný úrad pre spoluprácu zodpovedný okrem iného za zastupovanie koordinovanej pozície orgánov dohľadu nad trhom a pomoc v rámci spolupráce orgánov dohľadu nad trhom v rôznych členských štátoch.

(108) Na jednotné uplatňovanie tohto nariadenia by sa podľa článku 30 ods. 2 nariadenia (EÚ) 2019/1020 mala zriadiť špecializovaná skupina ADCO v oblasti kybernetickej odolnosti produktov s digitálnymi prvkami. Skupinu ADCO by mali tvoriť zástupcovia určených orgánov dohľadu nad trhom a v relevantnom prípade zástupcovia jednotných úradov pre spoluprácu. Komisia by mala podporovať a podnecovať spoluprácu medzi orgánmi dohľadu nad trhom prostredníctvom siete Únie pre súlad produktov zriadenej podľa článku 29 nariadenia (EÚ) 2019/1020, ktorá pozostáva zo zástupcov každého členského štátu vrátane zástupcu každého jednotného úradu pre spoluprácu uvedeného v článku 10 uvedeného nariadenia a prípadného národného experta, predsedov skupín ADCO a zástupcov z Komisie. Komisia by sa mala zúčastňovať na zasadnutiach siete Únie pre súlad produktov, jej podskupín a skupiny ADCO. Mala by takisto pomáhať skupine ADCO prostredníctvom výkonného sekretariátu, ktorý poskytuje technickú a logistickú podporu. Skupina ADCO môže takisto prizvať na účasť nezávislých odborníkov, a na spoluprácu s inými skupinami ADCO, napríklad tou, ktorá bola zriadená podľa smernice 2014/53/EÚ.

(109) Orgány dohľadu nad trhom by mali prostredníctvom skupiny ADCO zriadenej podľa tohto nariadenia úzko spolupracovať a mali by mať možnosť vypracovať usmerňovacie dokumenty na uľahčenie činností dohľadu nad trhom na vnútroštátnej úrovni, napríklad vypracovaním najlepších postupov a ukazovateľov na účinnú kontrolu súladu produktov s digitálnymi prvkami s týmto nariadením.

(110) 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.

(111) V určitých prípadoch môže produkt s digitálnymi prvkami, ktorý je v súlade s týmto nariadením, napriek tomu predstavovať významné kybernetickobezpečnostné riziko alebo riziko pre zdravie a bezpečnosť osôb, dodržiavanie povinností podľa práva Únie alebo vnútroštátneho práva, ktorých cieľom je ochrana základných práv, pre dostupnosť, pravosť, integritu alebo dôvernosť služieb ponúkaných prostredníctvom elektronického informačného systému základnými subjektmi uvedenými v článku 3 ods. 1 smernice (EÚ) 2022/2555 alebo iné aspekty ochrany verejného záujmu. Preto je potrebné stanoviť pravidlá, ktorými sa zaistí zmiernenie týchto rizík. Preto by orgány dohľadu nad trhom mali prijať opatrenia, ktorými by sa od hospodárskeho subjektu v závislosti od rizika vyžadovalo zaistenie toho, že produkt už nebude predstavovať uvedené riziko, alebo stiahnutie produktu od používateľa alebo z trhu. Keď orgán dohľadu nad trhom takto obmedzí alebo zakáže voľný pohyb produktu s digitálnymi prvkami, 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 s digitálnymi prvkami 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 subjektom. Ak sa opatrenie považuje za opodstatnené, Komisia by mala tiež zvážiť, či má prijať návrhy na revíziu príslušných právnych predpisov Únie.

(112) 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 sú v súlade s týmto nariadením, ale predstavujú iné významné riziká, napríklad riziká pre zdravie alebo bezpečnosť osôb, pre dodržiavanie povinností podľa práva Únie alebo vnútroštátneho práva, ktoré majú chrániť základné práva, alebo pre dostupnosť, pravosť, integritu alebo dôvernosť služieb poskytovaných pomocou elektronického informačného systému základnými subjektmi uvedenými v článku 3 ods. 1 smernice (EÚ) 2022/2555, by Komisia mala mať možnosť požiadať agentúru ENISA o vykonanie hodnotenia. Na základe tohto hodnotenia by Komisia mala mať možnosť prostredníctvom vykonávacích aktov prijať nápravné alebo reštriktívne opatrenia na úrovni Únie, ako aj požiadať o stiahnutie dotknutých produktov s digitálnymi prvkami z trhu alebo od používateľov v primeranej lehote úmernej povahe rizika. Komisia by mala mať možnosť využiť takýto zásah len za mimoriadnych okolností, ktoré opodstatňujú okamžitý zásah s cieľom zachovať riadne fungovanie vnútorného trhu, a len vtedy, ak orgány dohľadu nad trhom neprijali na nápravu situácie žiadne účinné opatrenia. Takýmito mimoriadnymi okolnosťami môžu byť núdzové situácie, keď napríklad výrobca vo veľkej miere sprístupňuje vo viacerých členských štátoch nevyhovujúci produkt s digitálnymi prvkami, ktorý používajú aj subjekty v kľúčových odvetviach, ktoré patria do rozsahu pôsobnosti smernice (EÚ) 2022/2555, i keď obsahuje známe zraniteľnosti, ktoré zneužívajú škodlivé subjekty a na ktoré výrobca neposkytuje dostupné záplaty. Komisia by mala mať možnosť v takýchto núdzových situáciách zasiahnuť len počas trvania mimoriadnych okolností a ak pretrváva nesúlad s týmto nariadením alebo prezentované významné riziká.

(113) Ak 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.

(114) 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 s digitálnymi prvkami sa často zisťuje, že predstavujú kybernetickobezpečnostné riziká. Okrem toho by orgány dohľadu nad trhom pri určovaní kategórií produktov, ktoré majú podliehať kontrolným akciám, mali zohľadniť aj okolnosti týkajúce sa netechnických rizikových faktorov. Na tento účel by orgány dohľadu nad trhom mali mať možnosť zohľadniť výsledky koordinovaného posúdenia bezpečnostných rizík kritických dodávateľských reťazcov na úrovni Únie, ktoré sa vykonáva v súlade s článkom 22 smernice (EÚ) 2022/2555, a to vrátane okolností týkajúcich sa netechnických rizikových faktorov. Agentúra ENISA by mala orgánom dohľadu nad trhom predložiť návrhy kategórií produktov s digitálnymi prvkami, v prípade ktorých by sa mohli organizovať kontrolné akcie okrem iného na základe prijatých oznámení o zraniteľnostiach produktov a incidentoch.

(115) Vzhľadom na svoje odborné znalosti a mandát by agentúra ENISA mala byť schopná podporovať proces vykonávania tohto nariadenia. Agentúra ENISA by najmä mala mať možnosť 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 kontrolné akcie. Za mimoriadnych okolností by agentúra ENISA mala mať možnosť na žiadosť Komisie vykonať hodnotenia konkrétnych produktov s digitálnymi prvkami, ktoré predstavujú významné kybernetickobezpečnostné riziko, keď sa vyžaduje okamžitý zásah v záujme zachovania riadneho fungovania vnútorného trhu.

(116) Týmto nariadením sa agentúra ENISA poveruje vykonávaním určitých úloh, ktoré si vyžadujú primerané zdroje, pokiaľ ide o odborné znalosti aj ľudské zdroje, aby mohla tieto úlohy účinne vykonávať. Komisia pri príprave návrhu všeobecného rozpočtu Únie navrhne potrebné rozpočtové zdroje pre plán pracovných miest agentúry ENISA v súlade s postupom stanoveným v článku 29 nariadenia (EÚ) 2019/881. Počas tohto procesu Komisia zváži celkové zdroje agentúry ENISA, ktoré jej umožnia plniť svoje úlohy vrátane tých, ktorými bola agentúra ENISA poverená podľa tohto nariadenia.

(117) S cieľom zabezpečiť, aby sa regulačný rámec mohol v prípade potreby upraviť, by sa mala na Komisiu delegovať právomoc prijímať akty v súlade s článkom 290 Zmluvy o fungovaní Európskej únie (ďalej len „ZFEÚ“), pokiaľ ide o aktualizáciu prílohy k tomuto nariadeniu so zoznamom dôležitých produktov s digitálnymi prvkami. 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 kritických produktov s digitálnymi prvkami stanovených v prílohe k tomuto nariadeniu v rámci európskej schémy certifikácie kybernetickej bezpečnosti, ako aj pokiaľ ide o aktualizáciu zoznamu kritických produktov s digitálnymi prvkami založenými na kritériách kritickosti stanovených v tomto nariadení a na spresnenie európskych schém certifikácie kybernetickej bezpečnosti prijatých podľa nariadenia (EÚ) 2019/881, ktoré možno použiť na preukázanie zhody so základnými požiadavkami kybernetickej bezpečnosti alebo ich časťami stanovenými v prílohe k tomuto nariadeniu. Na Komisiu by sa mala delegovať aj právomoc prijímať akty s cieľom stanoviť minimálne obdobie podpory pre konkrétne kategórie produktov, ak z údajov z dohľadu nad trhom vyplývajú neprimerané obdobia podpory, ako aj stanoviť podmienky uplatňovania dôvodov súvisiacich s kybernetickou bezpečnosťou v súvislosti s odkladom rozosielania oznámení o aktívne zneužívaných zraniteľnostiach. Okrem toho by sa mala na Komisiu delegovať právomoc prijímať akty s cieľom stanoviť dobrovoľné programy osvedčovania bezpečnosti na posudzovanie zhody produktov s digitálnymi prvkami, ktoré sa považujú za slobodný softvér a softvér s otvoreným zdrojovým kódom, so všetkými alebo určitými základnými požiadavkami kybernetickej bezpečnosti alebo inými povinnosťami stanovenými v tomto nariadení, ako aj špecifikovať minimálny obsah EÚ vyhlásenia o zhode a doplniť prvky, 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 ([31]). 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. Právomoc prijímať delegované akty podľa tohto nariadenia by sa Komisii mala udeliť na obdobie piatich rokov od 10. decembra 2024. Najneskôr deväť mesiacov pred uplynutím tohto päťročného obdobia by Komisia mala vypracovať správu týkajúcu sa delegovania právomoci. Delegovanie právomoci by sa malo automaticky predĺžiť o rovnako dlhé obdobia, pokiaľ Európsky parlament alebo Rada nevznesú voči takémuto predĺženiu námietku najneskôr tri mesiace pred koncom každého obdobia.

(118) S cieľom zabezpečiť jednotné podmienky vykonávania tohto nariadenia by sa mali na Komisiu preniesť vykonávacie právomoci s cieľom spresniť technický opis kategórií dôležitých produktov s digitálnymi prvkami stanovený v prílohe k tomuto nariadeniu, špecifikovať formát a prvky zoznamu softvéru, bližšie špecifikovať formát a postup oznamovania aktívne zneužívaných zraniteľností a závažných incidentov, ktoré majú vplyv na bezpečnosť produktov s digitálnymi prvkami predložených výrobcami, stanoviť spoločné špecifikácie zahŕňajúce technické požiadavky, ktoré poskytujú prostriedky na splnenie základných požiadaviek kybernetickej bezpečnosti stanovených v prílohe k tomuto nariadeniu, stanoviť technické špecifikácie pre štítky, piktogramy alebo akékoľvek iné značky týkajúce sa bezpečnosti produktov s digitálnymi prvkami, obdobia ich podpory a mechanizmov na propagáciu ich používania a na zvýšenie informovanosti verejnosti o bezpečnosti produktov s digitálnymi prvkami, špecifikovať zjednodušený dokumentačný formulár zameraný na potreby mikropodnikov a malých podnikov, a rozhodnúť

([31]) Ú. v. EÚ L 123, 12.5.2016, s. 1.

o nápravných alebo reštriktívnych opatreniach na úrovni Únie za výnimočných okolností, ktoré opodstatňujú okamžitý zásah na zachovanie riadneho fungovania vnútorného trhu. Uvedené právomoci by sa mali vykonávať v súlade s nariadením Európskeho parlamentu a Rady (EÚ) č. 182/2011 ([32]).

(119) 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.

(120) V záujme zabezpečenia účinného presadzovania povinností stanovených v tomto nariadení by každý orgán dohľadu nad trhom mal mať právomoc ukladať správne pokuty alebo požiadať o ich uloženie. Mali by sa preto zaviesť maximálne úrovne správnych pokút, ktoré sa majú stanoviť vo vnútroštátnom práve 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 je výrobca mikropodnikom alebo malým či stredným podnikom, prípadne startupom, a či už tomu istému hospodárskemu subjektu uložili tie isté alebo iné orgány dohľadu nad trhom správne poplatky za podobné porušenie. Takéto okolnosti by mohli byť buď priťažujúce 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 poľahčujúce, 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. Keďže správne pokuty sa nevzťahujú na mikropodniky alebo malé podniky za nedodržanie 24-hodinovej lehoty na včasné varovné oznámenia o aktívne zneužívaných zraniteľnostiach alebo závažných incidentoch, ktoré majú vplyv na bezpečnosť produktu s digitálnymi prvkami, ani na správcov softvéru s otvoreným zdrojovým kódom za akékoľvek porušenie tohto nariadenia, a s výhradou zásady, že sankcie by mali byť účinné, primerané a odrádzajúce, by členské štáty týmto subjektom nemali ukladať iné druhy peňažných sankcií.

(121) Ak sa správne pokuty ukladajú osobe, ktorá nie je 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.

(122) Členské štáty by mali s prihliadnutím na vnútroštátne okolnosti preskúmať možnosť použiť príjmy z pokút stanovených v tomto nariadení alebo ich finančný ekvivalent na podporu politík kybernetickej bezpečnosti a zvýšenie úrovne kybernetickej bezpečnosti v Únii okrem iného zvýšením počtu kvalifikovaných odborníkov v oblasti kybernetickej bezpečnosti, posilnením budovania kapacít mikropodnikov a malých a stredných podnikov a zlepšením informovanosti verejnosti o kybernetických hrozbách.

(123) Vo svojich vzťahoch s tretími krajinami sa Únia snaží podporovať medzinárodný obchod s regulovanými produktmi. Na uľahčenie obchodu sa môže uplatniť široká paleta opatrení vrátane viacerých právnych nástrojov, ako sú dvojstranné (medzivládne) dohody o vzájomnom uznávaní posudzovania zhody a označovania regulovaných produktov. Dohody o vzájomnom uznávaní sa uzatvárajú medzi Úniou a tretími krajinami, ktoré sú na porovnateľnej úrovni technického vývoja a majú kompatibilný prístup k posudzovaniu 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 uzavreté s niekoľkými tretími krajinami. Tieto dohody o vzájomnom uznávaní sú uzatvorené v mnohých špecifických odvetviach, ktoré sa môžu v jednotlivých tretích krajinách 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 uzatvárať dohody o vzájomnom uznávaní posúdení zhody pre produkty, na ktoré sa vzťahuje toto nariadenie. Dôležitá je aj spolupráca s partnerskými tretími krajinami s cieľom celosvetovo posilniť kybernetickú odolnosť, keďže z dlhodobého hľadiska to prispeje k posilnenému rámcu kybernetickej bezpečnosti v Únii aj mimo nej.

([32]) 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, ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(124) V súvislosti s povinnosťami uloženými hospodárskym subjektom podľa tohto nariadenia by spotrebitelia mali mať právo presadzovať svoje práva prostredníctvom žalôb v zastúpení v súlade so smernicou Európskeho parlamentu a Rady (EÚ) 2020/1828 ([33]). Na tento účel by sa v tomto nariadení malo stanoviť, že smernica (EÚ) 2020/1828 sa uplatňuje na žaloby v zastúpení týkajúce sa porušení tohto nariadenia, ktoré poškodzujú alebo môžu poškodiť kolektívne záujmy spotrebiteľov. Preto by sa mala zodpovedajúcim spôsobom zmeniť príloha I k uvedenej smernici. Úlohou členských štátov je zabezpečiť, aby sa tieto zmeny zohľadnili v transpozičných opatreniach prijatých v súlade s uvedenou smernicou, aj keď prijatie vnútroštátnych transpozičných opatrení v tejto súvislosti nie je podmienkou uplatniteľnosti uvedenej smernice na uvedené žaloby v zastúpení. Uplatniteľnosť uvedenej smernice na žaloby v zastúpení podané proti porušeniu ustanovení tohto nariadenia hospodárskymi subjektmi, ktoré poškodzujú alebo by mohli poškodiť kolektívne záujmy spotrebiteľov, by mala začať plynúť od 11. decembra 2027.

(125) Komisia by mala toto nariadenie pravidelne hodnotiť a preskúmavať po konzultácii s príslušnými zainteresovanými stranami najmä s cieľom určiť, či ho treba zmeniť na základe zmien spoločenských, politických, technologických alebo trhových podmienok. Týmto nariadením sa uľahčí dodržiavanie povinností v oblasti bezpečnosti dodávateľského reťazca pre subjekty, ktoré patria do rozsahu pôsobnosti nariadenia (EÚ) 2022/2554 a smernice (EÚ) 2022/2555 a ktoré používajú produkty s digitálnymi prvkami. V rámci tohto pravidelného preskúmania by Komisia mala vyhodnotiť kombinované účinky rámca kybernetickej bezpečnosti Únie.

(126) Hospodárskym subjektom by sa mal poskytnúť dostatočný čas prispôsobiť sa požiadavkám stanoveným v tomto nariadení. Toto nariadenie by sa malo uplatňovať od 11. decembra 2027 s výnimkou oznamovacích povinností týkajúcich sa aktívne zneužívaných zraniteľností a závažných incidentov, ktoré majú vplyv na bezpečnosť produktov s digitálnymi prvkami, ktoré by sa mali uplatňovať od 11. septembra 2026 a ustanovení o notifikácii orgánov posudzovania zhody, ktoré by sa mali uplatňovať od 11. júna 2026.

(127) Pri vykonávaní tohto nariadenia je dôležité poskytnúť podporu mikropodnikom a malým a stredným podnikom vrátane startupov a minimalizovať riziká pre vykonávanie vyplývajúce z nedostatku poznatkov a odborných znalostí na trhu, a to aj s cieľom uľahčiť výrobcom plnenie ich povinností stanovených v tomto nariadení. Program Digitálna Európa a iné príslušné programy Únie poskytujú finančnú a technickú podporu, ktorá týmto podnikom umožňuje prispievať k rastu hospodárstva Únie a k posilneniu spoločnej úrovne kybernetickej bezpečnosti v Únii. Európske centrum kompetencií v oblasti kybernetickej bezpečnosti a národné koordinačné centrá, ako aj európske centrá digitálnych inovácií zriadené Komisiou a členskými štátmi na úrovni Únie alebo na vnútroštátnej úrovni by mohli podporovať aj podniky a organizácie verejného sektora a mohli by prispieť k vykonávaniu tohto nariadenia. V rámci svojich príslušných úloh a oblastí pôsobnosti by mohli poskytovať technickú a vedeckú podporu mikropodnikom a malým a stredným podnikom, napríklad pri testovaní a posudzovaní zhody tretími stranami. Mohli by tiež podporiť zavádzanie nástrojov na uľahčenie vykonávania tohto nariadenia.

(128) Okrem toho by členské štáty mali zvážiť prijatie doplnkových opatrení zameraných na poskytovanie usmernení a podpory mikropodnikom a malým a stredným podnikom, ako je zriaďovanie experimentálnych regulačných prostredí a osobitných komunikačných kanálov. S cieľom posilniť úroveň kybernetickej bezpečnosti v Únii môžu členské štáty zvážiť aj poskytnutie podpory na rozvoj kapacít a zručností súvisiacich s kybernetickou bezpečnosťou produktov s digitálnymi prvkami, zlepšenie kybernetickej odolnosti hospodárskych subjektov, najmä mikropodnikov a malých a stredných podnikov, a zvýšenie informovanosti verejnosti o kybernetickej bezpečnosti produktov s digitálnymi prvkami.

(129) Keďže cieľ tohto nariadenia nie je možné uspokojivo dosiahnuť na úrovni 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 tohto cieľa.

(130) V súlade s článkom 42 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 ([34]) sa konzultovalo s európskym dozorným úradníkom pre ochranu údajov, ktorý vydal 9. novembra 2022 ([35]) svoje stanovisko,

([33]) Smernica Európskeho parlamentu a Rady (EÚ) 2020/1828 z 25. novembra 2020 o žalobách v zastúpení na ochranu kolektívnych záujmov spotrebiteľov a o zrušení smernice 2009/22/ES (Ú. v. EÚ L 409, 4.12.2020, s. 1).

([34]) 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).

([35]) Ú. v. EÚ C 452, 29.11.2022, s. 23.

PRIJALI TOTO NARIADENIE:

KAPITOLA I

VŠEOBECNÉ USTANOVENIA

Článok 1

Predmet úpravy

V tomto nariadení sa stanovujú:

a) pravidlá sprístupňovania produktov s digitálnymi prvkami na trhu s cieľom zaistiť ich kybernetickú bezpečnosť;

b) základné požiadavky kybernetickej bezpečnosti 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 kybernetickej bezpečnosti na procesy riešenia zraniteľností zavedené výrobcami s cieľom zaistiť kybernetickú bezpečnosť produktov s digitálnymi prvkami počas predpokladaného obdobia používania produktov, a povinnosti hospodárskych subjektov v súvislosti s týmito procesmi;

d) pravidlá dohľadu nad trhom vrátane monitorovania a presadzovanie pravidiel a požiadaviek uvedených v tomto článku.

Článok 2

Rozsah pôsobnosti

1. Toto nariadenie sa uplatňuje na produkty s digitálnymi prvkami sprístupnenými na trhu, ktorých zamýšľaný účel 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 právne 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. Toto nariadenie sa nevzťahuje na vybavenie, ktoré patrí do rozsahu pôsobnosti smernice Európskeho parlamentu a Rady 2014/90/EÚ ([36]).

5. 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 kybernetickej bezpečnosti stanovené 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) sa sektorovými predpismi dosahuje rovnaká alebo vyššia úroveň ochrany, ako je úroveň stanovená v tomto nariadení.

Komisia je v súlade s článkom 61 splnomocnená prijímať delegované akty s cieľom doplniť toto nariadenie stanovením toho, či je takéto obmedzenie alebo vylúčenie potrebné, dotknutých produktov a pravidiel, ako aj prípadného rozsahu obmedzenia.

([36]) Smernica Európskeho parlamentu a Rady 2014/90/EÚ z 23. júla 2014 o vybavení námorných lodí a o zrušení smernice Rady 96/98/ES (Ú. v. EÚ L 257, 28.8.2014, s. 146).

6. Toto nariadenie sa nevzťahuje na náhradné diely, ktoré sa sprístupňujú na trhu s cieľom nahradiť identické komponenty v produktoch s digitálnymi prvkami a ktoré sa vyrábajú podľa rovnakých špecifikácií ako komponenty, ktoré majú nahradiť.

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

8. Povinnosti stanovené v tomto nariadení nezahŕňajú poskytovanie informácií, ktorých zverejnenie by bolo v rozpore so základnými záujmami členských štátov v oblasti národnej bezpečnosti, verejnej bezpečnosti alebo obrany.

Článok 3

Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňuje toto vymedzenie pojmov:

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

2. „spracovanie údajov na diaľku“ je 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. „kybernetická bezpečnosť“ je kybernetická bezpečnosť v zmysle vymedzenia v článku 2 bode 1 nariadenia (EÚ) 2019/881;

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

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

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

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

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

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

10. „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;

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

12. „hospodársky subjekt“ je výrobca, splnomocnený zástupca, dovozca, distribútor alebo iná fyzická alebo právnická osoba, ktorá podlieha povinnostiam súvisiacim s výrobou produktov s digitálnymi prvkami alebo so sprístupňovaním produktov s digitálnymi prvkami na trhu v súlade s týmto nariadením;

13. „výrobca“ je 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, speňaženie alebo bezodplatne;

14. „správca softvéru s otvoreným zdrojovým kódom“ je právnická osoba iná ako výrobca, ktorej účelom alebo cieľom je systematicky a trvalo podporovať vývoj špecifických produktov s digitálnymi prvkami považovaných za slobodný softvér a softvér s otvoreným zdrojovým kódom a určených na obchodné činnosti, a ktorá zabezpečuje životaschopnosť týchto produktov;

15. „splnomocnený zástupca“ je fyzická alebo právnická osoba usadená v Únii, ktorej bolo doručené písomné splnomocnenie od výrobcu konať v jeho mene v súvislosti s konkrétnymi úlohami;

16. „dovozca“ je 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;

17. „distribútor“ je 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;

18. „spotrebiteľ“ je fyzická osoba, ktorá koná na účely, ktoré nesúvisia s jej obchodnou činnosťou, podnikaním, remeslom alebo povolaním;

19. „mikropodniky“, „malé podniky“ a „stredné podniky“ sú mikropodniky, malé a stredné podniky v zmysle vymedzenia v prílohe k odporúčaniu 2003/361/ES;

20. „obdobie podpory“ je obdobie, počas ktorého je výrobca povinný zabezpečiť účinné riešenie zraniteľností produktu s digitálnymi prvkami v súlade so základnými požiadavkami kybernetickej bezpečnosti stanovenými v časti II prílohy I;

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

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

23. „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;

24. „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;

25. „odôvodnene predvídateľné nesprávne použitie“ je použitie produktu s digitálnymi prvkami spôsobom, ktorý nie je v súlade so zamýšľaným účelom, ale ktorý môže vyplynúť z odôvodnene predvídateľného ľudského správania alebo interakcie s inými systémami;

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

27. „posudzovanie zhody“ je postup, ktorým sa overuje, či boli splnené základné požiadavky kybernetickej bezpečnosti stanovené v prílohe I;

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

29. „notifikovaná osoba“ je orgán posudzovania zhody určený v súlade s článkom 43 a inými relevantnými harmonizačnými právnymi predpismi Únie;

30. „podstatná úprava“ je zmena produktu s digitálnymi prvkami po jeho uvedení na trh, ktorá ovplyvňuje súlad produktu s digitálnymi prvkami so základnými požiadavkami kybernetickej bezpečnosti stanovenými v časti I prílohy I alebo ktorá vedie k úprave zamýšľaného účelu, pre ktoré bol produkt s digitálnymi prvkami posudzovaný;

31. „označenie CE“ je označenie, ktorým výrobca vyjadruje, že produkt s digitálnymi prvkami a procesy zavedené výrobcom sú v súlade so základnými požiadavkami kybernetickej bezpečnosti stanovenými v prílohe I a s inými uplatniteľnými harmonizačnými právnymi predpismi Únie, ktoré stanovujú umiestnenie tohto označenia;

32. „harmonizačné právne predpisy Únie“ sú právne predpisy Únie uvedené v prílohe I k nariadeniu (EÚ) 2019/1020 a akékoľvek iné právne predpisy Únie, ktorými sa harmonizujú podmienky uvádzania výrobkov, na ktoré sa uvedené nariadenie vzťahuje, na trh;

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

34. „medzinárodná norma“ je medzinárodná norma v zmysle vymedzenia v článku 2 ods. 1 písm. a) nariadenia (EÚ) č. 1025/2012;

35. „európska norma“ je európska norma v zmysle vymedzenia v článku 2 bode 1 písm. b) nariadenia (EÚ) č. 1025/2012;

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

37. „kybernetickobezpečnostné riziko“ je potenciál straty alebo narušenia v dôsledku incidentu a má byť vyjadrené ako kombinácia rozsahu takejto straty alebo narušenia a pravdepodobnosti výskytu incidentu;

38. „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;

39. „zoznam softvéru“ je formálny záznam obsahujúci podrobnosti a vzťahy v rámci dodávateľského reťazca komponentov zahrnutých v softvérových prvkoch produktu s digitálnymi prvkami;

40. „zraniteľnosť“ je slabá stránka, náchylnosť alebo chyba produktu s digitálnymi prvkami, ktorú môže zneužiť kybernetická hrozba;

41. „zneužiteľná zraniteľnosť“ je zraniteľnosť, ktorú môže nepriateľský subjekt účinne využiť za reálnych prevádzkových podmienok;

42. „aktívne zneužívaná zraniteľnosť“ je zraniteľnosť, v prípade ktorej existuje spoľahlivý dôkaz, že škodlivý subjekt ju zneužil v systéme bez povolenia vlastníka systému;

43. „incident“ je incident v zmysle vymedzenia v článku 6 bode 6 smernice (EÚ) 2022/2555;

44. „incident, ktorý ma vplyv na bezpečnosť produktu s digitálnymi prvkami“ je incident, ktorý negatívne ovplyvňuje alebo môže negatívne ovplyvniť schopnosť produktu s digitálnymi prvkami chrániť dostupnosť, pravosť, integritu alebo dôvernosť údajov alebo funkcií;

45. „udalosť odvrátená v poslednej chvíli“ je udalosť odvrátená v poslednej chvíli v zmysle vymedzenia v článku 6 bode 5 smernice (EÚ) 2022/2555;

46. „kybernetická hrozba“ je kybernetická hrozba v zmysle vymedzenia v článku 2 bode 8 nariadenia (EÚ) 2019/881;

47. „osobné údaje“ sú osobné údaje v zmysle vymedzenia v článku 4 bode 1 nariadenia (EÚ) 2016/679;

48. „slobodný softvér a softvér s otvoreným zdrojovým kódom“ je softvér, ktorého zdrojový kód je voľne dostupný a ktorý je vytvorený na základe bezplatnej a otvorenej licencie, ktorá udeľuje všetky práva na voľný prístup k nemu, jeho použiteľnosť, modifikovateľnosť a redistribúciu;

49. „spätné prevzatie“ je spätné prevzatie v zmysle vymedzenia v článku 3 bode 22 nariadenia (EÚ) 2019/1020;

50. „stiahnutie“ je stiahnutie v zmysle vymedzenia v článku 3 bode 23 nariadenia (EÚ) 2019/1020;

51. „jednotka CSIRT určená za koordinátora“ je jednotka CSIRT určená za koordinátora podľa článku 12 ods. 1 smernice (EÚ) 2022/2555.

Článok 4

Voľný pohyb

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

2. Na obchodných veľtrhoch, výstavách a predvádzaniach alebo podobných podujatiach nesmú členské štáty brániť ukážkam alebo používaniu produktu s digitálnymi prvkami, ktorý nie je v súlade s týmto nariadením, vrátane jeho prototypov, za predpokladu, že produkt je prezentovaný s viditeľným označením, ktoré jasne uvádza, že nie je v súlade s týmto nariadením a že nesmie byť sprístupnený na trhu, kým sa nedosiahne súlad.

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

4. Odsek 3 sa nevzťahuje na bezpečnostné komponenty uvedené v harmonizačných právnych predpisoch Únie iných, ako je toto nariadenie.

Článok 5

Obstarávanie alebo používanie produktov s digitálnymi prvkami

1. Toto nariadenie nebráni členským štátom, aby na produkty s digitálnymi prvkami uplatňovali dodatočné kybernetickobezpečnostné požiadavky na obstarávanie alebo používanie týchto produktov na konkrétne účely, a to aj v prípadoch, keď sa tieto produkty obstarávajú alebo používajú na účely národnej bezpečnosti alebo obrany, za predpokladu, že takéto požiadavky sú v súlade s povinnosťami členských štátov stanovenými v práve Únie a že sú potrebné a primerané na dosiahnutie týchto účelov.

2. Bez toho, aby boli dotknuté smernice 2014/24/EÚ a 2014/25/EÚ, ak sa obstarávajú produkty s digitálnymi prvkami, ktoré patria do rozsahu pôsobnosti tohto nariadenia, členské štáty zabezpečia, aby sa v postupoch obstarávania zohľadňoval súlad so základnými požiadavkami kybernetickej bezpečnosti stanovenými v prílohe I k tomuto nariadeniu vrátane schopnosti výrobcov účinne riešiť zraniteľnosti.

Článok 6

Požiadavky na produkty s digitálnymi prvkami

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

a) spĺňajú základné požiadavky kybernetickej bezpečnosti stanovené v časti I prílohy I za predpokladu, že sú riadne nainštalované, udržiavané, používané na ich zamýšľaný účel alebo za podmienok, ktoré možno odôvodnene predvídať, a prípadne s nainštalovanými potrebnými aktualizáciami; a

b) postupy zavedené výrobcom sú v súlade so základnými požiadavkami kybernetickej bezpečnosti stanovenými v časti II prílohy I.

Článok 7

Dôležité produkty s digitálnymi prvkami

1. Produkty s digitálnymi prvkami, ktoré majú základnú funkciu kategórie produktov stanovenej v prílohe III, sa považujú za dôležité produkty s digitálnymi prvkami a podliehajú postupom posudzovania zhody uvedeným v článku 32 ods. 2 a 3. Integrácia produktu s digitálnymi prvkami, ktorý má základnú funkciu kategórie produktov stanovenej v prílohe III, sama osebe nespôsobuje, že produkt, do ktorého je integrovaný, podlieha postupom posudzovania zhody uvedeným v článku 32 ods. 2 a 3.

2. Kategórie produktov s digitálnymi prvkami uvedené v odseku 1 tohto článku rozdelené do tried I a II, ako sa uvádza v prílohe III, spĺňajú aspoň jedno z týchto kritérií:

a) produkt s digitálnymi prvkami primárne vykonáva funkcie kritické pre kybernetickú bezpečnosť iných produktov, sietí alebo služieb vrátane zabezpečenia autentifikácie a prístupu, prevencie a odhaľovania narušení, bezpečnosti koncových bodov alebo ochrany siete;

b) produkt s digitálnymi prvkami vykonáva funkciu, ktorá predstavuje významné riziko nepriaznivých účinkov z hľadiska jeho intenzity a schopnosti narušiť, ovládať alebo spôsobiť poškodenie veľkého počtu iných produktov alebo zdravia, bezpečnosti alebo ochrany jeho používateľov prostredníctvom priamej manipulácie, ako je funkcia centrálneho systému vrátane riadenia siete, kontroly konfigurácie, virtualizácie alebo spracovania osobných údajov.

3. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 61 s cieľom zmeniť prílohu III zaradením novej kategórie v každej triede kategórií produktov s digitálnymi prvkami do zoznamu, stanovením jej vymedzenia, presunutím kategórie produktov z jednej triedy do druhej alebo vypustením existujúcej kategórie z tohto zoznamu. Pri posudzovaní potreby zmeniť zoznam uvedený v prílohe III Komisia zohľadní funkcie súvisiace s kybernetickou bezpečnosťou alebo funkciu a úroveň kybernetickobezpečnostného rizika, ktoré predstavujú produkty s digitálnymi prvkami, ako sa stanovuje v kritériách uvedených v odseku 2 tohto článku.

V delegovaných aktoch uvedených v prvom pododseku tohto odseku sa v prípade potreby stanoví minimálne prechodné obdobie 12 mesiacov, najmä ak sa nová kategória dôležitých produktov s digitálnymi prvkami doplní do triedy I alebo II alebo sa presunie z triedy I do triedy II, ako sa stanovuje v prílohe III, pred začatím uplatňovania príslušných postupov posudzovania zhody uvedených v článku 32 ods. 2 a 3, pokiaľ nie je z vážnych a naliehavých dôvodov opodstatnené kratšie prechodné obdobie.

4. Komisia do 11. decembra 2025 prijme vykonávací akt, v ktorom spresní technický opis kategórií produktov s digitálnymi prvkami v triedach I a II stanovených v prílohe III a technický opis kategórií produktov s digitálnymi prvkami stanovený v prílohe IV. Uvedený vykonávací akt sa prijme v súlade s postupom preskúmania uvedeným v článku 62 ods. 2.

Článok 8

Kritické produkty s digitálnymi prvkami

1. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 61 na doplnenie tohto nariadenia s cieľom určiť, ktoré produkty s digitálnymi prvkami, ktoré majú základnú funkciu kategórie produktov stanovenej v prílohe IV k tomuto nariadeniu, sa majú vyžadovať na získanie európskeho certifikátu kybernetickej bezpečnosti aspoň na úrovni záruky „významná“ v rámci európskej schémy certifikácie kybernetickej bezpečnosti prijatej podľa nariadenia (EÚ) 2019/881, aby sa preukázala zhoda so základnými požiadavkami kybernetickej bezpečnosti stanovenými v prílohe I k tomuto nariadeniu alebo jeho častí za predpokladu, že európska schéma certifikácie kybernetickej bezpečnosti, ktorá sa vzťahuje na tieto kategórie produktov s digitálnymi prvkami, bola prijatá podľa nariadenia (EÚ) 2019/881 a výrobcovia ju majú k dispozícii. V uvedených delegovaných aktoch sa stanoví požadovaná úroveň záruky, ktorá je primeraná úrovni kybernetickobezpečnostného rizika spojeného s produktmi s digitálnymi prvkami a zohľadňuje ich zamýšľaný účel vrátane kritickej závislosti kľúčových subjektov uvedených v článku 3 ods. 1 smernice (EÚ) 2022/2555 od nich.

Komisia pred prijatím takýchto delegovaných aktov vykoná posúdenie potenciálneho vplyvu plánovaných opatrení na trh a uskutoční konzultácie s príslušnými zainteresovanými stranami vrátane európskej skupiny pre certifikáciu kybernetickej bezpečnosti zriadenej podľa nariadenia (EÚ) 2019/881. V posúdení sa zohľadní pripravenosť a úroveň kapacity členských štátov na vykonávanie príslušnej európskej schémy certifikácie kybernetickej bezpečnosti. Ak neboli prijaté žiadne delegované akty uvedené v prvom pododseku tohto odseku, produkty s digitálnymi prvkami, ktoré majú základnú funkciu kategórie produktov stanovenej v prílohe IV, podliehajú postupom posudzovania zhody uvedeným v článku 32 ods. 3.

V delegovaných aktoch uvedených v prvom pododseku sa stanoví minimálne prechodné obdobie šiestich mesiacov, pokiaľ z vážnych a naliehavých dôvodov nie je opodstatnené kratšie prechodné obdobie.

2. Komisia je v súlade s článkom 61 splnomocnená prijímať delegované akty s cieľom zmeniť prílohu IV pridaním alebo vypustením kategórií kritických produktov s digitálnymi prvkami. Pri určovaní takýchto kategórií kritických produktov s digitálnymi prvkami a požadovanej úrovne záruky v súlade s odsekom 1 tohto článku Komisia zohľadní kritériá uvedené v článku 7 ods. 2 a zabezpečí, aby kategórie produktov s digitálnymi prvkami spĺňali aspoň jedno z týchto kritérií:

a) existuje kritická závislosť kľúčových subjektov uvedených v článku 3 smernice (EÚ) 2022/2555 od kategórie produktov s digitálnymi prvkami;

b) incidenty a zneužité zraniteľnosti kategórie produktov s digitálnymi prvkami by mohli viesť k vážnemu narušeniu kritických dodávateľských reťazcov na celom vnútornom trhu.

Pred prijatím takýchto delegovaných aktov Komisia vykoná typové posúdenie uvedené v odseku 1.

V delegovaných aktoch uvedených v prvom pododseku sa stanoví minimálne prechodné obdobie šiestich mesiacov, pokiaľ z vážnych a naliehavých dôvodov nie je opodstatnené kratšie prechodné obdobie.

Článok 9

Konzultácie so zainteresovanými stranami

1. Pri príprave opatrení na vykonávanie tohto nariadenia Komisia konzultuje s príslušnými zainteresovanými stranami, ako sú príslušné orgány členských štátov, podniky súkromného sektora vrátane mikropodnikov a malých a stredných podnikov, komunita v oblasti softvéru s otvoreným zdrojovým kódom, spotrebiteľské združenia, akademická obec a príslušné agentúry a orgány Únie, ako aj expertné skupiny zriadené na úrovni Únie, a ich stanoviská zohľadní. Komisia v prípade potreby vedie štruktúrované konzultácie s týmito zainteresovanými stranami a vyžiada si ich názor, najmä keď:

a) vypracúva usmernenia uvedené v článku 26;

b) vypracúva technické opisy kategórií produktov uvedených v prílohe III v súlade s článkom 7 ods. 4, pričom posudzuje potreby potenciálnych aktualizácií zoznamu kategórií produktov v súlade s článkom 7 ods. 3 a článkom 8 ods. 2 alebo vykonáva posúdenie potenciálneho vplyvu na trh podľa článku 8 ods. 1 bez toho, aby bol dotknutý článok 61;

c) vykonáva prípravné práce na hodnotení a preskúmaní tohto nariadenia.

2. Komisia aspoň raz ročne usporiada pravidelné konzultácie a informačné stretnutia s cieľom zhromaždiť názory zainteresovaných strán uvedených v odseku 1 na vykonávanie tohto nariadenia.

Článok 10

Zlepšovanie zručností v kyberneticky odolnom digitálnom prostredí

Na účely tohto nariadenia a s cieľom reagovať na potreby odborníkov na podporu vykonávania tohto nariadenia členské štáty podľa potreby s podporou Komisie, Európskeho centra kompetencií v oblasti kybernetickej bezpečnosti a agentúry ENISA, pričom plne rešpektujú zodpovednosť členských štátov v oblasti vzdelávania, presadzujú opatrenia a stratégie zamerané na:

a) rozvoj zručností v oblasti kybernetickej bezpečnosti a vytváranie organizačných a technologických nástrojov na zabezpečenie dostatočnej dostupnosti kvalifikovaných odborníkov s cieľom podporiť činnosti orgánov dohľadu nad trhom a orgánov posudzovania zhody;

b) rozšírenie spolupráce medzi súkromným sektorom, hospodárskymi subjektmi, a to aj prostredníctvom rekvalifikácie alebo zvyšovania kvalifikácie zamestnancov výrobcov, spotrebiteľov, poskytovateľov vzdelávania a odbornej prípravy, ako aj verejnej správy, čím sa rozšíria možnosti prístupu mladých ľudí k pracovným príležitostiam v odvetví kybernetickej bezpečnosti.

Článok 11

Všeobecná bezpečnosť produktov

Odchylne od článku 2 ods. 1 tretieho pododseku písm. b) nariadenia (EÚ) 2023/988 sa kapitola III oddiel 1, kapitoly V a VII a kapitoly IX až XI uvedeného nariadenia uplatňujú na produkty s digitálnymi prvkami, pokiaľ ide o aspekty a riziká alebo kategórie rizík, na ktoré sa nevzťahuje toto nariadenie, ak sa na tieto produkty nevzťahujú osobitné bezpečnostné požiadavky stanovené inými harmonizačnými právnymi predpismi Únie v zmysle vymedzenia v článku 3 bode 27 nariadenia (EÚ) 2023/988.

Článok 12

Vysokorizikové systémy AI

1. Bez toho, aby boli dotknuté požiadavky na presnosť a odolnosť stanovené v článku 15 nariadenia (EÚ) 2024/1689, produkty s digitálnymi prvkami, ktoré patria do rozsahu pôsobnosti tohto nariadenia a ktoré sú klasifikované ako vysokorizikové systémy AI podľa článku 6 uvedeného nariadenia, sa považujú za produkty spĺňajúce požiadavky kybernetickej bezpečnosti stanovené v článku 15 uvedeného nariadenia, ak:

a) tieto produkty spĺňajú základné požiadavky kybernetickej bezpečnosti stanovené v časti I prílohy I;

b) procesy zavedené výrobcom sú v súlade so základnými požiadavkami kybernetickej bezpečnosti stanovenými v časti II prílohy I; a

c) dosiahnutie úrovne ochrany kybernetickej bezpečnosti požadovanej podľa článku 15 nariadenia (EÚ) 2024/1689 je preukázané v EÚ vyhlásení o zhode vydanom podľa tohto nariadenia.

2. V prípade produktov s digitálnymi prvkami a požiadaviek na kybernetickú bezpečnosť uvedených v odseku 1 tohto článku sa uplatňuje príslušný postup posudzovania zhody stanovený v článku 43 nariadenia (EÚ) 2024/1689. Na účely uvedeného posudzovania sú notifikované osoby, ktoré sú kompetentné kontrolovať zhodu vysokorizikových systémov AI podľa nariadenia (EÚ) 2024/1689 kompetentné kontrolovať aj zhodu vysokorizikových systémov AI, ktoré patria do 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 39 tohto nariadenia bol posúdený v kontexte postupu notifikácie podľa nariadenia (EÚ) 2024/1689.

3. Odchylne od odseku 2 tohto článku dôležité produkty s digitálnymi prvkami uvedené v prílohe III k tomuto nariadeniu, ktoré podliehajú postupom posudzovania zhody uvedeným v článku 32 ods. 2 písm. a) a b) a článku 32 ods. 3 tohto nariadenia a kritické produkty s digitálnymi prvkami uvedené v prílohe IV k tomuto nariadeniu, ktoré musia zároveň získať európsky certifikát kybernetickej bezpečnosti podľa článku 8 ods. 1 tohto nariadenia alebo, ak ho nemajú, ktoré podliehajú postupom posudzovania zhody podľa článku 32 ods. 3 tohto nariadenia a ktoré sú klasifikované ako vysokorizikové systémy AI podľa článku 6 nariadenia (EÚ) 2024/1689 a na ktoré sa uplatňuje postup posudzovania zhody založený na vnútornej kontrole uvedenej v prílohe VI k nariadeniu (EÚ) 2024/1689, podliehajú postupom posudzovania zhody podľa tohto nariadenia, pokiaľ ide o základné požiadavky kybernetickej bezpečnosti stanovené v tomto nariadení.

4. Výrobcovia produktov s digitálnymi prvkami uvedenými v odseku 1 tohto článku sa môžu zúčastňovať na experimentálnych regulačných prostrediach pre AI uvedených v článku 57 nariadenia (EÚ) 2024/1689.

KAPITOLA II

POVINNOSTI HOSPODÁRSKYCH SUBJEKTOV A USTANOVENIA TÝKAJÚCE SA SLOBODNÉHO SOFTVÉRU A SOFTVÉRU S OTVORENÝM ZDROJOVÝM Kódom

Článok 13

Povinnosti výrobcov

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

2. Na účel dosiahnutia súladu s odsekom 1 výrobcovia vykonajú posúdenie kybernetickobezpečnostných rizík spojených s produktom s digitálnymi prvkami a výsledok tohto posúdenia zohľadňujú vo fáze plánovania, návrhu, vývoja, výroby, dodania a údržby produktu s digitálnymi prvkami s cieľom minimalizovať kybernetickobezpečnostné riziká, predchádzať incidentom a minimalizovať ich vplyv, a to aj v súvislosti so zdravím a bezpečnosťou používateľov.

3. Posúdenie kybernetickobezpečnostných rizík sa zdokumentuje a podľa potreby aktualizuje počas obdobia podpory, ktoré sa určí v súlade s odsekom 8 tohto článku. Toto posúdenie kybernetickobezpečnostných rizík zahŕňa aspoň analýzu kybernetickobezpečnostných rizík založenú na zamýšľanom účele a logicky predvídateľnom používaní a podmienkach používania produktu s digitálnymi prvkami, ako je prevádzkové prostredie alebo aktíva, ktoré sa majú chrániť, s ohľadom na dĺžku predpokladaného používania produktu. V posúdení kybernetickobezpečnostných rizík sa uvedie, či, a ak áno, akým spôsobom sa bezpečnostné požiadavky stanovené v bode 2 časti I prílohy I vzťahujú na príslušný produkt s digitálnymi prvkami a ako sa tieto požiadavky vykonávajú na základe posúdenia kybernetickobezpečnostných rizík. Takisto sa v ňom uvedie, ako má výrobca uplatňovať bod 1 časti I prílohy I a požiadavky na riešenie zraniteľností stanovené v časti II prílohy I.

4. Pri uvádzaní produktu s digitálnymi prvkami na trh výrobca zahrnie posudzovanie kybernetickobezpečnostných rizík podľa odseku 3 tohto článku do technickej dokumentácie požadovanej podľa článku 31 a prílohy VII. V prípade produktov s digitálnymi prvkami uvedených v článku 12, ktoré podliehajú aj iným právnym aktom Únie, môže byť posudzovanie kybernetickobezpečnostných rizík súčasťou posudzovania rizík vyžadovaného v týchto právnych aktoch Únie. Ak na produkt s digitálnymi prvkami nemožno uplatniť určité základné požiadavky kybernetickej bezpečnosti, výrobca zahrnie do uvedenej technickej dokumentácie jasné odôvodnenie.

5. Na účely dosiahnutia súladu s odsekom 1 výrobcovia uplatňujú náležitú starostlivosť pri integrácii komponentov získaných od tretích strán tak, aby tieto komponenty neohrozovali kybernetickú bezpečnosť produktu s digitálnymi prvkami, a to aj pri integrácii komponentov slobodného softvéru a softvéru s otvoreným zdrojovým kódom, ktoré neboli sprístupnené na trhu v priebehu obchodnej činnosti.

6. Výrobcovia pri identifikácii zraniteľnosti v komponente, a to aj v komponente s otvoreným zdrojovým kódom, ktorý je integrovaný do produktu s digitálnymi prvkami, oznámia zraniteľnosť osobe alebo subjektu, ktorý komponent vyrába alebo vykonáva jeho údržbu, a riešia a odstraňujú zraniteľnosť v súlade s požiadavkami na riešenie zraniteľnosti stanovenými v časti II prílohy I. Ak výrobcovia vyvinuli úpravu softvéru alebo hardvéru na riešenie zraniteľnosti daného komponentu, poskytnú príslušný kód alebo dokumentáciu osobe alebo subjektu, ktoré komponent vyrábajú alebo vykonávajú jeho údržbu, v prípade potreby v strojovo čitateľnom formáte.

7. Výrobcovia systematicky dokumentujú spôsobom, ktorý je primeraný povahe a kybernetickobezpečnostným rizikám, príslušné aspekty kybernetickej bezpečnosti týkajúce sa produktov s digitálnymi prvkami vrátane zraniteľností, o ktorých sa dozvedeli, a akékoľvek relevantné informácie získané od tretích strán a v relevantnom prípade aktualizujú posúdenie kybernetickobezpečnostných rizík produktov.

8. Pri uvádzaní produktu s digitálnymi prvkami na trh a počas obdobia podpory výrobcovia zaistia, aby sa zraniteľnosti tohto produktu vrátane jeho komponentov riešili účinne a v súlade so základnými požiadavkami kybernetickej bezpečnosti stanovenými v časti II prílohy I.

Výrobcovia určia obdobie podpory s ohľadom na dĺžku predpokladaného používania produktu, pričom zohľadnia najmä primerané očakávania používateľov, povahu produktu vrátane jeho zamýšľaného účelu, ako aj príslušné právo Únie, ktorým sa určuje životnosť produktov s digitálnymi prvkami. Pri určovaní obdobia podpory môžu výrobcovia zohľadniť aj obdobia podpory produktov s digitálnymi prvkami s podobnou funkciou, ktoré na trh uvádzajú iní výrobcovia, dostupnosť prevádzkového prostredia, obdobia podpory integrovaných komponentov so základnými funkciami, ktoré pochádzajú od tretích strán, ako aj príslušné usmernenia od špecializovanej skupiny pre administratívnu spoluprácu (ďalej len „ADCO“) zriadenej podľa článku 52 ods. 15 a Komisiou. Záležitosti, ktoré sa majú zohľadniť pri určovaní obdobia podpory, sa posudzujú spôsobom, ktorým sa zabezpečí proporcionalita.

Bez toho, aby bol dotknutý druhý pododsek, trvá obdobie podpory najmenej päť rokov. Ak sa predpokladá, že produkt s digitálnymi prvkami sa bude používať menej ako päť rokov, obdobie podpory musí zodpovedať očakávanému obdobiu používania.

S prihliadnutím na odporúčania skupiny ADCO uvedené v článku 52 ods. 16 môže Komisia prijať delegované akty v súlade s článkom 61 s cieľom doplniť toto nariadenie špecifikovaním minimálneho obdobia podpory pre konkrétne kategórie produktov, ak z údajov dohľadu nad trhom vyplýva neprimerané obdobie podpory.

Výrobcovia uvedú informácie, ktoré sa zohľadnili pri určovaní obdobia podpory produktu s digitálnymi prvkami, v technickej dokumentácii stanovenej v prílohe VII.

Výrobcovia majú vhodné politiky a postupy vrátane politík koordinovaného zverejňovania informácií o zraniteľnostiach uvedených v bode 5 časti II prílohy I na spracovanie a nápravu možných zraniteľností produktu s digitálnymi prvkami oznámených internými alebo externými zdrojmi.

9. Výrobcovia zabezpečia, aby každá bezpečnostná aktualizácia uvedená v bode 8 časti II prílohy I, ktorá bola sprístupnená používateľom počas obdobia podpory, zostala k dispozícii po jej vydaní minimálne 10 rokov alebo počas zvyšku obdobia podpory, podľa toho, čo trvá dlhšie.

10. Ak výrobca uviedol na trh následné podstatne upravené verzie softvérového produktov, môže zabezpečiť súlad so základnou požiadavkou kybernetickej bezpečnosti stanovenou v bode 2 časti II prílohy I len v prípade verzie, ktorú naposledy uviedol na trh, za predpokladu, že používatelia verzií, ktoré boli uvedené na trh predtým, majú bezplatný prístup k verzii naposledy uvedenej na trh a nevznikajú im dodatočné náklady na úpravu hardvérového a softvérového prostredia, v ktorom používajú pôvodnú verziu tohto produktu.

11. Výrobcovia môžu viesť verejné softvérové archívy na zlepšenie prístupu používateľov k historickým verziám. V týchto prípadoch musia byť používatelia jasne a jednoducho dostupným spôsobom informovaní o rizikách spojených s používaním softvéru, ktorý už nie je podporovaný.

12. Výrobcovia pred uvedením produktu s digitálnymi prvkami na trh vypracujú technickú dokumentáciu uvedenú v článku 31.

Vykonajú alebo dajú vykonať zvolené postupy posudzovania zhody uvedené v článku 32.

Keď bol súlad produktu s digitálnymi prvkami so základnými požiadavkami kybernetickej bezpečnosti stanovenými v časti I prílohy I a procesov zavedených výrobcom so základnými požiadavkami kybernetickej bezpečnosti stanovenými v časti II prílohy I preukázaný týmto postupom posudzovania zhody, výrobcovia vypracujú EÚ vyhlásenie o zhode v súlade s článkom 28 a umiestnia označenie CE v súlade s článkom 30.

13. Výrobcovia uchovávajú technickú dokumentáciu a EÚ vyhlásenie o zhode k dispozícii pre orgány pre dohľad nad trhom aspoň 10 rokov od uvedenia produktu s digitálnymi prvkami na trh alebo počas obdobia podpory, podľa toho, čo trvá dlhšie.

14. Výrobcovia zaistia, aby boli zavedené postupy, vďaka ktorým bude v sériovej výrobe zachovaná zhoda produktov s digitálnymi prvkami s týmto nariadením. Výrobcovia primerane zohľadnia zmeny v procese vývoja a výroby alebo v návrhu či vlastnostiach produktu s digitálnymi prvkami a zmeny v harmonizovaných normách, európskych schémach certifikácie kybernetickej bezpečnosti alebo spoločných špecifikáciách uvedených v článku 27, na základe ktorých sa zhoda produktu s digitálnymi prvkami vyhlásila alebo ktorých uplatnením sa zhoda overila.

15. Výrobcovia zabezpečia, aby ich produkty s digitálnymi prvkami boli označené číslom typu, šarže alebo série alebo iným prvkom umožňujúcim ich identifikáciu, alebo ak to nie je možné, aby sa tieto informácie uvádzali na obale alebo v sprievodnej dokumentácii produktu s digitálnymi prvkami.

16. Na produkte s digitálnymi prvkami, na jeho obale alebo v sprievodnej dokumentácii uvedú výrobcovia svoje meno, zapísané obchodné meno alebo zapísanú ochrannú známku, poštovú a e-mailovú adresu alebo iné digitálne kontaktné údaje, a prípadne webové sídlo, na ktorých sa s nimi možno skontaktovať. Tieto informácie sa uvedú aj v informáciách a návode pre používateľa stanovených v prílohe II. Kontaktné údaje sú v jazyku ľahko zrozumiteľnom pre používateľov a orgány dohľadu nad trhom.

17. Na účely tohto nariadenia určia výrobcovia jednotné kontaktné miesto, aby používatelia mohli s nimi priamo a rýchlo komunikovať, a to aj s cieľom uľahčiť nahlasovanie zraniteľností produktu s digitálnymi prvkami.

Výrobcovia zabezpečia, aby používatelia mohli jednotné kontaktné miesto ľahko identifikovať. Jednotné kontaktné miesto uvedú aj v informáciách a návode pre používateľa stanovených v prílohe II.

Jednotné kontaktné miesto umožní používateľom bez obmedzenia na automatizované nástroje vybrať si, ktoré prostriedky uprednostnia.

18. Výrobcovia zabezpečia, aby boli k produktom s digitálnymi prvkami priložené informácie a návod pre používateľa uvedené v prílohe II, a to v tlačenej alebo elektronickej podobe. Uvedené informácie a pokyny sa poskytujú v jazyku ľahko zrozumiteľnom pre používateľa a orgány dohľadu nad trhom. Musia byť jasné, zrozumiteľné, pochopiteľné a čitateľné. Musia umožniť bezpečnú inštaláciu, prevádzku a používanie produktov s digitálnymi prvkami. Pre potreby používateľov a orgánov dohľadu nad trhom uchovávajú výrobcovia informácie a návod pre používateľa uvedené v prílohe II aspoň 10 rokov od uvedenia produktu s digitálnymi prvkami na trh alebo počas obdobia podpory, podľa toho, čo trvá dlhšie. Ak sa takéto informácie a návod poskytujú online, výrobcovia zabezpečia, aby boli prístupné, používateľsky ústretové a dostupné online aspoň 10 rokov po uvedení produktu s digitálnymi prvkami na trh alebo počas obdobia podpory, podľa toho, čo trvá dlhšie.

19. Výrobcovia zabezpečia, aby bol v čase nákupu jasne a zrozumiteľne uvedený dátum skončenia obdobia podpory uvedeného v odseku 8, a to aspoň mesiac a rok, a to ľahko dostupným spôsobom a prípadne na produkte s digitálnymi prvkami, jeho obale alebo digitálnymi prostriedkami.

Ak je to vzhľadom na povahu produktu s digitálnymi prvkami technicky možné, výrobcovia zobrazia pre používateľov oznámenie s informáciou, že obdobie podpory ich produktu s digitálnymi prvkami sa skončilo.

20. Výrobcovia spolu s produktom s digitálnymi prvkami poskytnú buď kópiu EÚ vyhlásenia o zhode alebo zjednodušené EÚ vyhlásenie o zhode. Ak poskytnú zjednodušené EÚ vyhlásenie o zhode, musí obsahovať presnú internetovú adresu, na ktorej je sprístupnené úplné znenie EÚ vyhlásenia o zhode.

21. Od uvedenia na trh a počas obdobia podpory výrobcovia, ktorí majú vedomosť alebo dôvod domnievať sa, že produkt s digitálnymi prvkami alebo nimi zavedené postupy nie sú v súlade so základnými požiadavkami kybernetickej bezpečnosti stanovenými v prílohe I, bezodkladne prijmú podľa vhodnosti nápravné opatrenia potrebné na uvedenie tohto produktu s digitálnymi prvkami alebo postupov výrobcu do súladu s príslušnými požiadavkami alebo na stiahnutie produktu z trhu alebo od používateľa.

22. Na základe odôvodnenej žiadosti orgánu dohľadu nad trhom poskytnú výrobcovia danému orgánu v jazyku, ktorý je pre tento orgán ľahko zrozumiteľný, všetky informácie a dokumentáciu v tlačenej alebo elektronickej forme potrebné na preukázanie zhody produktu s digitálnymi prvkami a postupov zavedených výrobcom so základnými požiadavkami kybernetickej bezpečnosti stanovenými v prílohe I. Na žiadosť tohto orgánu s ním výrobcovia spolupracujú pri všetkých opatreniach na odstránení kybernetickobezpečnostných rizík, ktoré predstavuje produkt s digitálnymi prvkami nimi uvedený na trh.

23. Výrobca, ktorý ukončí svoju činnosť a v dôsledku toho nie je schopný dosiahnuť súlad s týmto nariadením, ešte pred ukončením činnosti informuje príslušné orgány dohľadu nad trhom a všetkými dostupnými prostriedkami a v maximálnej možnej miere aj používateľov relevantných produktov s digitálnymi prvkami uvedených na trh o nastávajúcom ukončení činnosti.

24. Komisia môže prostredníctvom vykonávacích aktov a s ohľadom na európske alebo medzinárodné normy a odporúčané postupy špecifikovať formát a prvky zoznamu softvéru uvedeného v bode 1 časti II prílohy I. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 62 ods. 2.

25. S cieľom posúdiť závislosť členských štátov a Únie ako celku od softvérových komponentov, a najmä od komponentov kvalifikovaných ako slobodný softvér a softvér s otvoreným zdrojovým kódom, sa skupina ADCO môže rozhodnúť, že posúdi závislosť celej Únie od konkrétnych kategórií produktov s digitálnymi prvkami. Na tento účel môžu orgány dohľadu nad trhom požadovať od výrobcov takýchto kategórií produktov s digitálnymi prvkami, aby poskytli príslušné zoznamy softvéru, ako sa uvádzajú v bode 1 časti II prílohy I. Na základe takýchto informácií môžu orgány dohľadu nad trhom poskytnúť skupine ADCO anonymizované a súhrnné informácie o závislosti od softvéru. Skupina ADCO poskytne správu o výsledkoch posúdenia závislosti skupine pre spoluprácu zriadenej podľa článku 14 smernice (EÚ) 2022/2555.

Článok 14

Ohlasovacie povinnosti výrobcov

1. Výrobca oznámi každú aktívne zneužitú zraniteľnosť produktu s digitálnymi prvkami, o ktorej sa dozvie, jednotke CSIRT určenej za koordinátora v súlade s odsekom 7 tohto článku a súčasne agentúre ENISA. Výrobca túto aktívne zneužitú zraniteľnosť oznámi prostredníctvom jednotnej oznamovacej platformy zriadenej podľa článku 16.

2. Na účely oznamovania uvedeného v odseku 1 výrobca poskytne:

a) včasné varovanie o aktívne zneužitej zraniteľnosti, a to bez zbytočného odkladu a v každom prípade do 24 hodín po tom, ako sa výrobca o tejto zraniteľnosti dozvedel, v relevantnom prípade s uvedením členských štátov, na území ktorých je podľa vedomosti výrobcu jeho produkt s digitálnymi prvkami sprístupnený;

b) pokiaľ už neboli poskytnuté príslušné informácie, oznámenie o zraniteľnosti, a to bez zbytočného odkladu a v každom prípade do 72 hodín po tom, ako sa výrobca dozvedel o aktívne zneužitej zraniteľnosti, v ktorom poskytne, ak sú k dispozícii, všeobecné informácie o dotknutom produkte s digitálnymi prvkami, všeobecnej povahe zneužitia a dotknutej zraniteľnosti, ako aj o všetkých prijatých nápravných alebo zmierňujúcich opatreniach, a nápravných alebo zmierňujúcich opatreniach, ktorú môžu prijať používatelia, a v ktorých sa v relevantnom prípade uvedie aj to, do akej miery sú podľa výrobcu oznámené informácie citlivé;

c) pokiaľ už neboli poskytnuté príslušné informácie, záverečnú správu najneskôr 14 dní od dostupnosti nápravného alebo zmierňujúceho opatrenia, ktorá obsahuje aspoň:

   i) opis zraniteľnosti vrátane jej závažnosti a vplyvu;

   ii) informácie o akomkoľvek subjekte so zlým úmyslom, ktorý zraniteľnosť zneužil alebo zneužíva, ak sú k dispozícii;

   iii) podrobnosti o bezpečnostnej aktualizácii alebo iných nápravných opatreniach, ktoré boli sprístupnené na nápravu zraniteľnosti.

3. Výrobca oznámi každý závažný incident, ktorý má vplyv na bezpečnosť produktu s digitálnymi prvkami, o ktorom sa dozvie, súčasne jednotke CSIRT určenej za koordinátora v súlade s odsekom 7 tohto článku a agentúre ENISA. Výrobca tento incident oznámi cez jednotnú oznamovaciu platformu zriadenú podľa článku 16.

4. Na účely oznamovania uvedeného v odseku 3 výrobca poskytne:

a) oznámenie s včasným varovaním o závažnom incidente, ktorý má vplyv na bezpečnosť produktu s digitálnymi prvkami, bez zbytočného odkladu a v každom prípade do 24 hodín po tom, ako výrobca o tejto zraniteľnosti získal vedomosť, vrátane aspoň toho, či je podozrenie, že incident bol spôsobený nezákonným konaním alebo konaním so zlým úmyslom, a v relevantnom prípade s uvedením členských štátov, na území ktorých je podľa vedomosti výrobcu jeho produkt s digitálnymi prvkami sprístupnený;

b) pokiaľ už neboli poskytnuté príslušné informácie, oznámenie o incidente bez zbytočného odkladu a v každom prípade do 72 hodín po tom, ako výrobca získal vedomosť o incidente, v ktorom poskytne, ak sú k dispozícii, všeobecné informácie o povahe incidentu, prvé hodnotenie incidentu, ako aj o všetkých prijatých nápravných alebo zmierňujúcich opatreniach, a nápravných alebo zmierňujúcich opatreniach, ktoré môžu používatelia prijať a v ktorých sa podľa potreby uvedie aj to, do akej miery sú podľa výrobcu oznámené informácie citlivé;

c) ak neboli príslušné informácie už poskytnuté, do jedného mesiaca po podaní oznámenia o incidente podľa písmena b) záverečnú správu, ktorá obsahuje aspoň tieto informácie:

   i) podrobný opis incidentu vrátane jeho závažnosti a dosahu;

   ii) druh hrozby alebo hlavnú príčinu, ktorá pravdepodobne incident spôsobila;

   iii) vykonané a prebiehajúce zmierňujúce opatrenia.

5. Na účely odseku 3 sa incident, ktorý má vplyv na bezpečnosť produktu s digitálnymi prvkami, považuje za závažný, ak:

a) negatívne ovplyvňuje alebo môže negatívne ovplyvniť schopnosť produktu s digitálnymi prvkami chrániť dostupnosť, pravosť, integritu alebo dôvernosť citlivých alebo dôležitých údajov alebo funkcií; alebo

b) viedol alebo môže viesť k zavedeniu alebo spusteniu škodlivého kódu v produkte s digitálnymi prvkami alebo v sieti a informačných systémoch používateľa produktu s digitálnymi prvkami.

6. Jednotka CSIRT určená za koordinátora, ktorý na začiatku prijme oznámenie, môže v prípade potreby požiadať výrobcov, aby poskytli priebežnú správu o relevantných aktuálnych informáciách o stave aktívne zneužívanej zraniteľnosti alebo závažného incidentu, ktoré majú vplyv na bezpečnosť produktu s digitálnymi prvkami.

7. Oznámenia uvedené v odsekoch 1 a 3 tohto článku sa podávajú cez jednotnú oznamovaciu platformu uvedenú v článku 16, pričom sa použije jeden z koncových bodov na elektronické oznamovanie uvedených v článku 16 ods. 1. Oznámenie sa podáva cez koncový bod na elektronické oznamovanie u jednotky CSIRT určenej za koordinátora toho členského štátu, v ktorom majú výrobcovia hlavné miesto podnikateľskej činnosti v Únii, a zároveň je prístupné agentúre ENISA.

Na účely tejto smernice sa o výrobcovi predpokladá, že má hlavné miesto podnikateľskej činnosti v Únii v tom členskom štáte, v ktorom sa najčastejšie prijímajú rozhodnutia o kybernetickej bezpečnosti jeho produktov s digitálnymi prvkami. Ak takýto členský štát nemožno určiť, za hlavné miesto podnikateľskej činnosti sa považuje ten členský štát, v ktorom má dotknutý výrobca prevádzku s najvyšším počtom zamestnancov v Únii.

Ak výrobca nemá hlavné miesto podnikateľskej činnosti v Únii, podáva oznámenia uvedené v odsekoch 1 a 3 cez koncový bod na elektronické oznamovanie u jednotky CSIRT určenej za koordinátora v členskom štáte stanovenom na základe informácií, ktoré má výrobca k dispozícii, v tomto poradí:

a) členský štát sídla splnomocneného zástupcu, ktorý koná v mene výrobcu pre najvyšší počet produktov s digitálnymi prvkami tohto výrobcu;

b) členský štát sídla dovozcu, ktorý uvádza na trh najvyšší počet produktov s digitálnymi prvkami daného výrobcu;

c) členský štát sídla distribútora, ktorý na trhu sprístupňuje najvyšší počet produktov s digitálnymi prvkami daného výrobcu;

d) členský štát s najvyšším počtom používateľov produktov s digitálnymi prvkami daného výrobcu.

V súvislosti s tretím pododsekom písm. d) môže výrobca podávať oznámenia o akejkoľvek následnej aktívne zneužívanej zraniteľnosti alebo závažnom incidente, ktoré majú vplyv na bezpečnosť produktu s digitálnymi prvkami, tej istej jednotke CSIRT určenej za koordinátora, ktorej podal oznámenie prvýkrát.

8. Po tom, ako sa výrobca dozvedel o aktívne zneužitej zraniteľnosti alebo závažnom incidente, ktoré majú vplyv na bezpečnosť produktu s digitálnymi prvkami, informuje postihnutých používateľov produktu s digitálnymi prvkami a v relevantnom prípade všetkých používateľov o uvedenej zraniteľnosti alebo incidente a v prípade potreby o akomkoľvek zmierňovaní rizík a nápravných opatreniach, ktoré môžu používatelia zaviesť na zmiernenie vplyvu tejto zraniteľnosti alebo incidentu, v relevantnom prípade v štruktúrovanom, strojovo čitateľnom formáte, ktorý je automaticky ľahko spracovateľný. Ak výrobca včas neinformuje používateľov o produkte s digitálnymi prvkami, notifikované jednotky CSIRT určené za koordinátorov môžu používateľom poskytnúť takéto informácie, ak to považujú za primerané a potrebné na predchádzanie vplyvu tejto zraniteľnosti alebo incidentu alebo na jeho zmiernenie.

9. Komisia prijme do 11. decembra 2025 delegované akty v súlade s článkom 61 tohto nariadenia s cieľom doplniť toto nariadenie vymedzením podmienok pre uplatnenie dôvodov súvisiacich s kybernetickou bezpečnosťou vo vzťahu k odloženému rozosielaniu oznámení, ako sa uvádza v článku 16 ods. 2 tohto nariadenia. Pri príprave návrhov delegovaných aktov spolupracuje Komisia so sieťou jednotiek CSIRT zriadenou podľa článku 15 smernice (EÚ) 2022/2555 a agentúrou ENISA.

10. Komisia môže prostredníctvom vykonávacích aktov bližšie určiť formát a postupy oznamovania uvedené v tomto článku, ako aj v článkoch 15 a 16. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 62 ods. 2. Pri príprave týchto návrhov delegovaných aktov spolupracuje Komisia so sieťou jednotiek CSIRT a agentúrou ENISA.

Článok 15

Dobrovoľné oznamovanie

1. Výrobcovia, ako aj iné fyzické alebo právnické osoby môžu jednotke CSIRT určenej za koordinátora alebo agentúre ENISA dobrovoľne oznámiť akúkoľvek zraniteľnosť produktu s digitálnymi prvkami, ako aj kybernetické hrozby, ktoré by mohli zasiahnuť rizikový profil produktu s digitálnymi prvkami.

2. Výrobcovia, ako aj iné fyzické alebo právnické osoby môžu jednotke CSIRT určenej za koordinátora alebo agentúre ENISA dobrovoľne oznámiť akýkoľvek incident, ktorý má vplyv na bezpečnosť produktu s digitálnymi prvkami, ako aj udalosti odvrátené v poslednej chvíli, ktorých následkom by mohol byť takýto incident.

3. Jednotka CSIRT určená za koordinátora alebo agentúra ENISA spracúvajú oznámenia uvedené v odsekoch 1 a 2 tohto článku v súlade s postupom stanoveným v článku 16.

Jednotka CSIRT určená za koordinátora môže uprednostniť spracovanie povinných oznámení pred dobrovoľnými.

4. Ak fyzická alebo právnická osoba iná ako výrobca oznámi aktívne zneužitú zraniteľnosť alebo závažný incident, ktorý má vplyv na bezpečnosť produktu s digitálnymi prvkami v súlade s odsekom 1 alebo 2, jednotka CSIRT určená za koordinátora bez zbytočného odkladu o tom informuje výrobcu.

5. Jednotka CSIRT určená za koordinátora, ako aj agentúra ENISA zabezpečia dôvernosť a primeranú ochranu informácií od oznamujúcej fyzickej alebo právnickej osoby. Bez toho, aby bola dotknutá prevencia, vyšetrovanie, odhaľovanie a stíhanie trestných činov, oznamujúcej fyzickej alebo právnickej osobe nevznikajú v dôsledku dobrovoľného oznámenia žiadne ďalšie povinnosti, ktoré by sa na ňu nevzťahovali, ak by oznámenie nepodala.

Článok 16

Zriadenie jednotnej oznamovacej platformy

1. Na účely oznámení uvedených v článku 14 ods. 1 a 3 a článku 15 ods. 1 a 2 a s cieľom zjednodušiť oznamovacie povinnosti výrobcov zriadi agentúra ENISA jednotnú oznamovaciu platformu. Agentúra ENISA spravuje každodennú prevádzku tejto jednotnej oznamovacej platformy a vykonáva jej údržbu. Architektúra jednotnej oznamovacej platformy umožňuje členským štátom a agentúre ENISA zriadiť si vlastné koncové body na elektronické oznamovanie.

2. Jednotka CSIRT určená za koordinátora, ktorej sa na začiatku oznámenie doručí, po jeho doručení bezodkladne rozošle oznámenie prostredníctvom jednotnej oznamovacej platformy jednotkám CSIRT určeným za koordinátorov, na území ktorých bol produkt s digitálnymi prvkami podľa informácií výrobcu sprístupnený.

Za výnimočných okolností, a najmä na žiadosť výrobcu a vzhľadom na úroveň citlivosti oznámených informácií, ako uvádza výrobca podľa článku 14 ods. 2 písm. a) tohto nariadenia, sa rozosielanie oznámenia môže odložiť z opodstatnených dôvodov súvisiacich s kybernetickou bezpečnosťou na nevyhnutne potrebné obdobie, a to aj vtedy, keď sa na zraniteľnosť vzťahuje koordinovaný postup zverejňovania zraniteľností, ako sa uvádza v článku 12 ods. 1 smernice (EÚ) 2022/2555. Ak sa jednotka CSIRT rozhodne oznámenie nevydať, bezodkladne o svojom rozhodnutí informuje agentúru ENISA a nevydanie oznámenia odôvodní s uvedením, kedy oznámenie rozošle v súlade s postupom rozosielania stanoveným v tomto odseku. Jednotku CSIRT môže pri uplatňovaní dôvodov súvisiacich s kybernetickou bezpečnosťou v súvislosti s odloženým rozosielaním oznámenia podporovať agentúra ENISA.

Za obzvlášť výnimočných okolností, keď výrobca v oznámení uvedenom v článku 14 ods. 2 písm. b) uvedie:

a) že oznámenú zraniteľnosť aktívne zneužil škodlivý subjekt a podľa dostupných informácií nebola zneužitá v žiadnom inom členskom štáte, než je členský štát jednotky CSIRT určenej za koordinátora, ktorej výrobca zraniteľnosť oznámil;

b) že akékoľvek okamžité ďalšie rozosielanie informácií o oznámenej zraniteľnosti by pravdepodobne viedlo k poskytnutiu informácií, ktorých zverejnenie by bolo v rozpore so základnými záujmami tohto členského štátu; alebo

c) že oznámená zraniteľnosť predstavuje vysoké bezprostredné kybernetickobezpečnostné riziko vyplývajúce z ďalšieho rozosielania informácií o nej;

agentúre ENISA sa súčasne sprístupnia len informácie o tom, že oznámenie poskytol výrobca, všeobecné informácie o produkte, informácie o všeobecnej povahe zneužitia a informácie o tom, že sa vyskytli dôvody súvisiace s bezpečnosťou, a to až do rozoslania úplného oznámenia dotknutým jednotkám CSIRT a agentúre ENISA. Ak sa agentúra ENISA na základe týchto informácií domnieva, že existuje systémové riziko ovplyvňujúce bezpečnosť na vnútornom trhu, odporučí prijímajúcej jednotke CSIRT, aby rozoslala úplné oznámenie ostatným jednotkám CSIRT určeným za koordinátorov a samotnej agentúre ENISA.

3. Po doručení oznámenia o aktívnom zneužití zraniteľnosti produktu s digitálnymi prvkami alebo o závažnom incidente, ktorý má vplyv na bezpečnosť produktu s digitálnymi prvkami, jednotky CSIRT určené za koordinátorov poskytnú orgánom dohľadu nad trhom svojich príslušných členských štátov oznámené informácie, ktoré orgány dohľadu nad trhom potrebujú na plnenie svojich povinností podľa tohto nariadenia.

4. Agentúra ENISA prijme vhodné a primerané technické, prevádzkové a organizačné opatrenia na riadenie rizík pre bezpečnosť jednotnej oznamovacej platformy a informácií podávaných alebo šírených prostredníctvom jednotnej oznamovacej platformy. Každý bezpečnostný incident, ktorý má vplyv na jednotnú oznamovaciu platformu, bez zbytočného odkladu oznámi sieti jednotiek CSIRT, ako aj Komisii.

5. Agentúra ENISA v spolupráci so sieťou jednotiek CSIRT poskytuje a vykonáva špecifikácie technických, prevádzkových a organizačných opatrení na zriadenie, údržbu a bezpečnú prevádzku jednotnej oznamovacej platformy uvedenej v odseku 1, a to aspoň vrátane bezpečnostných opatrení týkajúcich sa zriadenia, prevádzky a údržby jednotnej oznamovacej platformy, ako aj koncových bodov na elektronické oznamovanie zriadených jednotkami CSIRT určenými za koordinátorov na vnútroštátnej úrovni a agentúrou ENISA na úrovni Únie vrátane procesných aspektov na zabezpečenie toho, aby sa v prípade, že pre oznámenú zraniteľnosť nie sú nápravné alebo zmierňujúce opatrenia, vymieňali informácie o tejto zraniteľnosti podľa prísnych bezpečnostných protokolov a podľa zásady „need-to-know“.

6. Ak jednotka CSIRT určená za koordinátora bola informovaná o aktívne zneužitej zraniteľnosti v rámci koordinovaného postupu zverejňovania zraniteľností, ako sa uvádza v článku 12 ods. 1 smernice (EÚ) 2022/2555, jednotka CSIRT určená za koordinátora, ktorej bolo pôvodne doručené oznámenie, môže odložiť rozosielanie príslušného oznámenia cez jednotnú oznamovaciu platformu z opodstatnených dôvodov súvisiacich s kybernetickou bezpečnosťou na obdobie, ktoré nie je dlhšie, než je nevyhnutne potrebné, a až do získania súhlasu zúčastnených strán poskytujúcich koordinované informácie o zraniteľnostiach so zverejnením. Táto požiadavka nebráni výrobcom, aby dobrovoľne oznamovali takúto zraniteľnosť v súlade s postupom stanoveným v tomto článku.

Článok 17

Ďalšie ustanovenia o oznamovaní

1. Jednotka ENISA môže Európskej sieti styčných organizácií pre kybernetické krízy (EU-CyCLONe) zriadenej článkom 16 smernice (EÚ) 2022/2555 poskytnúť informácie oznámené podľa článku 14 ods. 1 a 3 a článku 15 ods. 1 a 2 tohto nariadenia, ak sú takéto informácie relevantné pre koordinované riadenie rozsiahlych kybernetickobezpečnostných incidentov a kríz na operačnej úrovni. Na určenie tejto relevantnosti môže agentúra ENISA zvážiť technické analýzy vykonávané sieťou jednotiek CSIRT, ak sú k dispozícii.

2. Ak je informovanosť verejnosti potrebná na zabránenie alebo zmiernenie závažného incidentu, ktorý má vplyv na bezpečnosť produktu s digitálnymi prvkami alebo na riešenie prebiehajúceho incidentu, alebo ak je zverejnenie incidentu inak vo verejnom záujme, jednotka CSIRT určená za koordinátora v príslušnom členskom štáte môže po konzultácii s dotknutým výrobcom a v relevantnom prípade v spolupráci s agentúrou ENISA informovať verejnosť o incidente alebo požiadať výrobcu, aby tak urobil.

3. Agentúra ENISA na základe oznámení doručených podľa článku 14 ods. 1 a 3 a článku 15 ods. 1 a 2 tohto nariadenia vypracuje každých 24 mesiacov technickú správu o nových trendoch kybernetickej bezpečnosti v prípade produktov s digitálnymi prvkami a poskytne ju skupine pre spoluprácu zriadenej podľa článku 14 smernice (EÚ) 2022/2555. Prvú takúto správu poskytne do 24 mesiacov odo dňa začatia uplatňovania povinností stanovených v článku 14 ods. 1 a 3 tohto nariadenia. Agentúra ENISA uvedie relevantné informácie z technických správ vo svojej správe o stave kybernetickej bezpečnosti v Únii podľa článku 18 smernice (EÚ) 2022/2555.

4. Samotným úkonom oznámenia v súlade s článkom 14 ods. 1 a 3 alebo článkom 15 ods. 1 a 2 nevzniká oznamujúcej fyzickej alebo právnickej osobe zvýšená zodpovednosť.

5. Keď je k dispozícii bezpečnostná aktualizácia alebo iná forma nápravného alebo zmierňujúceho opatrenia, agentúra ENISA po dohode s výrobcom dotknutého produktu s digitálnymi prvkami doplní verejne známu zraniteľnosť oznámenú podľa článku 14 ods. 1 alebo článku 15 ods. 1 tohto nariadenia do európskej databázy zraniteľností zriadenej podľa článku 12 ods. 2 smernice (EÚ) 2022/2555.

6. Jednotky CSIRT určené za koordinátorov poskytujú podporu asistenčnej služby v súvislosti s oznamovacími povinnosťami podľa článku 14 výrobcom, a to najmä výrobcom považovaným za mikropodniky alebo malé či stredné podniky.

Článok 18

Splnomocnení zástupcovia

1. Výrobca môže určiť splnomocneného zástupcu písomným splnomocnením.

2. Povinnosti stanovené v článku 13 ods. 1 až 11, článku 13 ods. 12 prvom pododseku a v článku 13 ods. 14 nie sú súčasťou splnomocnenia splnomocneného zástupcu.

3. Splnomocnený zástupca vykonáva úlohy uvedené v splnomocnení od výrobcu. Splnomocnený zástupca poskytne kópiu splnomocnenia na požiadanie orgánu dohľadu nad trhom. Splnomocnením sa splnomocnenému zástupcovi umožní prinajmenšom:

a) uchovávať EÚ vyhlásenie o zhode uvedené v článku 28 a technickú dokumentáciu uvedenú v článku 31 k dispozícii pre orgány dohľadu nad trhom aspoň 10 rokov od uvedenia produktu s digitálnymi prvkami na trh alebo počas obdobia podpory podľa toho, čo trvá dlhšie;

b) poskytnúť orgánu dohľadu nad trhom na základe jeho odôvodnenej žiadosti všetky informácie a dokumentáciu potrebnú 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 splnomocnenie splnomocneného zástupcu.

Článok 19

Povinnosti dovozcov

1. Dovozcovia uvádzajú na trh len produkty s digitálnymi prvkami, ktoré spĺňajú základné požiadavky kybernetickej bezpečnosti stanovené v časti I prílohy I, a len ak sú postupy zavedené výrobcom v súlade so základnými požiadavkami kybernetickej bezpečnosti stanovenými v časti II 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 32;

b) výrobca vypracoval technickú dokumentáciu;

c) produkt s digitálnymi prvkami má označenie CE uvedené v článku 30 a je k nemu priložené EÚ vyhlásenie o zhode uvedené v článku 13 ods. 20, a informácie a pokyny pre používateľa stanovené v prílohe II, v jazyku zrozumiteľnom pre používateľov a orgány dohľadu nad trhom;

d) výrobca splnil požiadavky stanovené v článku 13 ods. 15, 16 a 19.

Na účely tohto odseku musia byť dovozcovia schopní poskytnúť potrebné doklady preukazujúce splnenie požiadaviek stanovených v tomto článku.

3. Ak sa dovozca domnieva alebo má dôvod sa domnievať, že produkt s digitálnymi prvkami alebo postupy zavedené výrobcom nie sú v zhode s týmto nariadením, dovozca neuvedie produkt na trh, kým sa v prípade tohto produktu alebo postupov zavedených výrobcom nedosiahne zhoda s týmto nariadením. Ak produkt s digitálnymi prvkami predstavuje navyše významné kybernetickobezpečnostné riziko, dovozca o tom informuje výrobcu a orgány dohľadu nad trhom.

Ak má dovozca dôvod domnievať sa, že produkt s digitálnymi prvkami môže predstavovať významné kybernetickobezpečnostné riziko vzhľadom na netechnické rizikové faktory, informuje o tom orgány dohľadu nad trhom. Po doručení takýchto informácií sa orgány dohľadu nad trhom riadia postupmi uvedenými v článku 54 ods. 2.

4. Dovozcovia uvedú na produkte s digitálnymi prvkami, na jeho obale alebo v sprievodnej dokumentácii produktu s digitálnymi prvkami svoje meno, zapísané obchodné meno alebo zapísanú ochrannú známku, poštovú adresu, emailovú adresu alebo iný digitálny kontaktný údaj, ako aj prípadné webové sídlo, na ktorých sa s nimi možno skontaktovať. Kontaktné údaje sú v jazyku, ktorý je pre používateľov a orgány dohľadu nad trhom ľahko zrozumiteľný.

5. Dovozcovia, ktorí majú vedomosť alebo dôvod domnievať sa, že produkt s digitálnymi prvkami, ktorý uviedli na trh, nie je v zhode s týmto nariadením, bezodkladne prijmú nápravné opatrenia nevyhnutné na zabezpečenie toho, aby produkt s digitálnymi prvkami bol v súlade s týmto nariadením, alebo ho v prípade potreby stiahnu z trhu či od používateľa.

Po zistení zraniteľnosti produktu s digitálnymi prvkami dovozcovia bez zbytočného odkladu informujú o tejto zraniteľnosti výrobcu. Ak produkt s digitálnymi prvkami predstavuje navyše 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 nesúlade a o všetkých prijatých nápravných opatreniach.

6. Dovozcovia uchovávajú pre orgány dohľadu nad trhom k dispozícii kópiu EÚ vyhlásenia o zhode aspoň 10 rokov od uvedenia produktu s digitálnymi prvkami na trh alebo počas obdobia podpory podľa toho, čo trvá dlhšie a zaistia, aby bola týmto orgánom na ich žiadosť sprístupnená technická dokumentácia.

7. 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 kybernetickej bezpečnosti stanovenými v časti I prílohy I, ako aj postupov zavedených výrobcom so základnými požiadavkami kybernetickej bezpečnosti stanovenými v časti II prílohy I, a to v jazyku, ktorý je pre tento

orgán ľahko zrozumiteľný. Na žiadosť tohto orgánu s ním spolupracujú pri všetkých opatreniach prijatých na odstránenie kybernetickobezpečnostných rizík, ktoré predstavuje produkt s digitálnymi prvkami, ktorý uviedli na trh.

8. Ak sa dovozca produktu s digitálnymi prvkami dozvie, že výrobca tohto produktu ukončil činnosť a v dôsledku toho nie je schopný plniť povinnosti stanovené v tomto nariadení, dovozca informuje o tejto situácii príslušné orgány dohľadu nad trhom a všetkými dostupnými prostriedkami a v maximálnej možnej miere aj používateľov produktov s digitálnymi prvkami uvedených na trh.

Článok 20

Povinnosti distribútorov

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

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 si splnili povinnosti stanovené v článku 13 ods. 15, 16, 18, 19 a 20 a článku 19 ods. 4 a distribútorovi poskytli všetky potrebné dokumenty.

3. Ak sa distribútor na základe svojich informácií domnieva alebo má dôvod sa domnievať, že produkt s digitálnymi prvkami alebo postupy zavedené výrobcom nie sú v zhode so základnými požiadavkami kybernetickej bezpečnosti stanovenými v prílohe I, nesmie produkt s digitálnymi prvkami sprístupniť na trhu, kým sa tento produkt alebo postupy zavedené výrobcom neuvedú do zhody s týmto nariadením. Ak produkt s digitálnymi prvkami predstavuje navyše významné kybernetickobezpečnostné riziko, distribútor o tom bezodkladne informuje výrobcu a orgány dohľadu nad trhom.

4. Distribútori, ktorí na základe svojich informácií majú vedomosť alebo dôvod sa domnievať, že produkt s digitálnymi prvkami, ktorý sprístupnili na trhu, alebo postupy zavedené jeho výrobcom nie sú v súlade s týmto nariadením, zaistia, aby boli prijaté nápravné opatrenia potrebné na to, aby tento produkt s digitálnymi prvkami alebo postupy zavedené jeho výrobcom uviedli do súladu, alebo prípadne na stiahnutie produktu z trhu alebo od používateľa.

Po zistení zraniteľnosti produktu s digitálnymi prvkami distribútori bez zbytočného odkladu informujú o tejto zraniteľnosti výrobcu. Ak produkt s digitálnymi prvkami predstavuje navyše 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 najmä podrobnosti o nesúlade 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 postupov zavedených jeho výrobcom s týmto nariadením 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. Ak sa distribútor produktu s digitálnymi prvkami na základe svojich informácií dozvie, že výrobca tohto produktu ukončil svoju činnosť a v dôsledku toho nie je schopný splniť povinnosti stanovené v tomto nariadení, distribútor bezodkladne 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 21

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

Dovozca alebo distribútor sa na účely tohto nariadenia považuje za výrobcu a vzťahujú sa naňho články 13 a 14, ak tento dovozca alebo distribútor uvádza produkt s digitálnymi prvkami na trh pod svojím menom alebo svojou ochrannou známkou, alebo ak podstatne upraví produkt s digitálnymi prvkami už uvedený na trh.

Článok 22

Iné prípady uplatňovania povinností výrobcov

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

2. Na osobu uvedenú v odseku 1 tohto článku sa vzťahujú povinnosti uvedené v článkoch 13 a 14 za tú časť produktu s digitálnymi prvkami, 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 23

Identifikácia hospodárskych subjektov

1. Hospodárske subjekty poskytnú na požiadanie orgánom dohľadu nad trhom tieto informácie:

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, ak sú tieto informácie k dispozícii.

2. Hospodárske subjekty musia byť schopné poskytnúť informácie uvedené v odseku 1 počas obdobia 10 rokov po tom, čo im bol produkt s digitálnymi prvkami dodaný, a počas obdobia 10 rokov po tom, čo produkt s digitálnymi prvkami dodali.

Článok 24

Povinnosti správcov softvéru s otvoreným zdrojovým kódom

1. Na podporu vývoja bezpečného produktu s digitálnymi prvkami, ako aj účinné riešenie zraniteľností zo strany programátorov daného produktu správcovia softvéru s otvoreným zdrojovým kódom overiteľným spôsobom zavedú a zdokumentujú politiku kybernetickej bezpečnosti. Uvedenou politikou sa posilní aj dobrovoľné oznamovanie zraniteľností, ako sa stanovuje v článku 15, zo strany programátorov daného produktu a zohľadní sa osobitná povaha správcu softvéru s otvoreným zdrojovým kódom a právne a organizačné opatrenia, ktoré sa na neho vzťahujú. Súčasťou tejto politiky sú najmä aspekty súvisiace s dokumentovaním, riešením a nápravou zraniteľností a podpora výmeny informácií o zistených zraniteľnostiach v komunite otvorených zdrojov.

2. Správcovia softvéru s otvoreným zdrojovým kódom spolupracujú s orgánmi dohľadu nad trhom na ich žiadosť s cieľom zmierňovať kybernetickobezpečnostné riziká, ktoré predstavuje produkt s digitálnymi prvkami považovaný za slobodný softvér a softvér s otvoreným zdrojovým kódom.

Na základe odôvodnenej žiadosti orgánu dohľadu nad trhom správcovia softvéru s otvoreným zdrojovým kódom poskytnú tomuto orgánu dokumentáciu uvedenú v odseku 1 v papierovej alebo elektronickej forme v jazyku preň ľahko zrozumiteľnom.

3. Povinnosti stanovené v článku 14 ods. 1 sa vzťahujú na správcov softvéru s otvoreným zdrojovým kódom, pokiaľ sa podieľajú na vývoji produktov s digitálnymi prvkami. Povinnosti stanovené v článku 14 ods. 3 a 8 sa vzťahujú na správcov softvéru s otvoreným zdrojovým kódom, pokiaľ závažné incidenty, ktoré majú vplyv na bezpečnosť produktov s digitálnymi prvkami, majú vplyv na siete a informačné systémy, ktoré správcovia softvéru s otvoreným zdrojovým kódom poskytujú na vývoj takýchto produktov.

Článok 25

Osvedčovanie bezpečnosti slobodného softvéru a softvéru s otvoreným zdrojovým kódom

Na uľahčenie povinnosti náležitej starostlivosti stanovenej v článku 13 ods. 5, najmä pokiaľ ide o výrobcov, ktorí do svojich produktov s digitálnymi prvkami integrujú komponenty slobodného softvéru a softvéru s otvoreným zdrojovým kódom, je Komisia splnomocnená prijímať delegované akty v súlade s článkom 61 na doplnenie tohto nariadenia zavedením programov dobrovoľného osvedčovania bezpečnosti, ktoré programátorom alebo používateľom produktov s digitálnymi prvkami považovaným za slobodný softvér a softvér s otvoreným zdrojovým kódom, ako aj iným tretím stranám umožní posúdiť súlad takýchto produktov so všetkými alebo určitými základnými požiadavkami kybernetickej bezpečnosti alebo inými povinnosťami stanovenými v tomto nariadení.

Článok 26

Usmernenia

1. Na podporu vykonávania a zaistenie konzistentnosti vykonávania uverejní Komisia usmernenia na pomoc hospodárskym subjektom pri uplatňovaní tohto nariadenia s osobitným zameraním na podporu jeho dodržiavania mikropodnikmi a malými a strednými podnikmi.

2. Ak má Komisia v úmysle poskytnúť usmernenia uvedené v odseku 1, zaoberá sa minimálne týmito aspektmi:

a) rozsah pôsobnosti tohto nariadenia s osobitným zameraním na riešenia spracovania údajov na diaľku a slobodný softvér a softvér s otvoreným zdrojovým kódom;

b) uplatňovanie období podpory pre konkrétne kategórie produktov s digitálnymi prvkami;

c) usmernenia so zameraním na výrobcov, na ktorých sa vzťahuje toto nariadenie a na ktorých sa vzťahujú aj iné harmonizačné právne predpisy Únie než toto nariadenie alebo iné súvisiace právne akty Únie;

d) pojem podstatnej úpravy.

Komisia vedie aj ľahko prístupný zoznam delegovaných a vykonávacích aktov prijatých podľa tohto nariadenia.

3. Pri príprave usmernení podľa tohto článku sa Komisia radí s príslušnými zainteresovanými stranami.

KAPITOLA III

ZHODA PRODUKTU S DIGITÁLNYMI PRVKAMI

Článok 27

Predpoklad zhody

1. O produktoch s digitálnymi prvkami a postupoch zavedených výrobcom, ktoré sú v zhode s harmonizovanými normami alebo ich časťami, na ktoré boli uverejnené odkazy v *Úradnom vestníku Európskej únie*, sa predpokladá, že sú v zhode so základnými požiadavkami kybernetickej bezpečnosti stanovenými v prílohe I, na ktoré sa vzťahujú tieto normy alebo ich časti.

Komisia v súlade s článkom 10 ods. 1 nariadenia (EÚ) č. 1025/2012 požiada jednu alebo viacero európskych normalizačných organizácií o vypracovanie harmonizovaných noriem pre základné požiadavky kybernetickej bezpečnosti stanovené v prílohe I k tomuto nariadeniu. Pri príprave žiadostí o vypracovanie normy k tomuto nariadeniu sa Komisia snaží zohľadniť existujúce zavedené alebo pripravované európske a medzinárodné kybernetickobezpečnostné normy s cieľom zjednodušiť tvorbu harmonizovaných noriem v súlade s nariadením (EÚ) č. 1025/2012.

2. Komisia môže prijať vykonávacie akty, v ktorých sa stanovia spoločné špecifikácie technických požiadaviek, ktoré poskytnú prostriedok na dosiahnutie súladu so základnými požiadavkami kybernetickej bezpečnosti stanovenými v prílohe I pre produkty s digitálnymi prvkami v rozsahu pôsobnosti tohto nariadenia.

Uvedené vykonávacie akty sa prijmú len vtedy, ak sú splnené tieto podmienky:

a) Komisia podľa článku 10 ods. 1 nariadenia (EÚ) č. 1025/2012 požiadala jednu alebo viaceré európske normalizačné organizácie o vypracovanie harmonizovanej normy pre základné požiadavky kybernetickej bezpečnosti stanovené v prílohe I a:

   i) žiadosť nebola prijatá;

   ii) harmonizované normy, ktoré boli predmetom tejto žiadosti, neboli odovzdané v lehote stanovenej podľa článku 10 ods. 1 nariadenia (EÚ) č. 1025/2012; alebo

   iii) harmonizované normy nie sú v súlade so žiadosťou; a

b) v *Úradnom vestníku Európskej únie* nie je uverejnený odkaz na harmonizované normy pre relevantné základné požiadavky kybernetickej bezpečnosti stanovené v prílohe I k tomuto nariadeniu v súlade s nariadením (EÚ) č. 1025/2012 a nepredpokladá sa, že takýto odkaz bude v primeranej lehote uverejnený.

Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 62 ods. 2.

3. Pred vypracovaním návrhu vykonávacieho aktu podľa odseku 2 tohto článku Komisia informuje výbor uvedený v článku 22 nariadenia (EÚ) č. 1025/2012 o tom, že podľa jej názoru sú splnené podmienky uvedené v odseku 2 tohto článku.

4. Pri príprave návrhu vykonávacieho aktu podľa odseku 2 Komisia zohľadní názory príslušných orgánov a náležite sa radí so všetkými relevantnými zainteresovanými stranami.

5. Produkty s digitálnymi prvkami a postupy zavedené výrobcom, ktoré sú v zhode so spoločnými špecifikáciami stanovenými vo vykonávacích aktoch uvedených v odseku 2 tohto článku alebo v ich častiach, sa považujú za produkty a postupy v zhode so základnými požiadavkami kybernetickej bezpečnosti stanovenými v prílohe I, na ktoré sa tieto spoločné špecifikácie alebo ich časti vzťahujú.

6. Ak harmonizovanú normu prijme európska normalizačná organizácia a Komisii navrhne, aby odkaz na ňu uverejnila v *Úradnom vestníku Európskej únie*, Komisia túto harmonizovanú normu posúdi v súlade s nariadením (EÚ) č. 1025/2012. Keď sa v *Úradnom vestníku Európskej únie* uverejní odkaz na harmonizovanú normu, Komisia zruší vykonávacie akty uvedené v odseku 2 tohto článku alebo tie ich časti, ktoré sa vzťahujú na tie isté základné požiadavky kybernetickej bezpečnosti ako daná harmonizovaná norma.

7. Ak sa členský štát domnieva, že spoločná špecifikácia úplne nevyhovuje základným požiadavkám kybernetickej bezpečnosti stanoveným v prílohe I, informuje o tom Komisiu, ktorej poskytne podrobné vysvetlenie. Komisia toto podrobné vysvetlenie posúdi a v prípade potreby môže zmeniť vykonávací akt, ktorým sa predmetná spoločná špecifikácia stanovuje.

8. Produkty s digitálnymi prvkami a postupy zavedené výrobcom, pre ktoré bolo vydané EÚ vyhlásenie o zhode alebo certifikát v rámci európskej schémy certifikácie kybernetickej bezpečnosti prijatej podľa nariadenia (EÚ) 2019/881, sa považujú za produkty a postupy v zhode so základnými požiadavkami kybernetickej bezpečnosti stanovenými v prílohe I, pokiaľ sa na tieto požiadavky vzťahuje EÚ vyhlásenie o zhode alebo európsky certifikát kybernetickej bezpečnosti, alebo ich časti.

9. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 61 tohto nariadenia na doplnenie tohto nariadenia špecifikovaním európskych schém certifikácie kybernetickej bezpečnosti prijatých podľa nariadenia (EÚ) 2019/881, ktoré sa môžu použiť na preukázanie zhody produktov s digitálnymi prvkami so základnými požiadavkami kybernetickej bezpečnosti alebo s ich časťami stanovenými v prílohe I k tomuto nariadeniu. Vydaním európskeho certifikátu kybernetickej bezpečnosti v rámci takýchto schém aspoň na úrovni záruky „významná“ sa navyše ruší povinnosť výrobcu dať tretej strane vykonať posúdenie zhody s príslušnými požiadavkami, ako sa stanovuje v článku 32 ods. 2 písm. a) a b) a v článku 32 ods. 3 písm. a) a b) tohto nariadenia.

Článok 28

EÚ vyhlásenie o zhode

1. EÚ vyhlásenie o zhode vypracujú výrobcovia v súlade s článkom 13 ods. 12 a uvedú v ňom, že bolo preukázané splnenie uplatniteľných základných požiadaviek kybernetickej bezpečnosti stanovených v prílohe I.

2. EÚ vyhlásenie o zhode má štruktúru, ktorej vzor je stanovený v prílohe V, a obsahuje prvky špecifikované v príslušných postupoch posudzovania zhody stanovených v prílohe VIII. Takéto vyhlásenie sa podľa potreby aktualizuje. Sprístupní sa v jazykoch požadovaných členským štátom, v ktorom sa produkt s digitálnymi prvkami uvádza na trh alebo sprístupňuje na trhu.

Zjednodušené EÚ vyhlásenie o zhode uvedené v článku 13 ods. 20 má štruktúru, ktorej vzor je stanovený v prílohe VI. Sprístupní sa v 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, pre všetky tieto právne akty Únie sa vypracuje jediné EÚ vyhlásenie o zhode. V uvedenom vyhlásení sú uvedené dotknuté právne akty Únie vrátane odkazov na ich uverejnenie.

4. Vypracovaním EÚ vyhlásenia o zhode preberá výrobca zodpovednosť za zhodu produktu s digitálnymi prvkami.

5. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 61 na doplnenie tohto nariadenia pridaním prvkov do minimálneho obsahu EÚ vyhlásenia o zhode stanoveného v prílohe V s cieľom zohľadniť technologický vývoj.

Článok 29

Všeobecné zásady označenia CE

Označenie CE sa riadi všeobecnými zásadami stanovenými v článku 30 nariadenia (ES) č. 765/2008.

Článok 30

Pravidlá a podmienky umiestňovania označenia CE

1. Označenie CE sa na produkt s digitálnymi prvkami umiestni tak, aby bolo viditeľné a čitateľné a nedalo sa zmazať. 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 28, 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 28 alebo na sprievodné webové sídlo softvérového produktu. V druhom prípade musí byť príslušná časť webového sídla ľahko a priamo prístupná spotrebiteľom.

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 označujúca osobitné kybernetickobezpečnostné riziko alebo použitie stanovené vo vykonávacích aktoch uvedených v odseku 6.

4. Za označením CE nasleduje identifikačné číslo notifikovanej osoby, ak sa táto osoba zúčastňuje na postupe posudzovania zhody založeného na plnom zabezpečení kvality (podľa modulu H) uvedeného v článku 32.

Identifikačné číslo notifikovanej osoby umiestňuje samotná osoba alebo podľa jej pokynov výrobca či splnomocnený zástupca výrobcu.

5. Pri zabezpečovaní správneho uplatňovania režimu úpravy označenia CE vychádzajú členské štáty z existujúcich mechanizmov a v prípade nesprávneho použitia tohto označenia prijmú primerané opatrenia. Ak sa na produkt s digitálnymi prvkami vzťahujú iné harmonizačné právne predpisy Únie ako toto nariadenie, v ktorých sa tiež vyžaduje umiestnenie označenia CE, v označení CE sa uvedie, že produkt spĺňa aj požiadavky stanovené v takýchto iných harmonizačných právnych predpisoch Únie.

6. Komisia môže prostredníctvom vykonávacích aktov stanoviť technické špecifikácie pre značky, piktogramy alebo akékoľvek iné značky týkajúce sa bezpečnosti produktov s digitálnymi prvkami, ich obdobia podpory a mechanizmov na podporu ich používania a na zvýšenie informovanosti verejnosti o bezpečnosti produktov s digitálnymi prvkami. Pri príprave návrhov vykonávacích aktov sa Komisia radí s príslušnými zainteresovanými stranami a so skupinou ADCO, ak už bola zriadená podľa článku 52 ods. 15. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 62 ods. 2.

Článok 31

Technická dokumentácia

1. Technická dokumentácia obsahuje všetky príslušné údaje alebo podrobnosti o prostriedkoch, ktoré výrobca použil na zaistenie toho, aby produkt s digitálnymi prvkami a postupy zavedené výrobcom boli v súlade so základnými požiadavkami kybernetickej bezpečnosti stanovenými v prílohe I. Obsahuje aspoň prvky stanovené v prílohe VII.

2. Technická dokumentácia sa vypracuje pred uvedením produktu s digitálnymi prvkami na trh a v prípade potreby sa priebežne aktualizuje, a to aspoň počas obdobia podpory.

3. V prípade produktov s digitálnymi prvkami uvedených v článku 12, na ktoré sa vzťahujú aj iné právne akty Únie, v ktorých sa stanovuje technická dokumentácia, sa vypracuje jediné vyhotovenie technickej dokumentácie s informáciami uvedenými v prílohe VII a informáciami, ktoré požadujú uvedené právne akty Únie.

4. Technická dokumentácia a korešpondencia súvisiace s postupom posudzovania zhody sa vypracujú 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 61 na doplnenie tohto nariadenia doplnením prvkov, ktoré sa majú zahrnúť do technickej dokumentácie uvedenej v prílohe VII, aby sa zohľadnil technologický vývoj, ako aj vývoj, ktorý nastane pri vykonávaní tohto nariadenia. Na tento účel sa Komisia snaží zabezpečiť, aby administratívna záťaž mikropodnikov a malých a stredných podnikov bola primeraná.

Článok 32

Postupy posudzovania zhody produktov s digitálnymi prvkami

1. Výrobca posudzuje zhodu produktu s digitálnymi prvkami a postupov zavedených výrobcom s cieľom určiť, či sú splnené základné požiadavky kybernetickej bezpečnosti stanovené v prílohe I. Výrobca preukazuje zhodu so základnými požiadavkami kybernetickej bezpečnosti niektorým z týchto postupov:

a) postup vnútornej kontroly (podľa modulu A) stanovený v prílohe VIII;

b) EÚ skúška typu (podľa modulu B) stanovená v prílohe VIII, po ktorej nasleduje zhoda s EÚ typom na základe vnútornej kontroly výroby (podľa modulu C) stanovenej v prílohe VIII;

c) posudzovanie zhody založené na úplnom zabezpečení kvality (podľa modulu H) stanovené v prílohe VIII; alebo

d) ak je to možné a uplatniteľné, európska schéma certifikácie kybernetickej bezpečnosti podľa článku 27 ods. 9.

2. Ak výrobca pri posudzovaní súladu dôležitého produktu s digitálnymi prvkami, ktorý patrí do triedy I v zmysle v prílohy III, a postupov zavedených jeho výrobcom so základnými požiadavkami kybernetickej bezpečnosti stanovenými v prílohe I neuplatnil alebo len čiastočne uplatnil harmonizované normy, spoločné špecifikácie alebo európske schémy certifikácie kybernetickej bezpečnosti aspoň na úrovni záruky „významná“, ako sa uvádza v článku 27, alebo ak takéto harmonizované normy, spoločné špecifikácie alebo európske schémy certifikácie kybernetickej bezpečnosti neexistujú, dotknutý produkt s digitálnymi prvkami a postupy zavedené výrobcom s ohľadom na tieto základné požiadavky kybernetickej bezpečnosti sa podrobia niektorému z týchto postupov:

a) EÚ skúška typu (podľa modulu B) stanovená v prílohe VIII, po ktorej nasleduje zhoda s EÚ typom na základe vnútornej kontroly výroby (podľa modulu C) stanovená v prílohe VIII; alebo

b) posudzovanie zhody na základe úplného zabezpečenia kvality (podľa modulu H) stanovené v prílohe VIII.

3. Ak je produkt dôležitým produktom s digitálnymi prvkami, ktorý patrí do triedy II v zmysle prílohy III, výrobca preukazuje zhodu so základnými požiadavkami kybernetickej bezpečnosti stanovenými v prílohe I niektorým z týchto postupov:

a) EÚ skúška typu (podľa modulu B) stanovená v prílohe VIII, po ktorej nasleduje zhoda s EÚ typom na základe vnútornej kontroly výroby (podľa modulu C) stanovenej v prílohe VIII;

b) posudzovanie zhody na základe úplného zabezpečenia kvality (podľa modulu H) stanovené v prílohe VIII; alebo

c) ak je to možné a vhodné, európska schéma certifikácie kybernetickej bezpečnosti podľa článku 27 ods. 9 tohto nariadenia aspoň na úrovni záruky „významná“ podľa nariadenia (EÚ) 2019/881.

4. U kritických produktov s digitálnymi prvkami uvedených v zozname v prílohe IV sa zhoda so základnými požiadavkami kybernetickej bezpečnosti stanovenými v prílohe I preukazuje jedným z týchto postupov:

a) európskou schémou certifikácie kybernetickej bezpečnosti v súlade s článkom 8 ods. 1; alebo

b) ak nie sú splnené podmienky uvedené v článku 8 ods. 1, ktorýmkoľvek z postupov uvedeným v odseku 3 tohto článku.

5. Výrobcovia produktov s digitálnymi prvkami považovanými za slobodný softvér a softvér s otvoreným zdrojovým kódom, ktoré patria do kategórií uvedených v prílohe III, musia byť schopní preukázať zhodu so základnými požiadavkami kybernetickej bezpečnosti stanovenými v prílohe I jedným z postupov uvedených v odseku 1 tohto článku za predpokladu, že technická dokumentácia uvedená v článku 31 je v čase uvedenia týchto produktov na trh sprístupnená verejnosti.

6. Pri určovaní poplatkov za postupy posudzovania zhody sa zohľadňujú osobitné záujmy a potreby mikropodnikov a malých a stredných podnikov vrátane startupov a uvedené poplatky sa znížia úmerne k ich osobitným záujmom a potrebám.

Článok 33

Opatrenia na podporu mikropodnikov a malých a stredných podnikov vrátane startupov

1. Členské štáty v prípade potreby prijmú tieto opatrenia prispôsobené potrebám mikropodnikov a malých podnikov:

a) organizujú osobitné činnosti na zvyšovanie informovanosti a odbornú prípravu o uplatňovaní tohto nariadenia;

b) zriadia špecializovaný kanál na komunikáciu s mikropodnikmi a malými podnikmi a prípadne s miestnymi orgánmi verejnej moci s cieľom poskytovať poradenstvo a odpovedať na otázky o vykonávaní tohto nariadenia;

c) podporujú činnosti testovania a posudzovania zhody, v relevantných prípadoch aj s podporou Európskeho centra kompetencií v oblasti kybernetickej bezpečnosti.

2. V prípade potreby môžu členské štáty zriadiť experimentálne regulačné prostredie pre kybernetickú odolnosť. Takéto experimentálne regulačné prostredie poskytuje kontrolované prostredie pre testovanie inovačných produktov s digitálnymi prvkami na uľahčenie ich vývoja, navrhovania, validácie a testovania na dosiahnutie súladu s týmto nariadením na obmedzený čas pred uvedením na trh. Na zriadenie a prevádzku experimentálneho regulačného prostredia môže Komisia a v relevantnom prípade agentúra ENISA poskytovať technickú podporu, poradenstvo a nástroje. Experimentálne regulačné prostredie sa zriaďuje pod priamym dohľadom a vedením a s podporou orgánov dohľadu nad trhom. Členské štáty informujú Komisiu a ostatné orgány dohľadu nad trhom o zriadení experimentálneho regulačného prostredia prostredníctvom skupiny ADCO. Experimentálnym regulačným prostredím nie sú dotknuté právomoci dohľadu a nápravy príslušných orgánov. K experimentálnemu regulačnému prostrediu zabezpečia členské štáty otvorený, spravodlivý a transparentný prístup, a najmä uľahčia prístup pre mikropodniky a malé podniky vrátane startupov.

3. V súlade s článkom 26 poskytne Komisia usmernenia k vykonávaniu tohto nariadenia pre mikropodniky a malé a stredné podniky.

4. Komisia zverejní finančnú podporu, ktorá je k dispozícii podľa regulačného rámca existujúcich programov Únie najmä na zmiernenie finančnej záťaže mikropodnikov a malých podnikov.

5. Mikropodniky a malé podniky môžu poskytnúť všetky časti technickej dokumentácie uvedené v prílohe VII v zjednodušenom formáte. Komisia na tento účel prostredníctvom vykonávacích aktov špecifikuje zjednodušený formát technickej dokumentácie so zameraním na potreby mikropodnikov a malých podnikov vrátane toho, ako majú byť pripravené časti stanovené v prílohe VII. Ak sa mikropodnik alebo malý podnik rozhodne poskytnúť informácie stanovené v prílohe VII zjednodušeným spôsobom, použije formát uvedený v tomto odseku. Notifikované osoby akceptujú tento formát na účely posudzovania zhody.

Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 62 ods. 2.

Článok 34

Dohody o vzájomnom uznávaní

S cieľom podporiť a uľahčiť medzinárodný obchod môže Únia s ohľadom na úroveň technického rozvoja a prístup k posudzovaniu zhody v tretej krajine v súlade s článkom 218 ZFEÚ uzatvárať s tretími krajinami dohody o vzájomnom uznávaní.

KAPITOLA IV

NOTIFIKÁCIA ORGÁNOV POSUDZOVANIA ZHODY

Článok 35

Notifikácia

1. Členské štáty notifikujú Komisiu a ostatné členské štáty o tom, ktoré osoby sú oprávnené vykonávať posudzovanie zhody v súlade s týmto nariadením.

2. Aby sa zamedzilo problémovým miestam a prekážkam pri vstupe na trh, usilujú členské štáty o zabezpečenie toho, aby do 11. decembra 2026 bol na výkon posudzovania zhody v Únii k dispozícii dostatočný počet notifikovaných osôb.

Článok 36

Notifikujúce orgány

1. Každý členský štát určí notifikujúci orgán zodpovedný za stanovenie a výkon postupov nevyhnutných na účely posudzovania, určenia a notifikácie orgánov posudzovania zhody a na účely ich monitorovania, ako aj za súlad s článkom 41.

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

3. Ak notifikujúci orgán deleguje posudzovanie, notifikáciu alebo monitorovanie uvedené v odseku 1 tohto článku na iný ako vládny subjekt alebo ho inak poverí výkonom týchto úloh, tento subjekt musí byť právnym subjektom a *mutatis mutandis* musí spĺňať požiadavky článku 37. Okrem toho musí mať zavedené mechanizmy na krytie záväzkov vyplývajúcich z jeho činností.

4. Notifikujúci orgán nesie plnú zodpovednosť za úlohy, ktoré vykonáva subjekt uvedený v odseku 3.

Článok 37

Požiadavky na notifikujúce orgány

1. Notifikujúci orgán sa zriadi tak, aby nedochádzalo ku konfliktu záujmov s orgánmi posudzovania zhody.

2. Notifikujúci orgán má takú organizačnú štruktúru a funguje tak, aby bola zabezpečená objektívnosť a nestrannosť jeho činností.

3. Notifikujúci orgán má takú organizačnú štruktúru, aby každé rozhodnutie o notifikácii orgánu posudzovania zhody prijímali iné odborne spôsobilé osoby ako tie, ktoré posúdenie vykonali.

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

5. Notifikujúci orgán zabezpečuje dôvernosť informácií, ktoré získal.

6. Na riadne plnenie svojich úloh má notifikujúci orgán k dispozícii dostatočný počet odborne spôsobilých zamestnancov.

Článok 38

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 s nimi súvisiacich zmenách.

2. Komisia zabezpečí, aby informácie uvedené v odseku 1 boli verejne dostupné.

Článok 39

Požiadavky na notifikované osoby

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

2. Orgán posudzovania zhody sa zriadi podľa vnútroštátneho práva a musí mať právnu subjektivitu.

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

Ak je preukázaná jeho nezávislosť a nedochádza ku konfliktu záujmov, možno za takúto tretiu stranu považovať subjekt, ktorý patrí do záujmového združenia alebo profesijného zväzu zastupujúceho 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 výkon úloh posudzovania zhody nie sú konštruktéri, programátori, výrobcovia, dodávatelia, dovozcovia, distribútori, subjekty vykonávajúce inštaláciu, nákupcovia, vlastníci, používatelia alebo subjekty vykonávajúce údržbu produktov s digitálnymi prvkami, ktoré posudzujú, ani splnomocnení zástupcovia žiadnej z týchto strán. Tým 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 výkon úloh posudzovania zhody nie sú priamo zapojení do navrhovania, vývoja, výroby, dovozu, distribúcie, uvádzania na trh, inštalácie, používania alebo údržby produktov s digitálnymi prvkami, ktoré posudzujú, ani nezastupujú strany zapojené do týchto činností. Nezúčastňujú sa na žiadnej činnosti, ktorá môže ovplyvniť ich nezávislý úsudok alebo bezúhonnosť vo vzťahu k činnostiam posudzovania zhody, na ktorých vykonávanie sú notifikovaní. Týka sa to najmä poradenských služieb.

Orgány posudzovania zhody zabezpečia, aby činnosti ich dcérskych spoločností alebo ich subdodávateľov nemali vplyv na dôvernosť, objektivitu alebo 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 úsudok 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 VIII, 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 je notifikovaný, k dispozícii potrebný:

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

b) opis postupov, v súlade s ktorými sa má vykonávať posudzovanie zhody, na zaistenie 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) postup na výkon činností, ktorý náležitým spôsobom zohľadňuje veľkosť podniku, odvetvie, v ktorom podnik pôsobí, jeho štruktúru, stupeň zložitosti technológie daného produktu a hromadnú či sériovú povahu výrobného postupu.

Orgán posudzovania zhody má prostriedky nevyhnutné na náležitý výkon technických a administratívnych úloh spojených s činnosťami posudzovania zhody a má prístup k všetkému potrebnému vybaveniu alebo zariadeniam.

7. Zamestnanci zodpovední za výkon činností posudzovania zhody majú:

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

b) dostatočné vedomosti o požiadavkách na výkon posudzovania a požadovanú právomoc toto posudzovanie vykonávať;

c) vhodné znalosti a porozumenie základných požiadaviek kybernetickej bezpečnosti stanovených v prílohe I, uplatniteľných harmonizovaných noriem a spoločných špecifikácií a príslušných ustanovení harmonizačných právnych predpisov Únie a vykonávacích aktov;

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

8. Musí sa zaručiť nestrannosť orgánov posudzovania zhody, ich vrcholového manažmentu a pracovníkov, ktorí vykonávajú posudzovanie.

Odmeňovanie vrcholového manažmentu orgánu posudzovania zhody a jeho pracovníkov, ktorí vykonávajú posudzovanie, nesmie závisieť od počtu vykonaných posúdení, ani od ich výsledkov.

9. Orgán posudzovania zhody uzavrie poistenie zodpovednosti za škodu, ak túto zodpovednosť neprevzal jeho členský štát v súlade s vnútroštátnym právom alebo ak za posudzovanie zhody nie je priamo zodpovedný samotný členský štát.

10. Zamestnanci orgánu posudzovania zhody sú povinní dodržiavať služobné tajomstvo, pokiaľ ide o všetky informácie získané pri výkone úloh podľa prílohy VIII 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 činnosť. Vlastnícke práva sú chránené. Orgán posudzovania zhody má zdokumentované postupy na zaistenie súladu s týmto odsekom.

11. Orgány posudzovania zhody sa zúčastňujú na príslušných normalizačných činnostiach a činnostiach koordinačnej skupiny notifikovanej osoby zriadenej podľa článku 51 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, primeraných a odôvodnených podmienok, pričom, pokiaľ ide o poplatky, zamedzia zbytočnej záťaži hospodárskych subjektov, najmä s ohľadom na záujmy mikropodnikov a malých a stredných podnikov.

Článok 40

Predpoklad zhody notifikovaných osôb

Ak orgán posudzovania zhody preukáže, že je v zhode 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 39 v takom rozsahu, v akom sa uplatniteľné harmonizované normy vzťahujú na tieto požiadavky.

Článok 41

Dcérske spoločnosti a subdodávatelia notifikovaných osôb

1. Ak notifikovaná osoba zadá špecifické úlohy spojené s posudzovaním zhody subdodávateľovi alebo na to využije dcérsku spoločnosť, zabezpečí, aby subdodávateľ alebo dcérska spoločnosť spĺňali požiadavky stanovené v článku 39, a zodpovedajúcim spôsobom o tom informuje notifikujúci orgán.

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

3. Činnosti môže vykonávať subdodávateľ alebo dcérska spoločnosť len so súhlasom výrobcu.

4. Notifikované osoby uchovávajú k dispozícii pre notifikujúci orgán príslušnú dokumentáciu týkajúcu sa posúdenia kvalifikácie subdodávateľa alebo dcérskej spoločnosti a práce, ktorú vykonali podľa tohto nariadenia.

Článok 42

Žiadosť o notifikáciu

1. Orgán posudzovania zhody podáva žiadosť o notifikáciu notifikujúcemu orgánu členského štátu svojho sídla.

2. Súčasťou žiadosti je opis činností posudzovania zhody, postupu alebo postupov posudzovania zhody a produktu alebo produktov s digitálnymi prvkami, v súvislosti s ktorými orgán tvrdí, že je spôsobilý, ako aj prípadné osvedčenie o akreditácii vydané vnútroštátnym akreditačným orgánom, ktoré osvedčuje, že orgán posudzovania zhody spĺňa požiadavky stanovené v článku 39.

3. Ak príslušný orgán posudzovania zhody nemôže poskytnúť osvedčenie o akreditácii, poskytne notifikujúcemu orgánu všetku dokumentáciu potrebnú na overenie, uznanie a pravidelné monitorovanie svojho súladu s požiadavkami stanovenými v článku 39.

Článok 43

Postup notifikácie

1. Notifikujúce orgány notifikujú iba tie orgány posudzovania zhody, ktoré splnili požiadavky stanovené v článku 39.

2. Notifikujúci orgán notifikuje Komisiu a ostatné členské štáty prostredníctvom informačného systému NANDO (New Approach Notified and Designated Organisations), ktorý vyvinula a spravuje Komisia.

3. Notifikácia obsahuje všetky podrobnosti o činnostiach posudzovania zhody, module alebo moduloch posudzovania zhody, dotknutom produkte alebo produktoch s digitálnymi prvkami a príslušné potvrdenie odbornej spôsobilosti.

4. Ak sa notifikácia nezakladá na osvedčení o akreditácii uvedenom v článku 42 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 39.

5. Príslušný orgán môže vykonávať činnosti notifikovanej osoby iba v prípade, že Komisia ani ostatné členské štáty nevzniesli námietky 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 považuje za notifikovanú osobu na účely tohto nariadenia.

6. Všetky neskoršie relevantné zmeny týkajúce sa notifikácie sa notifikujú Komisii a ostatným členským štátom.

Článok 44

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 právnych aktov Únie.

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

Aktualizáciu tohto zoznamu zabezpečuje Komisia.

Článok 45

Zmeny notifikácií

1. Ak notifikujúci orgán zistí alebo je informovaný o tom, že notifikovaná osoba už nespĺňa požiadavky stanovené v článku 39 alebo že si neplní povinnosti, notifikujúci orgán podľa potreby obmedzí, pozastaví alebo odníme notifikáciu v závislosti od závažnosti nesplnenia týchto požiadaviek alebo neplnenia povinností. Bezodkladne o tom informuje Komisiu a ostatné členské štáty.

2. V prípade obmedzenia, pozastavenia alebo odňatia notifikácie alebo ak notifikovaná osoba ukončila 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 46

Pochybnosti o odbornej spôsobilosti notifikovaných osôb

1. Komisia vyšetrí všetky prípady, v súvislosti s ktorými má pochybnosti alebo ak bola na pochybnosti upozornená, pokiaľ ide o odbornú spôsobilosť notifikovanej osoby splniť alebo nepretržite plniť požiadavky a povinnosti, ktoré sa na ňu vzťahujú.

2. Notifikujúci členský štát poskytne Komisii na jej žiadosť všetky informácie o podkladoch pre notifikáciu alebo o zachovaní odbornej spôsobilosti dotknutej osoby.

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

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

Článok 47

Povinnosti notifikovaných osôb pri výkone činností

1. Notifikované osoby vykonávajú posudzovanie zhody podľa postupov posudzovania zhody stanovených v článku 32 a prílohe VIII.

2. Posudzovanie zhody sa vykonáva primeraným spôsobom tak, aby sa zamedzilo zbytočnej záťaži hospodárskych subjektov. Pri výkone svojej činnosti orgány posudzovania zhody náležite zohľadňujú veľkosť podniku, najmä v prípade mikropodnikov a malých a stredných podnikov, odvetvie jeho činnosti, jeho štruktúru, stupeň zložitosti a úroveň kybernetickobezpečnostných rizík produktu s digitálnymi prvkami a danej technológie a hromadnú či sériovú povahu výrobného postupu.

3. Notifikovaná osoba však pri tom dbá na stupeň prísnosti a úroveň ochrany, ktoré sú potrebné na zabezpečenie súladu produktu s digitálnymi prvkami s týmto nariadením.

4. Ak notifikovaná osoba zistí, že výrobca nespĺňa požiadavky stanovené v prílohe I alebo zodpovedajúcich harmonizovaných normách alebo v spoločných špecifikáciách uvedených v článku 27, 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 produkt s digitálnymi prvkami 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 nápravné opatrenia neprijme alebo ak nemajú požadovaný účinok, notifikovaná osoba podľa potreby obmedzí, pozastaví platnosť alebo odníme všetky certifikáty.

Článok 48

Odvolanie proti rozhodnutiam notifikovaných osôb

Členské štáty zabezpečia, aby sa proti rozhodnutiam notifikovaných osôb bolo možné odvolať.

Článok 49

Informačná povinnosť notifikovaných osôb

1. Notifikované osoby informujú notifikujúci orgán:

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

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

c) o každej žiadosti o informácie 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 každej 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 tých istých produktov s digitálnymi prvkami, príslušné informácie o otázkach týkajúcich sa negatívnych a na požiadanie aj pozitívnych výsledkov posudzovania zhody.

Článok 50

Výmena skúseností

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

Článok 51

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 na práci tejto skupiny priamo alebo prostredníctvom určených zástupcov zúčastňovali osoby, ktoré notifikovali.

KAPITOLA V

DOHĽAD NAD TRHOM A PRESADZOVANIE PRÁVA

Článok 52

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

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

2. Na účely zaistenia účinného vykonávania tohto nariadenia určí každý členský štát 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 určené podľa odseku 2 tohto článku sú zodpovedné aj za výkon činností dohľadu nad trhom v súvislosti s povinnosťami správcov softvéru s otvoreným zdrojovým kódom stanovenými v článku 24. Ak orgán dohľadu nad trhom zistí, že si správca softvéru s otvoreným zdrojovým kódom neplní povinnosti stanovené v uvedenom článku, požiada správcu softvéru s otvoreným zdrojovým kódom, aby zabezpečil prijatie všetkých príslušných nápravných opatrení. Správcovia softvéru s otvoreným zdrojovým kódom zabezpečia prijatie všetkých príslušných nápravných opatrení vzhľadom na svoje povinnosti podľa tohto nariadenia.

4. 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 14 tohto nariadenia, určené orgány dohľadu nad trhom spolupracujú s jednotkami CSIRT určenými za koordinátorov a agentúrou ENISA a vymieňajú si s nimi pravidelne informácie.

5. Orgány dohľadu nad trhom môžu požiadať jednotku CSIRT určenú za koordinátora alebo agentúru ENISA o poskytnutie technického poradenstva v otázkach súvisiacich s vykonávaním a presadzovaním tohto nariadenia. Na podporu hodnotení zhody produktov s digitálnymi prvkami môžu orgány dohľadu nad trhom pri vedení vyšetrovania podľa článku 54 požiadať o analýzu jednotku CSIRT určenú za koordinátora alebo agentúru ENISA.

6. V relevantných prípadoch orgány dohľadu nad trhom spolupracujú s inými orgánmi dohľadu nad trhom určenými na základe iných harmonizačných právnych predpisov Únie ako toto nariadenie a pravidelne si vymieňajú informácie.

7. Orgány dohľadu nad trhom podľa potreby spolupracujú s orgánmi dohľadu nad právnymi predpismi Únie v oblasti ochrany osobných údajov. Takáto spolupráca zahŕňa informovanie uvedených orgánov o každom zistení relevantnom z hľadiska výkonu ich právomocí, a to aj pri vydávaní usmernení a poskytovaní poradenstva podľa odseku 10, ak sa takéto usmernenia a poradenstvo týkajú spracovania osobných údajov.

Orgány dohľadu nad právnymi predpismi Únie v oblasti ochrany osobných údajov majú právomoc požadovať akúkoľvek dokumentáciu založenú 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.

8. Členské štáty zaistia, aby určené orgány dohľadu nad trhom mali na plnenie svojich úloh podľa tohto nariadenia k dispozícii primerané finančné a technické zdroje, podľa potreby vrátane nástrojov na automatické spracovanie údajov, ako aj ľudské zdroje s primeranými kybernetickobezpečnostnými zručnosťami.

9. Komisia odporúča a podporuje výmenu skúseností medzi určenými orgánmi dohľadu nad trhom.

10. S podporou Komisie a podľa potreby jednotiek CSIRT a agentúry ENISA môžu orgány dohľadu nad trhom poskytovať hospodárskym subjektom usmernenia a poradenstvo v oblasti vykonávania tohto nariadenia.

11. Orgány dohľadu nad trhom informujú spotrebiteľov o tom, kde majú podávať sťažnosti, ktoré by mohli uvádzať nesúlad s týmto nariadením, v súlade s článkom 11 nariadenia (EÚ) 2019/1020 a spotrebiteľom poskytujú informácie o tom, kde a ako získať prístup k mechanizmom na uľahčenie oznamovania zraniteľností, incidentov a kybernetických hrozieb, ktoré môžu mať vplyv na produkty s digitálnymi prvkami.

12. Orgány dohľadu nad trhom podľa potreby uľahčujú spoluprácu relevantných zainteresovaných strán vrátane vedeckých, výskumných a spotrebiteľských organizácií.

13. 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 hospodárskej súťaže, oznámia orgány dohľadu nad trhom bezodkladne Komisii a príslušným vnútroštátnym orgánom na ochranu hospodárskej súťaže.

14. V prípade produktov s digitálnymi prvkami, ktoré patria do rozsahu pôsobnosti tohto nariadenia, klasifikovaných ako vysokorizikové systémy AI podľa článku 6 nariadenia (EÚ) 2024/1689, sú orgány dohľadu nad trhom určené na účely uvedeného nariadenia orgánmi zodpovednými za činnosti dohľadu nad trhom vyžadovanými podľa tohto nariadenia. Orgány dohľadu nad trhom určené podľa nariadenia (EÚ) 2024/1689 spolupracujú podľa potreby s orgánmi dohľadu nad trhom určenými podľa tohto nariadenia a pri dohľade nad výkonom oznamovacích povinností podľa článku 14 tohto nariadenia s jednotkami CSIRT určenými za koordinátorov a s agentúrou ENISA. Orgány dohľadu nad trhom určené podľa nariadenia (EÚ) 2024/1689 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.

15. Na jednotné uplatňovanie tohto nariadenia sa podľa článku 30 ods. 2 nariadenia (EÚ) 2019/1020 zriadi skupina ADCO. Skupinu ADCO tvoria zástupcovia určených orgánov dohľadu nad trhom a v relevantnom prípade zástupcovia ústredných kontaktných kancelárií. Skupina ADCO rieši aj osobitné záležitosti súvisiace s činnosťami dohľadu nad trhom v súvislosti s povinnosťami uloženými správcom softvéru s otvoreným zdrojovým kódom.

16. Orgány dohľadu nad trhom monitorujú, ako výrobcovia pri určovaní obdobia podpory pre svoje produkty s digitálnymi prvkami uplatňujú kritériá uvedené v článku 13 ods. 8.

Skupina ADCO uverejní vo verejne prístupnej a používateľsky ústretovej forme príslušné štatistiky o kategóriách produktov s digitálnymi prvkami vrátane priemerných období podpory, ako ich určil výrobca podľa článku 13 ods. 8, a poskytne usmernenia s orientačnými obdobiami podpory pre kategórie produktov s digitálnymi prvkami.

Ak z údajov vyplýva, že obdobia podpory pre konkrétne kategórie produktov s digitálnymi prvkami sú neadekvátne, skupina ADCO môže vydať odporúčania pre orgány dohľadu nad trhom, aby svoju činnosť zamerali na uvedené kategórie produktov s digitálnymi prvkami.

Článok 53

Prístup k údajom a dokumentácii

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

Článok 54

Vnútroštátny postup pre produkty s digitálnymi prvkami, ktoré predstavujú významné kybernetickobezpečnostné riziko

1. Ak má orgán dohľadu nad trhom členského štátu dostatočný dôvod domnievať sa, že produkt s digitálnymi prvkami vrátane riešenia jeho zraniteľností predstavuje významné kybernetickobezpečnostné riziko, bez zbytočného odkladu a v prípadnej spolupráci s príslušnou jednotkou CSIRT vykoná hodnotenie súladu produktu s digitálnymi prvkami so všetkými požiadavkami stanovenými v tomto nariadení. Príslušné hospodárske subjekty spolupracujú podľa potreby s orgánom dohľadu nad trhom.

Ak pri tomto hodnotení 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 s digitálnymi prvkami do súladu s uvedenými požiadavkami alebo aby produkt stiahol z trhu alebo od používateľov v primeranej lehote, ktorú môže orgán dohľadu nad trhom stanoviť a ktorá je úmerná povahe kybernetickobezpečnostného rizika.

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

2. Pri určovaní závažnosti kybernetickobezpečnostného rizika uvedeného v odseku 1 tohto článku orgány dohľadu nad trhom zohľadňujú aj netechnické rizikové faktory, najmä faktory zistené na základe koordinovaných posúdení bezpečnostných rizík kritických dodávateľských reťazcov na úrovni Únie vykonaných v súlade s článkom 22 smernice (EÚ) 2022/2555. Ak má orgán dohľadu nad trhom dostatočný dôvod domnievať sa, že produkt s digitálnymi prvkami predstavuje významné kybernetickobezpečnostné riziko vzhľadom na netechnické rizikové faktory, informuje o tom príslušné orgány určené alebo zriadené podľa článku 8 smernice (EÚ) 2022/2555 a podľa potreby s uvedenými orgánmi spolupracuje.

3. 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.

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

5. Ak hospodársky subjekt 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 sprístupňovanie uvedeného produktu s digitálnymi prvkami na svojom vnútroštátnom trhu, stiahnuť produkt z daného trhu alebo od používateľa.

Tento orgán bezodkladne oznámi uvedené opatrenia Komisii a ostatným členským štátom.

6. Informácie uvedené v odseku 5 zahŕňajú všetky dostupné podrobné údaje, najmä údaje potrebné na identifikáciu nevyhovujúceho produktu s digitálnymi prvkami, pôvod tohto produktu s digitálnymi prvkami, povahu údajného nesúladu a možného rizika, povahu a trvanie prijatých vnútroštátnych opatrení a stanoviská, ktoré poskytol príslušný hospodársky subjekt. Orgán dohľadu nad trhom predovšetkým uvedie, či k nesúladu došlo z jedného alebo viacerých týchto dôvodov:

a) produkt s digitálnymi prvkami alebo postupy zavedené výrobcom nespĺňajú základné požiadavky kybernetickej bezpečnosti stanovené v prílohe I;

b) nedostatky v harmonizovaných normách, európskych schémach certifikácie kybernetickej bezpečnosti alebo spoločných špecifikáciách uvedených v článku 27.

7. Orgány dohľadu nad trhom členských štátov iné než orgán dohľadu nad trhom členského štátu, ktorý postup začal, bezodkladne oznámia Komisii a ostatným členským štátom všetky prijaté opatrenia a všetky dodatočné informácie o nesúlade dotknutého produktu s digitálnymi prvkami, ktoré majú k dispozícii, a ak nesúhlasia s oznámeným vnútroštátnym opatrením, aj so svojimi námietkami.

8. Ak do troch mesiacov od doručenia oznámenia uvedeného v odseku 5 tohto článku žiaden členský štát ani Komisia nevznesú námietku proti predbežnému opatreniu prijatému členským štátom, opatrenie sa považuje za opodstatnené. Týmto nie sú dotknuté procesné práva dotknutého hospodárskeho subjektu v súlade s článkom 18 nariadenia (EÚ) 2019/1020.

9. Orgány dohľadu nad trhom všetkých členských štátov zabezpečia, aby sa vo vzťahu k dotknutému produktu s digitálnymi prvkami bezodkladne prijali primerané reštriktívne opatrenia, ako je napríklad stiahnutie daného produktu z ich trhu.

Článok 55

Ochranný postup Únie

1. Ak do troch mesiacov od doručenia oznámenia uvedeného v článku 54 ods. 5 členský štát vznesie námietky proti opatreniu prijatému iným členským štátom, alebo ak Komisia považuje toto opatrenie za také, ktoré je v rozpore s právom 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 54 ods. 5 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 nepovažuje za opodstatnené, 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 11 nariadenia (EÚ) č. 1025/2012.

4. Ak sa vnútroštátne opatrenie považuje za opodstatnené a nesúlad produktu s digitálnymi prvkami sa pripisuje nedostatkom v európskej schéme certifikácie kybernetickej bezpečnosti uvedenej v článku 27, Komisia zváži, či má zmeniť alebo zrušiť akýkoľvek delegovaný akt prijatý podľa článku 27 ods. 9, v ktorom sa uvádza predpoklad zhody pre túto schému certifikácie.

5. Ak sa vnútroštátne opatrenie považuje za opodstatnené a nesúlad produktu s digitálnymi prvkami sa pripisuje nedostatkom v spoločných špecifikáciách uvedených v článku 27, Komisia zváži, či má zmeniť alebo zrušiť akýkoľvek vykonávací akt prijatý podľa článku 27 ods. 2, ktorým sa stanovujú tieto spoločné špecifikácie.

Článok 56

Postup na úrovni Únie pre produkty s digitálnymi prvkami, ktoré predstavujú významné kybernetickobezpečnostné riziko

1. Ak má Komisia dostatočný dôvod 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, informuje o tom príslušné orgány dohľadu nad trhom. Ak orgány dohľadu nad trhom vykonávajú hodnotenie daného produktu s digitálnymi prvkami, ktorý môže predstavovať významné kybernetickobezpečnostné riziko z hľadiska jeho súladu s požiadavkami stanovenými v tomto nariadení, uplatňujú sa postupy uvedené v článkoch 54 a 55.

2. Ak má Komisia dostatočný dôvod domnievať sa, že produkt s digitálnymi prvkami predstavuje významné kybernetickobezpečnostné riziko vzhľadom na netechnické rizikové faktory, informuje o tom príslušné orgány dohľadu nad trhom a podľa potreby príslušné orgány určené alebo zriadené podľa článku 8 smernice (EÚ) 2022/2555 a podľa potreby s uvedenými orgánmi spolupracuje. Komisia takisto zváži relevantnosť zistených rizík daného produktu s digitálnymi prvkami so zreteľom na svoje úlohy koordinovaného posudzovania bezpečnostných rizík kritických dodávateľských reťazcov na úrovni Únie stanovených v článku 22 smernice (EÚ) 2022/2555 a v prípade potreby konzultuje so skupinou pre spoluprácu zriadenou podľa článku 14 smernice (EÚ) 2022/2555 a agentúrou ENISA.

3. Za okolností, ktoré odôvodňujú okamžitý zásah na zachovanie riadneho fungovania vnútorného trhu, a ak má Komisia dostatočný dôvod domnievať sa, že produkt s digitálnymi prvkami uvedený v odseku 1 naďalej nie je v súlade s požiadavkami stanovenými v tomto nariadení a príslušné orgány dohľadu nad trhom neprijali účinné opatrenia, Komisia vykoná hodnotenie súladu a môže požiadať agentúru ENISA, aby poskytla analýzu na jeho podporu. Komisia o tom informuje príslušné orgány dohľadu nad trhom. Príslušné hospodárske subjekty spolupracujú podľa potreby s agentúrou ENISA.

4. Komisia môže na základe hodnotenia uvedeného v odseku 3 rozhodnúť, že sú potrebné nápravné alebo reštriktívne opatrenia na úrovni Únie. Na tento účel bezodkladne konzultuje s dotknutými členskými štátmi a príslušným hospodárskym subjektom alebo subjektmi.

5. Na základe konzultácie uvedenej v odseku 4 tohto článku môže Komisia prijať vykonávacie akty na zabezpečenie nápravných alebo reštriktívnych opatrení na úrovni Únie, ako aj nariadiť stiahnutie dotknutých produktov s digitálnymi prvkami z trhu alebo od používateľov v primeranej lehote úmernej povahe rizika. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 62 ods. 2.

6. Komisia bezodkladne oznámi vykonávacie akty uvedené v odseku 5 príslušnému hospodárskemu subjektu alebo subjektom. Členské štáty bezodkladne vykonajú uvedené vykonávacie akty a náležite o tom informujú Komisiu.

7. Odseky 3 až 6 sa uplatňujú počas výnimočnej situácie, ktorá odôvodnila zásah Komisie, za predpokladu, že produkt s dotknutými digitálnymi prvkami nie je uvedený do súladu s týmto nariadením.

Článok 57

Produkty s digitálnymi prvkami, ktoré sú v súlade a predstavujú významné kybernetickobezpečnostné riziko

1. Orgán dohľadu nad trhom členského štátu požiada hospodársky subjekt, aby prijal všetky vhodné opatrenia, ak po vykonaní hodnotenia podľa článku 54 zistí, že hoci produkt s digitálnymi prvkami a postupy zavedené výrobcom sú v súlade s týmto nariadením, predstavujú významné kybernetickobezpečnostné riziko, ako aj riziko pre:

a) zdravie alebo bezpečnosť osôb;

b) súlad s povinnosťami vyplývajúcimi z práva Únie alebo vnútroštátneho práva, ktorého zámerom je ochrana základných práv;

c) dostupnosť, pravosť, integritu alebo dôvernosť služieb, ktoré prostredníctvom elektronického informačného systému ponúkajú kľúčové subjekty uvedené v článku 3 ods. 1 smernice (EÚ) 2022/2555; alebo

d) iné aspekty ochrany verejného záujmu.

K opatreniam uvedeným v prvom pododseku môžu patriť opatrenia na zabezpečenie toho, aby príslušný produkt s digitálnymi prvkami a postupy zavedené výrobcom pri sprístupňovaní na trhu už nepredstavovali relevantné riziká, stiahnutie dotknutého produktu s digitálnymi prvkami z trhu alebo jeho stiahnutie od používateľov a musia byť primerané povahe uvedených rizík.

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, povahu možného rizika a povahu 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 uvedené v odseku 4 je určené členským štátom.

6. Ak má Komisia dostatočný dôvod 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 tohto článku, informuje o tom a môže požiadať príslušný orgán alebo orgány dohľadu nad trhom, aby vykonali hodnotenie a riadili sa postupmi uvedenými v článku 54 a v odsekoch 1, 2 a 3 tohto článku.

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

8. Komisia môže na základe hodnotenia uvedeného v odseku 7 potvrdiť, že sú potrebné nápravné alebo reštriktívne opatrenia na úrovni Únie. Na tento účel bezodkladne konzultuje s dotknutými členskými štátmi a príslušným hospodárskym subjektom alebo subjektmi.

9. Na základe konzultácie uvedenej v odseku 8 tohto článku môže Komisia prijať vykonávacie akty s cieľom rozhodnúť o nápravných alebo reštriktívnych opatreniach na úrovni Únie, ako aj nariadiť stiahnutie dotknutých produktov s digitálnymi prvkami z trhu alebo od používateľov v primeranej lehote úmernej povahe rizika. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 62 ods. 2.

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

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

Článok 58

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 CE je umiestnené v rozpore s článkami 29 a 30;

b) označenie CE nie je vôbec umiestnené;

c) EÚ vyhlásenie o zhode nie je vypracované;

d) EÚ vyhlásenie o zhode nie je vypracované správne;

e) identifikačné číslo notifikovanej osoby zapojenej do postupu posudzovania zhody nie je v relevantných prípadoch pripojené;

f) technická dokumentácia nie je dostupná alebo nie je úplná.

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

Článok 59

Spoločné činnosti orgánov dohľadu nad trhom

1. Orgány dohľadu nad trhom sa môžu dohodnúť s inými príslušnými orgánmi na výkone 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 s digitálnymi prvkami, v prípade ktorých sa často zistí, že predstavujú kybernetickobezpečnostné riziká.

2. Komisia alebo agentúra ENISA navrhne spoločné činnosti na kontrolu 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 s digitálnymi prvkami, ktoré patria do rozsahu pôsobnosti tohto nariadenia, s požiadavkami stanovenými v tomto nariadení.

3. Orgány dohľadu nad trhom a v relevantnom prípade 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, ktoré získal pri spoločných činnostiach vykonávaných v rámci akéhokoľvek vyšetrovania, ktoré vedie.

5. Dotknutý orgán dohľadu nad trhom a v relevantnom prípade Komisia sprístupnia verejnosti dohodu o spoločných činnostiach vrátane mien/názvov zúčastnených strán.

Článok 60

Kontrolné akcie

1. Orgány dohľadu nad trhom vykonávajú súbežné koordinované akcie na kontrolu (ďalej len „kontrolné akcie“) konkrétnych produktov s digitálnymi prvkami alebo ich kategórií na kontrolu súladu s týmto nariadením alebo odhaľovanie jeho porušení. Súčasťou uvedených kontrolných akcií môžu byť kontroly produktov s digitálnymi prvkami nadobudnutými pod utajenou totožnosťou.

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

3. Ak agentúra ENISA pri plnení svojich úloh, a to aj na základe oznámení doručených podľa článku 14 ods. 1 a 3, identifikuje kategórie produktov s digitálnymi prvkami, pre ktoré sa môžu organizovať kontrolné akcie, podá návrh kontrolnej akcie koordinátorovi uvedenému v odseku 2 tohto článku na zváženie orgánom dohľadu nad trhom.

4. Pri výkone kontrolných akcií môžu zapojené orgány dohľadu nad trhom využívať vyšetrovacie právomoci stanovené v článkoch 52 až 58 a akékoľvek iné právomoci, ktoré im boli zverené podľa 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 61

Výkon delegovania právomoci

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

2. Právomoc prijímať delegované akty uvedené v článku 2 ods. 5 druhom pododseku, článku 7 ods. 3, článku 8 ods. 1 a 2, článku 13 ods. 8 štvrtom pododseku, článku 14 ods. 9, článku 25, článku 27 ods. 9, článku 28 ods. 5 a článku 31 ods. 5 sa Komisii udeľuje na obdobie piatich rokov odo 10. decembra 2024. Komisia vypracuje správu týkajúcu sa delegovania právomoci najneskôr deväť mesiacov pred uplynutím tohto päťročného obdobia. Delegovanie právomoci sa automaticky predlžuje o rovnako dlhé obdobia, pokiaľ Európsky parlament alebo Rada nevznesú voči takémuto predĺženiu námietku najneskôr tri mesiace pred uplynutím každého obdobia.

3. Delegovanie právomoci uvedené v článku 2 ods. 5 druhom pododseku, článku 7 ods. 3, článku 8 ods. 1 a 2, článku 13 ods. 8 štvrtom pododseku, článku 14 ods. 9, článku 25, článku 27 ods. 9, článku 28 ods. 5 a článku 31 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. 5 druhého pododseku, článku 7 ods. 3, článku 8 ods. 1 alebo 2, článku 13 ods. 8 štvrtého pododseku, článku 14 ods. 9, článku 25, článku 27 ods. 9, článku 28 ods. 5 alebo článku 31 ods. 5 nadobudne účinnosť, len ak Európsky parlament alebo Rada voči nemu nevzniesli námietku v lehote dvoch mesiacov od dátumu 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 62

Postup výboru

1. Komisii pomáha výbor. Uvedený 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 INFORMÁCIÍ A SANKCIE

Článok 63

Dôvernosť informácií

1. Všetky strany, ktoré sa zúčastňujú na uplatňovaní tohto nariadenia, sú povinné zachovávať dôvernosť informácií a údajov nadobudnutých pri výkone svojich úloh a činností tak, 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 (EÚ) 2016/943 ([37]);

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 si dôverne vymieňajú orgány dohľadu nad trhom navzájom a orgány dohľadu nad trhom s Komisiou, nezverejňujú bez predchádzajúceho súhlasu orgánu dohľadu nad trhom, od ktorého 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.

Článok 64

Sankcie

1. Členské štáty stanovia pravidlá, pokiaľ ide o sankcie uplatniteľné pri porušení tohto nariadenia, a prijmú všetky opatrenia potrebné na zabezpečenie ich vykonávania. Stanovené sankcie musia byť účinné, primerané a odrádzajúce. Členské štáty o týchto pravidlách a opatreniach bezodkladne informujú Komisiu a bezodkladne jej oznámia každú ďalšiu zmenu, ktorá ich ovplyvní.

2. Za nesúlad so základnými požiadavkami kybernetickej bezpečnosti stanovenými v prílohe I a s povinnosťami stanovenými v článkoch 13 a 14 sa ukladajú správne pokuty až do výšky 15 000 000 EUR, alebo ak je porušiteľom podnik, až do výšky 2,5 % jeho celkového ročného celosvetového obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia.

3. Za neplnenie povinností stanovených v článkoch 18 až 23, článku 28, článku 30 ods. 1 až 4, článku 31 ods. 1 až 4, článku 32 ods. 1, 2 a 3, článku 33 ods. 5 a článkoch 39, 41, 47, 49 a 53 sa ukladajú správne pokuty až do výšky 10 000 000 EUR, alebo ak je porušiteľom podnik, až do výšky 2 % jeho celkového ročného celosvetového obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia.

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

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

5. Pri rozhodovaní o výške správnej pokuty sa v každom 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 tie isté alebo iné orgány dohľadu nad trhom uložili tomu istému hospodárskemu subjektu správne pokuty za podobné porušenie;

c) veľkosť, najmä pokiaľ ide o mikropodniky a malé a stredné podniky vrátane startupov, a trhový podiel hospodárskeho subjektu, ktorý sa dopustil porušenia.

6. Orgány dohľadu nad trhom, ktoré ukladajú správne pokuty, oznámia uloženie uvedenej pokuty orgánom dohľadu nad trhom ostatných členských štátov prostredníctvom informačného a komunikačného systému uvedeného v článku 34 nariadenia (EÚ) 2019/1020.

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

8. 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 v daných členských štátoch na vnútroštátnej úrovni. Uplatňovanie takýchto pravidiel v uvedených členských štátoch má rovnocenný účinok.

9. Podľa okolností každého jednotlivého prípadu sa správne pokuty môžu ukladať spolu s akýmikoľvek inými nápravnými alebo reštriktívnymi opatreniami, ktoré uplatnia orgány dohľadu nad trhom na to isté porušenie.

10. Odchylne od odsekov 3 až 9 sa správne pokuty uvedené v daných odsekoch neuplatňujú na:

a) výrobcov považovaných za mikropodniky alebo malé podniky, pokiaľ ide o akékoľvek nedodržanie lehoty uvedenej v článku 14 ods. 2 písm. a) alebo článku 14 ods. 4 písm. a);

b) akékoľvek porušenie tohto nariadenia správcami softvéru s otvoreným zdrojovým kódom.

Článok 65

Žaloby v zastúpení

Na žaloby v zastúpení podané na hospodárske subjekty vo veci porušenia ustanovení tohto nariadenia, ktoré poškodzujú alebo môžu poškodiť kolektívne záujmy spotrebiteľov, sa vzťahuje smernica (EÚ) 2020/1828.

KAPITOLA VIII

PRECHODNÉ A ZÁVEREČNÉ USTANOVENIA

Článok 66

Zmena nariadenia (EÚ) 2019/1020

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

„72. Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 (*).

(*) Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti) (Ú. v. EÚ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).“

Článok 67

Zmena smernice (EÚ) 2020/1828

V prílohe I k smernici (EÚ) 2020/1828 sa dopĺňa tento bod:

„69. Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 (*).

(*) Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti) (Ú. v. EÚ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).“

Článok 68

Zmena nariadenia (EÚ) č. 168/2013

V časti C1 prílohy II k nariadeniu Európskeho parlamentu a Rady (EÚ) č. 168/2013 ([38]) sa v tabuľke dopĺňa táto položka:

„

16	18	ochrana vozidla pred kybernetickými útokmi		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

“

Článok 69

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 ako toto nariadenie, zostávajú v platnosti do 11. júna 2028, pokiaľ ich platnosť neuplynie pred týmto dátumom, alebo pokiaľ nie je v takýchto iných harmonizačných právnych predpisoch Únie uvedené inak, pričom v takom prípade zostávajú v platnosti tak, ako sa v daných právnych predpisoch uvádza.

2. Na produkty s digitálnymi prvkami, ktoré boli uvedené na trh pred 11. decembrom 2027 sa vzťahujú požiadavky stanovené v tomto nariadení len vtedy, ak sú tieto produkty od uvedeného dátumu predmetom podstatnej úpravy.

3. Odchylne od odseku 2 tohto článku sa povinnosti stanovené v článku 14 uplatňujú na všetky produkty s digitálnymi prvkami, ktoré patria do rozsahu pôsobnosti tohto nariadenia a boli uvedené na trh pred 11. decembrom 2027.

Článok 70

Hodnotenie a preskúmanie

1. Komisia do 11. decembra 2030 a potom každé štyri roky podáva Európskemu parlamentu a Rade správu o hodnotení a preskúmaní tohto nariadenia. Uvedené správy sa zverejnia.

2. Komisia do 11. septembra 2028 po konzultácii s agentúrou ENISA a sieťou jednotiek CSIRT podá Európskemu parlamentu a Rade správu, v ktorej posúdi účinnosť jednotnej oznamovacej platformy stanovenej v článku 16, ako aj vplyv uplatňovania dôvodov súvisiacich s kybernetickou bezpečnosťou uvedených v článku 16 ods. 2 jednotkami CSIRT určenými za koordinátorov na účinnosť jednotnej oznamovacej platformy, pokiaľ ide o včasné rozosielanie doručených oznámení iným príslušným jednotkám CSIRT.

Článok 71

Nadobudnutie účinnosti a uplatňovanie

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

([38]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 168/2013 z 15. januára 2013 o schvaľovaní a dohľade nad trhom dvoj- alebo trojkolesových vozidiel a štvorkoliek (Ú. v. EÚ L 60, 2.3.2013, s. 52).

2. Toto nariadenie sa uplatňuje od 11. decembra 2027.

Článok 14 sa však uplatňuje od 11. septembra 2026 a kapitola IV (články 35 až 51) sa uplatňuje od 11. júna 2026.

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

V Štrasburgu 23. októbra 2024

Za Európsky parlament	*Za Radu*
predsedníčka	*predseda*
R. METSOLA	ZSIGMOND B. P.

PRÍLOHA I

ZÁKLADNÉ POŽIADAVKY KYBERNETICKEJ BEZPEČNOSTI

Časť I Požiadavky kybernetickej bezpečnosti pre vlastností produktov s digitálnymi prvkami

1. Produkty s digitálnymi prvkami sa navrhujú, vyvíjajú a vyrábajú tak, aby sa zaistila primeraná úroveň ich kybernetickej bezpečnosti voči rizikám.

2. Produkty s digitálnymi prvkami sa na základe posúdenia kybernetickobezpečnostných rizík uvedeného v článku 13 ods. 2 a podľa potreby:

   a) sprístupňujú na trhu bez známych zneužiteľných zraniteľností;

   b) sprístupňujú na trhu v konfigurácii zabezpečenej na úrovni štandardného nastavenia, pokiaľ sa výrobca a komerčný používateľ v súvislosti s individualizovaným produktom s digitálnymi prvkami nedohodnú inak, vrátane možnosti vrátiť nastavenie produktu na pôvodné;

   c) zaisťujú, aby zraniteľnosti bolo možné riešiť bezpečnostnými aktualizáciami, prípadne aj automatickými bezpečnostnými aktualizáciami, ktoré sa inštalujú v primeranom čase aktiváciou podľa predvoleného nastavenia, s jasnou a ľahko použiteľnou možnosťou pre používateľa odmietnuť ich po oznámení o dostupných aktualizáciách a možnosti ich dočasného odkladu;

   d) zabezpečujú ochranu pred neoprávneným prístupom vhodnými mechanizmami kontroly, a to okrem iného aj systémami na správu overovania, identity alebo prístupu, a oznamujú, že došlo k možnému neoprávnenému prístupu;

   e) chránia dôvernosť uložených, vysielaných alebo inak spracúvaných osobných alebo iných údajov, napríklad šifrovaním príslušných neaktívnych alebo prenášaných údajov najmodernejšími mechanizmami, a použitím iných technických prostriedkov;

   f) chránia integritu uložených, vysielaných alebo inak spracúvaných osobných alebo iných údajov, príkazov, programov a konfigurácie proti akejkoľvek manipulácii alebo úprave, ktorú neschválil používateľ, a oznamujú prípady poškodenia;

   g) spracúvajú iba osobné alebo iné údaje, ktoré sú primerané, relevantné a obmedzené na to, čo je potrebné vo vzťahu k účelu produktu s digitálnymi prvkami (minimalizácia údajov), na ktorý bol určený;

   h) chránia dostupnosť hlavných a základných funkcií aj po incidente, a to aj prostredníctvom opatrení na zvýšenie odolnosti a zmiernenie útokov na vyradenie služby;

   i) minimalizujú nepriaznivý vplyv samotných produktov alebo pripojených zariadení na dostupnosť služieb iných zariadení alebo sietí;

   j) navrhujú, vyvíjajú a vyrábajú na obmedzenie plochy útoku vrátane externých rozhraní;

   k) navrhujú, vyvíjajú a vyrábajú na obmedzenie vplyvu incidentu s využitím vhodných mechanizmov a techník na zmiernenie zneužitia zraniteľností;

   l) poskytujú bezpečnostné informácie zaznamenávaním a monitorovaním príslušnej internej činnosti vrátane prístupu k údajom, službám alebo funkciám a ich zmene s mechanizmom odmietnutia (opt-out) pre používateľa;

   m) poskytujú používateľom možnosť bezpečne a jednoducho natrvalo odstrániť všetky údaje a nastavenia a ak takéto údaje možno preniesť do iných produktov alebo systémov, zabezpečiť, aby sa tak dialo bezpečne.

Časť II Požiadavky na riešenie zraniteľností

Výrobcovia produktov s digitálnymi prvkami:

1. identifikujú a dokumentujú zraniteľnosti a komponenty v produktoch s digitálnymi prvkami, a to aj zostavením zoznamu softvéru v obvykle používanom strojovo čitateľnom formáte, ktorý obsahuje závislosti produktu minimálne na najvyššej úrovni;

2. vo vzťahu k rizikám, ktorým sú vystavené produkty s digitálnymi prvkami, bezodkladne riešia a naprávajú zraniteľnosti, a to aj poskytovaním bezpečnostných aktualizácií; ak je to technicky možné, nové bezpečnostné aktualizácie sa poskytujú oddelene od aktualizácií funkcií;

3. vykonávajú účinné a pravidelné testy a kontroly zabezpečenia produktu s digitálnymi prvkami;

4. po sprístupnení bezpečnostnej aktualizácie poskytujú a zverejňujú informácie o opravených zraniteľnostiach vrátane opisu zraniteľností, informácie umožňujúce používateľom identifikovať postihnutý produkt s digitálnymi prvkami, vplyvy zraniteľností, ich závažnosť a jasné a prístupné informácie, ktoré používateľom pomôžu zraniteľnosti napraviť; keď sa výrobcovia domnievajú, že bezpečnostné riziká zverejnenia prevažujú nad bezpečnostnými prínosmi, v riadne odôvodnených prípadoch môžu odložiť zverejnenie informácií o vyriešenej zraniteľnosti dovtedy, kým používateľom neposkytnú možnosť použiť príslušnú záplatu;

5. zavádzajú a presadzujú politiku koordinovaného zverejňovania informácií o zraniteľnostiach;

6. prijímajú opatrenia na uľahčenie výmeny informácií o potenciálnych zraniteľnostiach svojho produktu s digitálnymi prvkami, ako aj komponentov tretích strán vo svojom produkte, a to aj poskytnutím kontaktnej adresy na oznamovanie zraniteľností zistených v produkte s digitálnymi prvkami;

7. zaistia mechanizmy bezpečnej distribúcie aktualizácií pre produkty s digitálnymi prvkami s cieľom zabezpečiť včasnú opravu zraniteľností alebo ich zmiernenie a aby sa v relevantnom prípade bezpečnostné aktualizácie uskutočňovali automaticky;

8. ak sú k dispozícii bezpečnostné aktualizácie na riešenie zistených bezpečnostných problémov, zabezpečujú ich bezodkladné šírenie a ak sa výrobca a komerčný používateľ nedohodli v súvislosti s individualizovaným produktom s digitálnymi prvkami inak, bezplatné šírenie sprievodných informačných správ s relevantnými informáciami pre používateľov, aj o možných potrebných krokoch.

PRÍLOHA II

INFORMÁCIE A NÁVOD PRE POUŽÍVATEĽA

K produktu s digitálnymi prvkami sa priloží aspoň:

1. meno, registrované obchodné meno alebo registrovaná ochranná známka výrobcu, poštová adresa, e-mailová adresa alebo iný digitálny kontakt, a ak je k dispozícii, aj webové sídlo, na ktorom možno výrobcu kontaktovať;
2. jednotné kontaktné miesto, na ktorom možno oznamovať a prijímať informácie o zraniteľnostiach produktu s digitálnymi prvkami a kde sa nachádza politika výrobcu pre koordinované oznámenia o zraniteľnostiach;
3. názov a typ produktu s digitálnymi prvkami a akékoľvek doplňujúce informácie umožňujúce jeho jedinečnú identifikáciu;
4. plánovaný účel produktu s digitálnymi prvkami vrátane bezpečnostného prostredia poskytovaného výrobcom, ako aj základné funkcie produktu a informácie o bezpečnostných vlastnostiach;
5. každá známa alebo predvídateľná okolnosť v súvislosti s použitím produktu s digitálnymi prvkami v súlade s jeho plánovaným účelom alebo za podmienok logicky predvídateľného nesprávneho použitia, ktoré môže viesť k významným kybernetickobezpečnostným rizikám;
6. v relevantnom prípade internetová adresa, na ktorej možno nájsť EÚ vyhlásenie o zhode;
7. druh technickej bezpečnostnej podpory, ktorú ponúka výrobca, a posledný deň obdobia podpory, počas ktorého môžu používatelia predpokladať riešenie zraniteľností a poskytovanie bezpečnostných aktualizácií;
8. podrobný návod alebo internetová adresa s odkazom na takýto podrobný návod a informácie o:
   a) opatreniach potrebných na zaistenie bezpečného používania produktu s digitálnymi prvkami pri prvom uvedení do prevádzky a počas celej jeho životnosti;
   b) možnom vplyve zmien produktu s digitálnymi prvkami na bezpečnosť údajov;
   c) postupe pri inštalácii bezpečnostných aktualizácií;
   d) bezpečnom vyradení produktu s digitálnymi prvkami z prevádzky vrátane informácií o možnosti bezpečného odstránenia údajov používateľa;
   e) spôsobe vypnutia predvoleného nastavenia umožňujúceho automatickú inštaláciu bezpečnostných aktualizácií, ako sa vyžaduje v časti I bode 2 písm. c) prílohy I;
   f) tom, čo potrebuje integrátor na splnenie základných požiadaviek kybernetickej bezpečnosti stanovených v prílohe I a o požiadavkách na dokumentáciu stanovených v prílohe VII, ak je produkt s digitálnymi prvkami určený na zabudovanie do iných produktov s digitálnymi prvkami.
9. Ak sa výrobca rozhodne sprístupniť zoznam softvéru používateľovi, informácie o tom, kde možno prístup k tomuto zoznamu softvéru získať.

PRÍLOHA III

DÔLEŽITÉ PRODUKTY S DIGITÁLNYMI PRVKAMI

Trieda I

1. Systémy správy identifikačných údajov a softvér a hardvér na správu privilegovaného prístupu vrátane čítačiek na autentifikáciu a kontrolu prístupu vrátane biometrických čítačiek.
2. Samostatné a zabudované prehliadače.
3. Správcovia hesiel.
4. Softvér na vyhľadávanie, odstraňovanie alebo uzatváranie škodlivého softvéru do karantény.
5. Produkty s digitálnymi prvkami s funkciou virtuálnej neverejnej siete (VPN).
6. Systémy správy sietí.
7. Systémy riadenia bezpečnostných informácií a udalostí (SIEM).
8. Správcovia spúšťania.
9. Infraštruktúra verejných kľúčov a softvér na vytváranie elektronických certifikátov.
10. Fyzické a virtuálne sieťové rozhrania.
11. Operačné systémy.
12. Smerovače, modemy určené na pripojenie k internetu a prepínače.
13. Mikroprocesory s bezpečnostnými funkciami.
14. Mikroradiče s bezpečnostnými funkciami.
15. Integrované obvody pre konkrétne aplikácie (ASIC) a logické hradlá programovateľné po výrobe (FPGA) s bezpečnostnými funkciami.
16. Virtuálni asistenti pre inteligentné domácnosti na všeobecné účely.
17. Produkty pre inteligentné domácnosti s bezpečnostnými funkciami vrátane inteligentných zámkov dverí, bezpečnostných kamier, systémov na monitorovanie detí a poplašných systémov.
18. Hračky pripojené na internet, na ktoré sa vzťahuje smernica Európskeho parlamentu a Rady 2009/48/ES ([1]) s funkciami na spoločenskú interakciu (napr. hovorenie alebo filmovanie) alebo s funkciami sledovania polohy.
19. Produkty, ktoré sa majú nosiť alebo byť umiestnené na ľudskom tele na účely zdravotného monitorovania (napríklad sledovanie) a na ktoré sa nevzťahuje nariadenie (EÚ) 2017/745 ani (EÚ) 2017/746, alebo produkty na nosenie na tele určené na použitie deťmi a pre deti.

Trieda II

1. Hypervízory a kontajnerové systémy režimu runtime, ktoré podporujú virtualizované spúšťanie operačných systémov a podobných prostredí.
2. Brány firewall, systémy na detekciu a prevenciu narušení.
3. Mikroprocesory odolné proti neoprávnenej manipulácii.
4. Mikroovládače odolné proti neoprávnenej manipulácii.

([1]) Smernica Európskeho parlamentu a Rady 2009/48/ES z 18. júna 2009 o bezpečnosti hračiek (Ú. v. EÚ L 170, 30.6.2009, s. 1).

PRÍLOHA IV

KRITICKÉ PRODUKTY S DIGITÁLNYMI PRVKAMI

1. Hardvérové zariadenia s bezpečnostnými schránkami.
2. Prístroje smart meter gateway v inteligentných meracích systémoch vymedzených v článku 2 bode 23 smernice Európskeho parlamentu a Rady (EÚ) 2019/944 ([1]) a iné zariadenia na vyššie bezpečnostné účely vrátane bezpečného kryptografického spracovania.
3. Čipové karty alebo podobné zariadenia s bezpečnostnými prvkami.

([1]) Smernica Európskeho parlamentu a Rady (EÚ) 2019/944 z 5. júna 2019 o spoločných pravidlách pre vnútorný trh s elektrinou a o zmene smernice 2012/27/EÚ (Ú. v. EÚ L 158, 14.6.2019, s. 125).

PRÍLOHA V

EÚ VYHLÁSENIE O ZHODE

EÚ vyhlásenie o zhode uvedené v článku 28 obsahuje všetky tieto informácie:

1. názov a druh a akékoľvek doplňujúce informácie umožňujúce jedinečnú identifikáciu produktu s digitálnymi prvkami;
2. meno a adresa výrobcu alebo jeho splnomocneného zástupcu;
3. vyhlásenie o tom, že EÚ vyhlásenie o zhode sa vydáva na výhradnú zodpovednosť poskytovateľa;
4. predmet vyhlásenia (identifikácia produktu s digitálnymi prvkami umožňujúcimi dosledovateľnosť, ktorej súčasťou môže byť podľa potreby aj fotografia);
5. vyhlásenie o tom, že predmet opísaný v uvedenom vyhlásení sa zhoduje s príslušnými požiadavkami harmonizačných právnych predpisov Únie;
6. odkazy na všetky použité príslušné harmonizované normy alebo inú spoločnú špecifikáciu alebo certifikáciu kybernetickej bezpečnosti, v súvislosti s ktorými sa zhoda vyhlasuje;
7. prípadne meno a identifikačné číslo notifikovanej osoby, opis použitého postupu posudzovania zhody a identifikácia vydaného certifikátu;
8. doplňujúce informácie:

   podpis za a v mene:

   (miesto a dátum vydania):

   (meno, funkcia) (podpis):

PRÍLOHA VI

ZJEDNODUŠENÉ EÚ VYHLÁSENIE O ZHODE

Zjednodušené EÚ vyhlásenie o zhode uvedené v článku 13 ods. 20 má takéto znenie:

… [meno výrobcu] týmto vyhlasuje, že produkt s digitálnymi prvkami typu … [označenie typu produktu s digitálnym prvkom] je v súlade s nariadením (EÚ) 2024/2847 ([1]).

Úplné znenie EÚ vyhlásenia o zhode je k dispozícii na tejto internetovej adrese: …

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

PRÍLOHA VII

OBSAH TECHNICKEJ DOKUMENTÁCIE

Technická dokumentácia uvedená v článku 31 obsahuje aspoň tieto informácie o príslušnom produkte s digitálnymi prvkami:

1. všeobecný opis produktu s digitálnymi prvkami vrátane:
   a) jeho plánovaného účelu;
   b) verzií softvéru, ktoré majú vplyv na súlad so základnými požiadavkami kybernetickej bezpečnosti;
   c) ak je produkt s digitálnymi prvkami hardvérovým produktom, fotografií alebo ilustrácií jeho vonkajšieho vzhľadu, označenia a vnútornej štruktúry;
   d) informácií pre používateľa a návodu uvedených v prílohe II;
2. opis riešenia, vývoja a výroby produktu s digitálnymi prvkami a postupov riešenia zraniteľností vrátane:
   a) nevyhnutných informácií o návrhu a vývoji produktu s digitálnymi prvkami, v relevantnom prípade aj výkresov, schém a opisu architektúry systému s vysvetlením vzájomných vzťahov alebo prepojenia softvérových komponentov a ich zapojenia do celkového spracovania;
   b) nevyhnutných informácií o postupoch riešenia zraniteľností zavedených výrobcom a špecifikácií týchto postupov vrátane zoznamu softvéru, politiky koordinovaného zverejňovania informácií o zraniteľnostiach, dôkazu o poskytnutí kontaktnej adresy na ohlasovanie zraniteľností a opisu technických riešení zvolených na bezpečnú distribúciu aktualizácií;
   c) nevyhnutných informácií o postupoch výroby a monitorovania produktu s digitálnymi prvkami, ich špecifikácií a validácie uvedených postupov;
3. posúdenie kybernetickobezpečnostných rizík, proti ktorým je produkt s digitálnymi prvkami navrhnutý, vyvinutý, vyrobený, dodávaný a udržiavaný podľa článku 13 vrátane spôsobu uplatňovania základných požiadaviek kybernetickej bezpečnosti stanovených v časti I prílohy I;
4. relevantné informácie zohľadnené pri určovaní obdobia podpory podľa článku 13 ods. 8 pre produkt s digitálnymi prvkami;
5. zoznam harmonizovaných noriem uplatnených plne alebo čiastočne, na ktoré boli uverejnené odkazy v *Úradnom vestníku Európskej únie*, spoločné špecifikácie podľa článku 27 tohto nariadenia alebo európske schémy certifikácie kybernetickej bezpečnosti prijaté podľa nariadenia (EÚ) 2019/881 a v zmysle článku 27 ods. 8 tohto nariadenia, a ak neboli uplatnené uvedené harmonizované normy, spoločné špecifikácie ani európske schémy certifikácie kybernetickej bezpečnosti, opisy riešení prijatých na účely splnenia základných požiadaviek kybernetickej bezpečnosti stanovených v častiach I a II prílohy I vrátane zoznamu ostatných uplatnených relevantných technických špecifikácií; v prípade čiastočného uplatnenia harmonizovaných noriem, spoločných špecifikácií alebo európskych schém certifikácie kybernetickej bezpečnosti sa v technickej dokumentácii špecifikujú časti, ktoré boli uplatnené;
6. správy o skúškach vykonaných na overenie zhody produktu s digitálnymi prvkami a postupov riešenia zraniteľností s uplatniteľnými základnými požiadavkami kybernetickej bezpečnosti stanovenými v častiach I a II prílohy I;
7. kópia EÚ vyhlásenia o zhode;
8. v relevantnom prípade zoznam softvéru na základe odôvodnenej žiadosti orgánu dohľadu nad trhom, ak je to potrebné na to, aby bol tento orgán schopný skontrolovať súlad so základnými požiadavkami kybernetickej bezpečnosti stanovenými v prílohe I.

PRÍLOHA VIII

POSTUPY POSUDZOVANIA ZHODY

Časť I Postup posudzovania zhody na základe vnútornej kontroly (podľa modulu A)

1. Vnútorná kontrola je postup posudzovania zhody, ktorým si výrobca plní povinnosti stanovené v bodoch 2, 3 a 4 tejto časti a na svoju výhradnú zodpovednosť zaručuje a vyhlasuje, že produkty s digitálnymi prvkami vyhovujú všetkým základným požiadavkám kybernetickej bezpečnosti stanoveným v časti I prílohy I a že výrobca spĺňa základné požiadavky kybernetickej bezpečnosti stanovené v časti II prílohy I.

2. Výrobca vypracuje technickú dokumentáciu opísanú v prílohe VII.

3. Návrh, vývoj, výroba a riešenie zraniteľností produktov s digitálnymi prvkami

   Výrobca prijme všetky opatrenia potrebné na to, aby sa postupmi navrhovania, vývoja, výroby a riešenia zraniteľností a ich monitorovaním zabezpečil súlad vyrábaných alebo vyvíjaných produktov s digitálnymi prvkami a postupov zavedených výrobcom so základnými požiadavkami kybernetickej bezpečnosti stanovenými v častiach I a II prílohy I.

4. Označenie zhody a vyhlásenie o zhode

   4.1. Výrobca umiestňuje označenie CE na každý jednotlivý produkt s digitálnymi prvkami, ktorý vyhovuje príslušným požiadavkám stanoveným v tomto nariadení.

   4.2. Výrobca vypracuje písomné EÚ vyhlásenie o zhode pre každý produkt s digitálnymi prvkami v súlade s článkom 28 a uchováva ho spolu s technickou dokumentáciou k dispozícii pre vnútroštátne orgány 10 rokov po uvedení produktu s digitálnymi prvkami na trh alebo počas obdobia podpory, podľa toho, čo trvá dlhšie. V EÚ vyhlásení o zhode sa identifikuje produkt s digitálnymi prvkami, pre ktorý bolo vyhlásenie vypracované. Príslušným orgánom sa poskytuje kópia EÚ vyhlásenia o zhode na požiadanie.

5. Splnomocnení zástupcovia

   Povinnosti výrobcu stanovené v bode 4 môžu byť v jeho mene a na jeho zodpovednosť splnené jeho splnomocneným zástupcom za predpokladu, že príslušné povinnosti sú uvedené v splnomocnení.

Časť II EÚ skúška typu (podľa modulu B)

1. EÚ skúška typu je súčasťou postupu posudzovania zhody, pri ktorej notifikovaná osoba preskúma technický návrh a vývoj produktu s digitálnymi prvkami a postupy riešenia zraniteľností zavedené výrobcom, a potvrdí, že produkt s digitálnymi prvkami vyhovuje základným požiadavkám kybernetickej bezpečnosti stanoveným v časti I prílohy I a že výrobca spĺňa základné požiadavky kybernetickej bezpečnosti stanovené v časti II prílohy I.

2. EÚ skúška typu sa vykonáva posúdením primeranosti technického návrhu a vývoja produktu s digitálnymi prvkami preskúmaním technickej dokumentácie a podpornej dokumentácie uvedenými v bode 3 a preskúmaním vzoriek jednej alebo viacerých kritických častí produktu (kombinácia typovej výroby a typového návrhu).

3. Žiadosť o EÚ skúšku typu predkladá výrobca jedinej notifikovanej osobe podľa vlastného výberu.

   Žiadosť obsahuje:

   3.1. meno a adresu výrobcu a ak žiadosť podáva jeho splnomocnený zástupca, meno a adresu tohto splnomocneného zástupcu;

   3.2. písomné vyhlásenie o tom, že rovnaká žiadosť nebola podaná inej notifikovanej osobe,

   3.3. technickú dokumentáciu, ktorá má umožniť posúdenie zhody produktu s digitálnymi prvkami s uplatniteľnými základnými požiadavkami kybernetickej bezpečnosti stanovenými v časti I prílohy I a postupov riešenia zraniteľností zavedených výrobcom stanovených v časti II prílohy I a musí obsahovať primeranú analýzu a posúdenie rizík; v technickej dokumentácii sa uvedú príslušné požiadavky a zahrnie sa do nej, ak je to z hľadiska posudzovania relevantné, návrh, výroba a používanie produktu s digitálnymi prvkami; technická dokumentácia obsahuje vždy, keď je to potrebné, aspoň prvky uvedené v prílohe VII;

3.4. podporné dôkazy o primeranosti technického návrhu, riešení vývoja a postupov riešenia zraniteľností; v týchto podporných dôkazoch sa uvádzajú všetky dokumenty, ktoré sa použili, predovšetkým v tých prípadoch, keď sa príslušné harmonizované normy alebo technické špecifikácie nepoužili v plnom rozsahu; podporné dôkazy v prípade potreby zahŕňajú výsledky skúšok, ktoré vykonalo vhodné laboratórium výrobcu alebo iné skúšobné laboratórium v jeho mene a na jeho zodpovednosť.

4. Notifikovaná osoba:

4.1. preskúma technickú dokumentáciu a podporné dôkazy s cieľom posúdiť primeranosť technického návrhu a vývoja produktu s digitálnymi prvkami vzhľadom na základné požiadavky kybernetickej bezpečnosti stanovené v časti I prílohy I a postupy riešenia zraniteľností zavedené výrobcom vzhľadom na základné požiadavky kybernetickej bezpečnosti stanovené v časti II prílohy I;

4.2. overí, či vzorky boli vyvinuté alebo vyrobené v súlade s technickou dokumentáciou, a určí prvky, ktoré boli navrhnuté a vyvinuté v súlade s uplatniteľnými ustanoveniami relevantných harmonizovaných noriem alebo technickými špecifikáciami, ako aj prvky, ktoré boli navrhnuté a vyvinuté bez uplatnenia príslušných ustanovení týchto noriem;

4.3. vykoná alebo dá vykonať vhodné preskúmania a skúšky s cieľom skontrolovať, že v prípade, keď sa výrobca pri požiadavkách stanovených v prílohe I rozhodol uplatniť riešenia uvedené v príslušných harmonizovaných normách alebo technických špecifikáciách, boli uplatnené správne;

4.4. vykoná alebo dá vykonať vhodné preskúmania a skúšky s cieľom skontrolovať, že v prípade, keď pri požiadavkách stanovených v prílohe I riešenia uvedené v príslušných harmonizovaných normách alebo technických špecifikáciách neboli uplatnené, riešenia prijaté výrobcom spĺňajú zodpovedajúce základné požiadavky kybernetickej bezpečnosti;

4.5. dohodne s výrobcom miesto, kde sa vykonajú skúšky a testy.

5. Notifikovaná osoba vypracuje hodnotiacu správu, v ktorej zaznamená činnosti vykonané v súlade s bodom 4 a ich výsledky. Bez ohľadu na svoje povinnosti voči notifikujúcim orgánom notifikovaná osoba sprístupňuje úplný alebo čiastočný obsah uvedenej správy iba so súhlasom výrobcu.

6. Ak typ a postupy riešenia zraniteľností spĺňajú základné požiadavky kybernetickej bezpečnosti stanovené v prílohe I, notifikovaná osoba vydá výrobcovi certifikát EÚ skúšky typu. Certifikát obsahuje meno a adresu výrobcu, závery preskúmania, podmienky jeho platnosti (ak existujú) a údaje potrebné na určenie schváleného typu a postupov riešenia zraniteľností. K certifikátu možno pripojiť jednu alebo viac príloh.

Certifikát a jeho prílohy obsahujú všetky príslušné informácie, ktoré umožňujú vyhodnotenie zhody vyrobených alebo vyvinutých produktov s digitálnymi prvkami s preskúmaným typom a postupmi riešenia zraniteľností a umožňujú kontrolu za prevádzky.

Ak typ a postupy riešenia zraniteľností nespĺňajú uplatniteľné základné požiadavky kybernetickej bezpečnosti stanovené v prílohe I, notifikovaná osoba odmietne vydať certifikát EÚ skúšky typu a náležite o tom informuje žiadateľa, pričom uvedie podrobné dôvody odmietnutia.

7. Notifikovaná osoba sa oboznámi so všetkými zmenami v súvislosti so všeobecne uznávaným stavom techniky, ktoré naznačujú, že schválený typ a postupy riešenia zraniteľností už nemusia spĺňať uplatniteľné základné požiadavky kybernetickej bezpečnosti stanovené v prílohe I, a stanoví, či si takéto zmeny vyžadujú ďalšie prešetrenie. Ak áno, notifikovaná osoba o tom informuje výrobcu.

Výrobca informuje notifikovanú osobu, ktorá má technickú dokumentáciu týkajúcu sa certifikátu EÚ skúšky typu, o všetkých úpravách schváleného typu a postupoch riešenia zraniteľností, ktoré môžu ovplyvniť zhodu so základnými požiadavkami kybernetickej bezpečnosti stanovenými v prílohe I, alebo s podmienkami platnosti certifikátu. Takéto zmeny si vyžadujú dodatočné schválenie vo forme dodatku k pôvodnému certifikátu EÚ skúšky typu.

8. Notifikovaná osoba vykonáva pravidelné audity s cieľom zabezpečiť primerané vykonávanie postupov riešenia zraniteľností stanovených v časti II prílohy I.

9. Každá notifikovaná osoba informuje svoje notifikujúce orgány o certifikátoch EÚ skúšky typu a ich dodatkoch, ktoré vydala alebo zrušila, a pravidelne alebo na ich žiadosť poskytuje svojim notifikujúcim orgánom zoznam certifikátov a dodatkov k nim, ktoré boli zamietnuté, pozastavené alebo inak obmedzené.

   Každá notifikovaná osoba informuje ostatné notifikované osoby o certifikátoch EÚ skúšky typu a akýchkoľvek dodatkoch k nim, ktoré zamietla, odňala, pozastavila alebo inak obmedzila, a na požiadanie ich informuje o certifikátoch a dodatkoch k nim, ktoré vydala.

   Komisia, členské štáty a ostatné notifikované osoby môžu na žiadosť získať kópiu certifikátov EÚ skúšky typu a akýchkoľvek dodatkov k nim. Komisia a členské štáty môžu na požiadanie získať kópiu technickej dokumentácie a výsledkov skúšok, ktoré vykonala notifikovaná osoba. Do uplynutia platnosti certifikátu uchováva notifikovaná osoba kópiu certifikátu EÚ skúšky typu, jeho príloh a dodatkov, ako aj technické podklady vrátane dokumentácie poskytnutej zo strany výrobcu.

10. Výrobca uchováva kópiu certifikátu EÚ skúšky typu, jeho príloh a dodatkov k nemu spolu s technickou dokumentáciou k dispozícii pre vnútroštátne orgány 10 rokov po uvedení produktu s digitálnymi prvkami na trh alebo počas obdobia podpory, podľa toho, čo trvá dlhšie.

11. Splnomocnený zástupca výrobcu môže podať žiadosť uvedenú v bode 3 a plniť povinnosti stanovené v bodoch 7 a 10 za predpokladu, že príslušné povinnosti sú uvedené v splnomocnení.

Časť III Zhoda s typom na základe vnútornej kontroly výroby (podľa modulu C)

1. Zhoda s typom na základe na vnútornej kontrole výroby je tou časťou postupu posudzovania zhody, v ktorej výrobca plní povinnosti stanovené v bodoch 2 a 3 tejto časti a zabezpečuje a vyhlasuje, že dotknuté produkty s digitálnymi prvkami sú v zhode s typom opísaným v certifikáte EÚ skúšky typu a spĺňajú základné požiadavky kybernetickej bezpečnosti stanovené v časti I prílohy I a že výrobca spĺňa základné požiadavky kybernetickej bezpečnosti stanovené v časti II prílohy I.

2. Výroba

   Výrobca prijme všetky opatrenia potrebné na to, aby sa výrobou a jej monitorovaním zabezpečila zhoda vyrobených produktov s digitálnymi prvkami so schváleným typom opísaným v certifikáte EÚ skúšky typu a so základnými požiadavkami kybernetickej bezpečnosti stanovenými v časti I prílohy I a zabezpečuje, aby výrobca spĺňal základné požiadavky kybernetickej bezpečnosti stanovené v časti II prílohy I.

3. Označenie zhody a vyhlásenie o zhode

   3.1. Výrobca umiestňuje označenie CE na každý jednotlivý produkt s digitálnymi prvkami, ktorý je v súlade s typom opísaným v certifikáte EÚ skúšky typu a spĺňa príslušné požiadavky stanovené v tomto nariadení.

   3.2. Pre model produktu vydá výrobca písomné vyhlásenie o zhode, ktoré uchováva k dispozícii pre vnútroštátne orgány 10 rokov od uvedenia produktu s digitálnymi prvkami na trh alebo počas obdobia podpory podľa toho, čo trvá dlhšie. Vo vyhlásení o zhode sa uvedie model produktu, pre ktorý bolo vydané. Kópiu vyhlásenia o zhode na požiadanie sprístupní príslušným orgánom.

4. Splnomocnený zástupca

   Povinnosti výrobcu stanovené v bode 3 môžu byť v jeho mene a na jeho zodpovednosť splnené jeho splnomocneným zástupcom za predpokladu, že príslušné povinnosti sú uvedené v splnomocnení.

Časť IV Zhoda na základe plného zabezpečenia kvality (podľa modulu H)

1. Zhoda na základe plného zabezpečenia kvality je postup posudzovania zhody, ktorým si výrobca splní povinnosti stanovené v bodoch 2 a 5 tejto časti a na svoju výhradnú zodpovednosť zaručí a vyhlási, že dotknuté produkty s digitálnymi prvkami alebo dotknuté kategórie produktov vyhovujú základným požiadavkám kybernetickej bezpečnosti stanoveným v časti I prílohy I a že postupy riešenia zraniteľností zavedené výrobcom spĺňajú požiadavky stanovené v časti II prílohy I.

2. Návrh, vývoj, výroba a riešenie zraniteľností produktov s digitálnymi prvkami

Výrobca prevádzkuje schválený systém kvality špecifikovaný v bode 3 pre návrh, vývoj, finálnu kontrolu a testovanie dotknutých produktov s digitálnymi prvkami a riešenie zraniteľností, udržiava jeho účinnosť počas celého obdobia podpory a podrobuje ho dohľadu tak, ako je špecifikovaný v bode 4.

3. Systém kvality

3.1. Výrobca podáva žiadosť o posúdenie svojho systému kvality pre príslušné produkty s digitálnymi prvkami notifikovanej osobe podľa vlastného výberu.

Žiadosť obsahuje:

a) meno a adresu výrobcu a v prípade, že žiadosť podáva jeho splnomocnený zástupca, meno a adresu tohto splnomocneného zástupcu;

b) technickú dokumentáciu jedného modelu z každej kategórie produktov s digitálnymi prvkami, ktoré sa majú vyrábať alebo vyvíjať; technická dokumentácia v relevantnom prípade obsahuje aspoň prvky uvedené v prílohe VII;

c) dokumentáciu o systéme kvality; a

d) písomné vyhlásenie, že tá istá žiadosť nebola podaná inej notifikovanej osobe.

3.2. Systém kvality zabezpečuje súlad produktov s digitálnymi prvkami so základnými požiadavkami kybernetickej bezpečnosti stanovenými v časti I prílohy I a súlad postupov riešenia zraniteľností zavedených výrobcom s požiadavkami stanovenými v časti II prílohy I.

Všetky prvky, požiadavky a opatrenia prijaté výrobcom sa systematicky a usporiadane zdokumentujú vo forme písomných zásad, postupov a návodu. Táto dokumentácia systému kvality umožňuje dôsledný výklad programov, plánov, príručiek a záznamov týkajúcich sa kvality.

Musí obsahovať najmä primeraný opis:

a) cieľov kvality a organizačnej štruktúry, povinností a právomocí manažmentu vzhľadom na kvalitu návrhu, vývoja a produktov a riešenie zraniteľností;

b) technických špecifikácií pre navrhovanie a vývoj vrátane noriem, ktoré sa budú uplatňovať, a ak sa príslušné harmonizované normy alebo technické špecifikácie nebudú uplatňovať v plnom rozsahu, prostriedkov, ktoré sa použijú na zabezpečenie splnenia základných požiadaviek kybernetickej bezpečnosti stanovených v časti I prílohy I, ktoré sa na produkty s digitálnymi prvkami vzťahujú;

c) procesných špecifikácií vrátane noriem, ktoré sa budú uplatňovať, a ak sa príslušné harmonizované normy alebo technické špecifikácie nebudú uplatňovať v plnom rozsahu, prostriedkov, ktoré sa použijú na zabezpečenie splnenia základných požiadaviek kybernetickej bezpečnosti stanovených v časti II prílohy I, ktoré sa vzťahujú na výrobcu;

d) kontroly návrhu a vývoja, ako aj techník overovania návrhu a vývoja, postupov a systematických činností, ktoré sa použijú pri navrhovaní a vývoji produktov s digitálnymi prvkami v dotknutej kategórii produktov;

e) zodpovedajúcich techník, postupov a systematických činností výroby, kontroly a zabezpečovania kvality, ktoré sa budú používať;

f) overovaní a skúšok, ktoré sa budú vykonávať pred výrobou, počas výroby a po nej, vrátane časových intervalov, v ktorých sa budú vykonávať;

g) záznamov o kvalite, ako sú správy o kontrolách a údaje o skúškach, kalibračné údaje a správy o kvalifikácii dotknutých zamestnancov;

h) prostriedkov monitorovania požadovanej kvality návrhu a produktu a účinnej prevádzky systému kvality.

3.3. Notifikovaná osoba posúdi systém kvality s cieľom určiť, či spĺňa požiadavky uvedené v bode 3.2.

V prípade prvkov systému kvality, ktoré sú v zhode s príslušnými špecifikáciami vnútroštátnej normy, ktorou sa vykonáva príslušná harmonizovaná norma alebo technické špecifikácie, predpokladá zhodu s týmito požiadavkami.

Okrem skúseností v oblasti systémov riadenia kvality musí mať audítorský tím aspoň jedného člena so skúsenosťami v posudzovaní príslušnej oblasti produktov a dotknutej technológie produktov a musí byť oboznámený s príslušnými požiadavkami stanovenými v tomto nariadení. Súčasťou auditu je hodnotiaca návšteva v priestoroch výrobcu, pokiaľ takéto priestory existujú. Audítorský tím preskúmava technickú dokumentáciu uvedenú v bode 3.1 písm. b) s cieľom overiť schopnosť výrobcu identifikovať príslušné požiadavky stanovené v tomto nariadení a vykonať potrebné preskúmania na zabezpečenie súladu produktu s digitálnymi prvkami s uvedenými požiadavkami.

Rozhodnutie sa oznámi výrobcovi alebo jeho splnomocnenému zástupcovi.

V oznámení sa uvedú závery auditu a odôvodnené rozhodnutie o posúdení.

3.4. Výrobca sa zaväzuje, že splní povinnosti vyplývajúce zo systému kvality tak, ako bol schválený, a bude ho udržiavať tak, aby zostal primeraný a účinný.

3.5. Výrobca informuje notifikovanú osobu, ktorá systém kvality schválila, o každej zamýšľanej zmene tohto systému.

Notifikovaná osoba vyhodnotí všetky navrhované zmeny a rozhodne, či upravený systém kvality bude naďalej spĺňať požiadavky uvedené v bode 3.2, alebo je potrebné opätovné posúdenie.

Svoje rozhodnutie oznámi výrobcovi. V oznámení uvedie závery preskúmania a odôvodnené rozhodnutie o posúdení.

4. Dohľad, za ktorý zodpovedá notifikovaná osoba

4.1. Cieľom dohľadu je zabezpečiť, aby si výrobca riadne plnil povinnosti vyplývajúce zo schváleného systému kvality.

4.2. Na účely posúdenia umožní výrobca notifikovanej osobe vstup do priestorov určených na navrhovanie, vývoj, výrobu, kontrolu, testovanie a skladovanie a poskytne jej všetky potrebné informácie, najmä:

a) dokumentáciu systému kvality;

b) záznamy o kvalite, ako sú stanovené v časti systému kvality pre navrhovanie, ako sú napríklad výsledky analýz, výpočtov a skúšok;

c) záznamy o kvalite, ako sú stanovené v časti systému kvality pre výrobu, napríklad správy o kontrolách a údaje zo skúšok, kalibračné údaje a správy o kvalifikácii dotknutých zamestnancov.

4.3. Notifikovaná osoba vykonáva pravidelné audity s cieľom zabezpečiť, aby výrobca udržiaval a uplatňoval systém kvality, a výrobcovi poskytuje správu o audite.

5. Označenie zhody a vyhlásenie o zhode

5.1. Na každý jednotlivý produkt s digitálnymi prvkami, ktorý spĺňa požiadavky stanovené v časti I prílohy I, umiestni výrobca označenie CE a na zodpovednosť notifikovanej osoby uvedenej v bode 3.1 jej identifikačné číslo.

5.2. Výrobca vydá pre každý model produktu písomné vyhlásenie o zhode, ktoré uchováva k dispozícii pre vnútroštátne orgány 10 rokov od uvedenia produktu s digitálnymi prvkami na trh alebo počas obdobia podpory podľa toho, čo trvá dlhšie. Vo vyhlásení o zhode sa uvedie model produktu, pre ktorý bolo vydané.

Kópiu vyhlásenia o zhode na požiadanie sprístupní príslušným orgánom.

6. Najmenej 10 rokov od uvedenia produktu s digitálnymi prvkami na trh alebo počas obdobia podpory podľa toho, čo trvá dlhšie, uchováva výrobca pre potreby vnútroštátnych orgánov:

a) technickú dokumentáciu uvedenú v bode 3.1;

b) dokumentáciu systému kvality uvedenú v bode 3.1;

c) zmenu uvedenú v bode 3.5 tak, ako je schválená;

d) rozhodnutia a správy notifikovanej osoby uvedené v bodoch 3.5 a 4.3.

7. Každá notifikovaná osoba informuje svoje notifikujúce orgány o schváleniach systému kvality, ktoré vydala alebo odňala, a pravidelne alebo na požiadanie sprístupňuje svojim notifikujúcim orgánom zoznam zamietnutých, pozastavených alebo inak obmedzených schválení systémov kvality.

Každá notifikovaná osoba informuje ostatné notifikované osoby o zamietnutých, pozastavených alebo odňatých schválení systémov kvality a na požiadanie aj o vydaných schváleniach systémov kvality.

8. Splnomocnený zástupca

Povinnosti výrobcu stanovené v bodoch 3.1, 3.5, 5 a 6 môže v jeho mene a na jeho zodpovednosť splniť jeho splnomocnený zástupca za predpokladu, že príslušné povinnosti sú uvedené v splnomocnení.

K tomuto aktu bolo urobené vyhlásenie, ktoré možno nájsť v Ú. v. EÚ C, 2024/6786, 20.11.2024, ELI: http://data.europa.eu/eli/C/2024/6786/oj.