SMERNICE

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)

(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 Európskej centrálnej banky ([1]),

so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru ([2]),

po porade s Výborom regiónov,

konajúc v súlade s riadnym legislatívnym postupom ([3]),

keďže:

(1) Cieľom smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 ([4]) bolo budovať kapacity v oblasti kybernetickej bezpečnosti v celej Únii, zmierňovať hrozby pre siete a informačné systémy používané na poskytovanie základných služieb v kľúčových odvetviach a zabezpečiť kontinuitu takýchto služieb pri riešení incidentov, a tým prispievať k bezpečnosti Únie a účinnému fungovaniu jej hospodárstva a spoločnosti.

(2) Od nadobudnutia účinnosti smernice (EÚ) 2016/1148 sa dosiahol významný pokrok pri zvyšovaní úrovne kybernetickej odolnosti Únie. Preskúmanie uvedenej smernice ukázalo, že slúžila ako katalyzátor inštitucionálneho a regulačného prístupu ku kybernetickej bezpečnosti v Únii a pripravila pôdu pre dôležitú zmenu v zmýšľaní. Uvedenou smernicou sa zabezpečilo dokončenie vnútroštátnych rámcov v oblasti bezpečnosti sietí a informačných systémov stanovením národných stratégií v oblasti bezpečnosti sietí a informačných systémov a stanovením vnútroštátnych kapacít a vykonávaním regulačných opatrení vzťahujúcich sa na kľúčové infraštruktúry a subjekty identifikované v každom členskom štáte. Smernica (EÚ) 2016/1148 prispela aj k spolupráci na úrovni Únie zriadením skupiny pre spoluprácu a siete národných jednotiek pre riešenie počítačových bezpečnostných incidentov. Bez ohľadu na tieto úspechy sa pri preskúmaní smernice (EÚ) 2016/1148 odhalili prirodzené nedostatky, ktoré jej bránia účinne riešiť súčasné a vznikajúce výzvy v oblasti kybernetickej bezpečnosti.

(3) Siete a informačné systémy sa spolu s rýchlou digitálnou transformáciou a prepojenosťou spoločnosti, a to aj pri cezhraničných výmenách, stali bežnou súčasťou každodenného života. Uvedený vývoj viedol k nárastu kybernetických hrozieb a prináša nové výzvy, ktoré si vyžadujú prispôsobené, koordinované a inovatívne reakcie vo všetkých členských štátoch. Počet, rozsah, sofistikovanosť, frekvencia a vplyv incidentov sa zvyšujú a pre fungovanie sietí a informačných systémov predstavujú veľkú hrozbu. Vo výsledku môžu incidenty zabraňovať realizácii ekonomických aktivít na vnútornom trhu, spôsobovať finančné straty, narúšať dôveru používateľov a spôsobovať značné škody spoločnosti a hospodárstvu Únie. Pripravenosť a účinnosť v oblasti kybernetickej bezpečnosti sú

([1]) Ú. v. EÚ C 233, 16.6.2022, s. 22.
([2]) Ú. v. EÚ C 286, 16.7.2021, s. 170.
([3]) Pozícia Európskeho parlamentu z 10. novembra 2022 (zatiaľ neuverejnená v úradnom vestníku) a rozhodnutie Rady z 28. novembra 2022.
([4]) Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194, 19.7.2016, s. 1).

preto teraz pre riadne fungovanie vnútorného trhu dôležitejšie ako kedykoľvek predtým. Kybernetická bezpečnosť je navyše kľúčovým faktorom, ktorý mnohým kritickým odvetviam umožňuje úspešne zvládnuť digitálnu transformáciu a plne využívať hospodárske, sociálne a udržateľné prínosy digitalizácie.

(4) Právnym základom smernice (EÚ) 2016/1148 bol článok 114 Zmluvy o fungovaní Európskej únie (ďalej len „ZFEÚ“), ktorého cieľom je vytvorenie a fungovanie vnútorného trhu posilnením opatrení na aproximáciu vnútroštátnych pravidiel. Požiadavky na kybernetickú bezpečnosť uložené subjektom poskytujúcim služby alebo vykonávajúcim činnosti, ktoré sú ekonomicky významné, sa v jednotlivých členských štátoch značne líšia, pokiaľ ide o typ požiadaviek, ich úroveň podrobnosti a metódu dohľadu. Uvedené rozdiely spôsobujú dodatočné náklady a subjektom, ktoré ponúkajú tovar alebo služby cezhranične, spôsobujú ťažkosti. Požiadavky jedného členského štátu, ktoré sa líšia od požiadaviek iného členského štátu alebo sú s nimi dokonca v rozpore, môžu takéto cezhraničné činnosti podstatne ovplyvniť. Okrem toho môžu mať nedostatočne navrhnuté alebo vykonávané požiadavky na kybernetickú bezpečnosť v jednom členskom štáte vplyv na úroveň kybernetickej bezpečnosti v iných členských štátoch, najmä vzhľadom na intenzitu cezhraničných výmen. Preskúmanie smernice (EÚ) 2016/1148 ukázalo, že v jej vykonávaní členskými štátmi existujú veľké rozdiely, a to aj pokiaľ ide o jej rozsah pôsobnosti, ktorého určenie bolo do veľmi veľkej miery ponechané na voľnom uvážení členských štátov. Smernica (EÚ) 2016/1148 poskytla členským štátom veľmi široký priestor na voľné konanie, aj pokiaľ ide o vykonávanie povinností týkajúcich sa bezpečnosti a oznamovania incidentov, ktoré sú v nej stanovené. Uvedené povinnosti boli preto na úrovni členských štátov vykonávané značne odlišne. Podobné rozdiely existujú vo vykonávaní ustanovení smernice (EÚ) 2016/1148 týkajúcich sa dohľadu a presadzovania.

(5) Všetky tieto rozdiely spôsobujú fragmentáciu vnútorného trhu a môžu mať škodlivý vplyv na jeho fungovanie, a to najmä pokiaľ ide o cezhraničné poskytovanie služieb a úroveň kybernetickej odolnosti, v dôsledku uplatňovania rôznych opatrení. Uvedené rozdiely by v konečnom dôsledku mohli viesť k väčšej zraniteľnosti niektorých členských štátov voči kybernetickým hrozbám s možnými účinkami presahovania v celej Únii. Cieľom tejto smernice je odstrániť takéto veľké rozdiely medzi členskými štátmi, a to najmä stanovením minimálnych pravidiel týkajúcich sa fungovania koordinovaného regulačného rámca, stanovením mechanizmov účinnej spolupráce medzi zodpovednými orgánmi v každom členskom štáte, aktualizáciou zoznamu odvetví a činností podliehajúcich povinnostiam v oblasti kybernetickej bezpečnosti a poskytnutím účinných nápravných opatrení a opatrení presadzovania práva, ktoré sú kľúčové pre účinné presadzovanie týchto povinností. Smernica (EÚ) 2016/1148 by sa preto mala zrušiť a nahradiť touto smernicou.

(6) Zrušením smernice (EÚ) 2016/1148 by sa rozsah uplatňovania podľa odvetví mal rozšíriť na väčšiu časť hospodárstva, aby boli komplexne pokryté odvetvia a služby, ktoré majú zásadný význam pre kľúčové spoločenské a hospodárske činnosti v rámci vnútorného trhu. Cieľom tejto smernice je najmä odstránenie nedostatkov v rozlišovaní medzi prevádzkovateľmi základných služieb a poskytovateľmi digitálnych služieb, ktoré sa ukázalo ako zastarané, pretože neodráža význam odvetví alebo služieb pre spoločenské a hospodárske činnosti na vnútornom trhu.

(7) Podľa smernice (EÚ) 2016/1148 boli členské štáty zodpovedné za identifikáciu subjektov, ktoré spĺňali kritériá na zaradenie medzi prevádzkovateľov základných služieb. S cieľom odstrániť veľké rozdiely medzi členskými štátmi v tejto súvislosti a zabezpečiť právnu istotu, pokiaľ ide o opatrenia na riadenie kybernetických rizík a oznamovacie povinnosti pre všetky príslušné subjekty, by sa malo stanoviť jednotné kritérium, ktorým sa určia subjekty, ktoré patria do rozsahu pôsobnosti tejto smernice. Uvedené kritérium by malo spočívať v uplatňovaní pravidla obmedzenia veľkosti, podľa ktorého všetky subjekty, ktoré sa považujú za stredné podniky podľa článku 2 prílohy k odporúčaniu Komisie 2003/361/ES ([5]), alebo ktoré prekračujú limity pre stredné podniky uvedené v odseku 1 uvedeného článku a pôsobia v rámci odvetví a poskytujú druhy služieb alebo vykonávajú činnosti, na ktoré sa vzťahuje táto smernica, patria do rozsahu jej pôsobnosti. Členské štáty by tiež mali stanoviť, že určité malé podniky

([5]) Odporúčanie Komisie 2003/361/ES zo 6. mája 2003 o vymedzení pojmov mikropodnik, malý a stredný podnik (Ú. v. EÚ L 124, 20.5.2003, s. 36).

a mikropodniky vymedzené v článku 2 ods. 2 a 3 uvedenej prílohy, ktoré spĺňajú osobitné kritériá, ktoré naznačujú kľúčovú úlohu pre spoločnosť, hospodárstvo alebo pre určité odvetvia alebo druhy služieb, patria do rozsahu pôsobnosti tejto smernice.

(8) Vylúčenie subjektov verejnej správy z rozsahu pôsobnosti tejto smernice by sa malo vzťahovať na subjekty, ktorých činnosti sa prevažne vykonávajú v oblastiach národnej bezpečnosti, verejnej bezpečnosti, obrany alebo presadzovania práva vrátane prevencie, vyšetrovania, odhaľovania a stíhania trestných činov. Subjekty verejnej správy, ktorých činnosti s uvedenými oblasťami súvisia len okrajovo, by však nemali byť vylúčené z rozsahu pôsobnosti tejto smernice. Na účely tejto smernice sa subjekty s regulačnými právomocami nepovažujú za subjekty vykonávajúce činnosti v oblasti presadzovania práva, a preto nie sú z uvedeného dôvodu vylúčené z rozsahu pôsobnosti tejto smernice. Subjekty verejnej správy, ktoré sú zriadené spoločne s treťou krajinou v súlade s medzinárodnou dohodou, sú vylúčené z rozsahu pôsobnosti tejto smernice. Táto smernica sa nevzťahuje na diplomatické a konzulárne misie členských štátov v tretích krajinách ani na ich siete a informačné systémy, pokiaľ sa takéto systémy nachádzajú v priestoroch misie alebo sú prevádzkované pre používateľov v tretej krajine.

(9) Členské štáty by mali mať možnosť prijať potrebné opatrenia s cieľom zaručiť ochranu základných záujmov národnej bezpečnosti, chrániť verejný poriadok a verejnú bezpečnosť a umožniť prevenciu, vyšetrovanie, odhaľovanie a stíhanie trestných činov. Na tento účel by členské štáty mali mať možnosť vyňať konkrétne subjekty, ktoré vykonávajú činnosti v oblastiach národnej bezpečnosti, verejnej bezpečnosti, obrany alebo presadzovania práva vrátane prevencie, vyšetrovania, odhaľovania a stíhania trestných činov z určitých povinností stanovených v tejto smernici v súvislosti s uvedenými činnosťami. Ak subjekt poskytuje služby výlučne subjektu verejnej správy, ktorý je vylúčený z rozsahu pôsobnosti tejto smernice, členské štáty by mali mať možnosť vyňať daný subjekt z určitých povinností stanovených v tejto smernici v súvislosti s uvedenými službami. Okrem toho by žiaden členský štát nemal byť povinný poskytovať informácie, ktorých sprístupnenie by odporovalo základným záujmom jeho národnej bezpečnosti, verejnej bezpečnosti alebo obrany. V uvedenom kontexte by sa malo prihliadať na pravidlá Únie alebo členských štátov na ochranu utajovaných skutočností, dohody o zachovaní mlčanlivosti a neformálne dohody o zachovaní mlčanlivosti, ako napríklad semaforový protokol. Semaforový protokol sa má chápať ako prostriedok na poskytovanie informácií o akýchkoľvek obmedzeniach, pokiaľ ide o ďalšie šírenie informácií. Používa sa takmer vo všetkých jednotkách pre riešenie počítačových bezpečnostných incidentov (ďalej len „jednotky CSIRT“) a v niektorých centrách pre analýzu a výmenu informácií.

(10) Hoci sa táto smernica vzťahuje na subjekty vykonávajúce činnosti v oblasti výroby elektrickej energie v jadrových elektrárňach, niektoré z uvedených činností môžu súvisieť s národnou bezpečnosťou. V takom prípade by členský štát mal mať v súlade so zmluvami možnosť uplatniť svoju zodpovednosť za ochranu národnej bezpečnosti v súvislosti s týmito činnosťami vrátane činností v rámci jadrového hodnotového reťazca.

(11) Niektoré subjekty vykonávajú činnosti v oblastiach národnej bezpečnosti, verejnej bezpečnosti, obrany alebo presadzovania práva vrátane prevencie, vyšetrovania, odhaľovania a stíhania trestných činov a zároveň poskytujú dôveryhodné služby. Poskytovatelia dôveryhodných služieb, ktorí patria do rozsahu pôsobnosti nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 ([6]), by mali patriť do rozsahu pôsobnosti tejto smernice s cieľom zabezpečiť rovnakú úroveň bezpečnostných požiadaviek a dohľadu, aká bola predtým stanovená v uvedenom nariadení, pokiaľ ide o poskytovateľov dôveryhodných služieb. V súlade s vyňatím určitých osobitných služieb z nariadenia (EÚ) č. 910/2014 by sa táto smernica nemala vzťahovať na poskytovanie dôveryhodných služieb, ktoré sa používajú výhradne v uzavretých systémoch na základe vnútroštátneho práva alebo dohôd medzi vymedzenou skupinou účastníkov.

([6]) 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).

(12) Poskytovatelia poštových služieb v zmysle smernice Európskeho parlamentu a Rady 97/67/ES ([7]) vrátane poskytovateľov kuriérskych služieb by mali podliehať tejto smernici, ak zabezpečujú aspoň jeden z krokov v reťazci poštového doručovania, a to najmä vyberanie, triedenie, prepravu alebo distribúciu poštových zásielok vrátane služieb zberu, pričom treba zohľadniť stupeň ich závislosti od sietí a informačných systémov. Dopravné služby, ktoré sa nevykonávajú v spojení s jedným z týchto krokov, by mali byť vyňaté z rozsahu poštových služieb.

(13) Vzhľadom na zintenzívnenie a zvýšenú sofistikovanosť kybernetických hrozieb by sa členské štáty mali usilovať zabezpečiť, aby subjekty vylúčené z rozsahu pôsobnosti tejto smernice dosiahli vysokú úroveň kybernetickej bezpečnosti, a mali by podporovať vykonávanie rovnocenných opatrení na riadenie kybernetických rizík, ktoré odrážajú citlivú povahu týchto subjektov.

(14) Na každé spracúvanie osobných údajov podľa tejto smernice sa vzťahuje právo Únie v oblasti ochrany údajov a právo Únie v oblasti ochrany súkromia. Touto smernicou konkrétne nie je dotknuté nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 ([8]) ani smernica Európskeho parlamentu a Rady 2002/58/ES ([9]). Touto smernicou by preto nemali byť dotknuté okrem iného úlohy a právomoci orgánov príslušných na monitorovanie dodržiavania platného práva Únie v oblasti ochrany údajov a práva Únie v oblasti ochrany súkromia.

(15) Subjekty, ktoré patria do rozsahu pôsobnosti tejto smernice na účely dodržiavania opatrení na riadenie kybernetických rizík a oznamovacích povinností, by sa mali rozdeliť do dvoch kategórií, na kľúčové subjekty a dôležité subjekty, a to na základe rozsahu, v akom sú kritické, pokiaľ ide o ich odvetvie alebo druh služieb, ktoré poskytujú, ako aj ich veľkosti. V tejto súvislosti by sa v relevantných prípadoch mali náležite zohľadniť aj všetky príslušné odvetvové posúdenia rizík alebo usmernenia zo strany príslušných orgánov. Malo by sa rozlišovať medzi režimom dohľadu a režimom presadzovania práva pre tieto dve kategórie subjektov, aby sa zabezpečila spravodlivá rovnováha medzi požiadavkami a povinnosťami založenými na riziku na jednej strane a administratívnou záťažou vyplývajúcou z dohľadu nad dodržiavaním predpisov na strane druhej.

(16) S cieľom zabrániť tomu, aby sa subjekty, ktoré majú partnerské podniky, alebo ktoré sú prepojenými podnikmi, považovali za kľúčové alebo dôležité subjekty v prípadoch, kde by to bolo neprimerané, môžu členské štáty pri uplatňovaní článku 6 ods. 2 prílohy k odporúčaniu 2003/361/ES zohľadniť mieru nezávislosti subjektu vo vzťahu k jeho partnerským alebo prepojeným podnikom. Členské štáty môžu zohľadniť najmä skutočnosť, že subjekt je nezávislý od svojich partnerských alebo prepojených podnikov, pokiaľ ide o siete a informačné systémy, ktoré daný subjekt používa pri poskytovaní svojich služieb, a pokiaľ ide o služby, ktoré daný subjekt poskytuje. Na tomto základe môžu členské štáty podľa potreby považovať takýto subjekt za subjekt, ktorý nemožno kvalifikovať ako stredný podnik podľa článku 2 prílohy k odporúčaniu 2003/361/ES, alebo za subjekt, ktorý neprekračuje limity pre stredný podnik stanovené v odseku 1 uvedeného článku, ak by sa po zohľadnení stupňa nezávislosti tohto subjektu tento subjekt nepovažoval za subjekt, ktorý možno kvalifikovať ako stredný podnik alebo ktorý prekračuje uvedené limity v prípade, že by sa zohľadnili len jeho vlastné údaje. Týmto nie sú dotknuté povinnosti, ktoré táto smernica ukladá partnerským a prepojeným podnikom, ktoré patria do rozsahu jej pôsobnosti.

(17) Členské štáty by mali mať možnosť rozhodnúť, že subjekty, ktoré boli pred nadobudnutím účinnosti tejto smernice identifikované ako prevádzkovatelia základných služieb v súlade so smernicou (EÚ) 2016/1148, sa majú považovať za kľúčové subjekty.

([7]) Smernica Európskeho parlamentu a Rady 97/67/ES z 15. decembra 1997 o spoločných pravidlách rozvoja vnútorného trhu poštových služieb Spoločenstva a zlepšovaní kvality služieb (Ú. v. ES L 15, 21.1.1998, s. 14).

([8]) 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).

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

(18) S cieľom zabezpečiť jasný prehľad o subjektoch, ktoré patria do rozsahu pôsobnosti tejto smernice, by členské štáty mali zostaviť zoznam kľúčových a dôležitých subjektov ako aj subjektov poskytujúcich služby registrácie názvov domén. Na tento účel by členské štáty mali od subjektov vyžadovať, aby príslušným orgánom predložili aspoň tieto informácie, t. j. názov, adresu a aktuálne kontaktné údaje vrátane e-mailových adries, rozsahov IP adries a telefónnych čísel subjektu, a podľa potreby príslušné odvetvie a pododvetvie uvedené v prílohách, ako aj prípadne zoznam členských štátov, v ktorých poskytujú služby patriace do rozsahu pôsobnosti tejto smernice. Na tento účel by Komisia s pomocou Agentúry Európskej únie pre kybernetickú bezpečnosť (ďalej len „ENISA“) mala bez zbytočného odkladu poskytnúť usmernenia a vzory týkajúce sa povinnosti predkladať informácie. S cieľom uľahčiť zostavenie a aktualizáciu zoznamu kľúčových a dôležitých subjektov, ako aj subjektov poskytujúcich služby registrácie názvov domén, by členské štáty mali mať možnosť zaviesť vnútroštátne mechanizmy, pomocou ktorých by sa subjekty mohli zaregistrovať samé. Ak existujú registre na vnútroštátnej úrovni, členské štáty môžu rozhodnúť o vhodných mechanizmoch, ktoré umožnia identifikáciu subjektov, ktoré patria do rozsahu pôsobnosti tejto smernice.

(19) Členské štáty by mali byť zodpovedné za to, aby Komisii predložili aspoň počet kľúčových a dôležitých subjektov za každé odvetvie a pododvetvie uvedené v prílohách, ako aj relevantné informácie o počte identifikovaných subjektov a o ustanovení tejto smernice, na základe ktorého boli identifikované, a o druhu služieb, ktoré poskytujú. Členské štáty sa vyzývajú, aby si s Komisiou vymieňali informácie o kľúčových a dôležitých subjektoch a v prípade rozsiahleho kybernetického incidentu relevantné informácie, napríklad názov dotknutého subjektu.

(20) Komisia by mala v spolupráci so skupinou pre spoluprácu a po porade s relevantnými zainteresovanými stranami poskytnúť usmernenia o vykonávaní kritérií uplatniteľných na mikropodniky a malé podniky na účely posúdenia, či patria do rozsahu pôsobnosti tejto smernice. Komisia by takisto mala zabezpečiť, aby sa mikropodnikom a malým podnikom, ktoré patria do rozsahu pôsobnosti tejto smernice, poskytli primerané usmernenia. Komisia by v tejto súvislosti mala s pomocou členských štátov poskytovať informácie mikropodnikom a malým podnikom.

(21) Komisia by mohla poskytovať usmernenia na podporu členských štátov pri vykonávaní ustanovení tejto smernice týkajúcich sa rozsahu jej pôsobnosti a hodnotení primeranosti opatrení, ktoré sa majú prijať podľa tejto smernice, najmä pokiaľ ide o subjekty s komplexnými obchodnými modelmi alebo prevádzkovým prostredím, keď subjekt môže súčasne spĺňať kritériá pre kľúčové aj dôležité subjekty alebo môže súčasne vykonávať činnosti, z ktorých niektoré patria do rozsahu pôsobnosti tejto smernice a niektoré sú z neho vyňaté.

(22) V tejto smernici sa stanovuje základ pre opatrenia na riadenie kybernetických rizík a oznamovacie povinnosti v odvetviach, ktoré patria do jej rozsahu pôsobnosti. Aby sa zabránilo fragmentácii ustanovení o kybernetickej bezpečnosti v rámci právnych aktov Únie, Komisia by v prípade, ak sa v záujme zabezpečenia vysokej úrovne kybernetickej bezpečnosti v celej Únii považujú za potrebné ďalšie odvetvové právne akty Únie, ktoré sa týkajú opatrení na riadenie kybernetických rizík a oznamovacích povinností, mala posúdiť, či by sa takéto ďalšie ustanovenia mohli stanoviť vo vykonávacom akte prijatom podľa tejto smernice. V prípade, ak by takýto vykonávací akt nebol na tento účel vhodný, k zabezpečeniu vysokej úrovne kybernetickej bezpečnosti v celej Únii by mohli prispieť odvetvové právne akty Únie, pričom by sa v nich plne zohľadnili špecifiká a zložitosti dotknutých odvetví. Preto sa touto smernicou nebráni prijatiu ďalších odvetvových právnych aktov Únie, ktoré sa zaoberajú opatreniami na riadenie kybernetických rizík a oznamovacími povinnosťami a ktoré riadne zohľadňujú potrebu komplexného a súdržného rámca pre kybernetickú bezpečnosť. Touto smernicou nie sú dotknuté existujúce vykonávacie právomoci, ktoré boli Komisii udelené vo viacerých odvetviach vrátane dopravy a energetiky.

(23) Ak odvetvový právny akt Únie obsahuje ustanovenia vyžadujúce, aby kľúčové alebo dôležité subjekty prijali opatrenia na riadenie kybernetických rizík, alebo aby oznamovali významné incidenty, a ak majú tieto požiadavky aspoň rovnocenný účinok ako povinnosti stanovené v tejto smernici, uvedené ustanovenia vrátane ustanovení

o dohľade a presadzovaní práva by sa mali vzťahovať na takéto subjekty. Ak sa odvetvový právny akt Únie nevzťahuje na všetky subjekty v konkrétnom odvetví, ktoré patria do rozsahu pôsobnosti tejto smernice, na subjekty, na ktoré sa uvedený akt nevzťahuje, by sa mali naďalej vzťahovať príslušné ustanovenia tejto smernice.

(24) Ak sa v ustanoveniach odvetvového právneho aktu Únie vyžaduje, aby kľúčové alebo dôležité subjekty dodržiavali oznamovacie povinnosti, ktoré majú aspoň rovnocenný účinok ako oznamovacie povinnosti stanovené v tejto smernici, mala by sa zabezpečiť konzistentnosť a účinnosť vybavovania oznámení o incidentoch. Na tento účel by ustanovenia odvetvového právneho aktu Únie týkajúce sa oznamovania incidentov mali poskytovať jednotkám CSIRT, príslušným orgánom alebo jednotným kontaktným miestam pre kybernetickú bezpečnosť (ďalej len „jednotné kontaktné miesta“) podľa tejto smernice okamžitý prístup k oznámeniam o incidentoch predkladaným v súlade s odvetvovým právnym aktom Únie. Takýto okamžitý prístup možno zabezpečiť najmä vtedy, ak sa oznámenia o incidentoch bez zbytočného odkladu postupujú jednotke CSIRT, príslušnému orgánu alebo jednotnému kontaktnému miestu podľa tejto smernice. V prípade potreby by členské štáty mali zaviesť mechanizmus automatického a priameho oznamovania, ktorý zabezpečí systematickú a okamžitú výmenu informácií s jednotkami CSIRT, príslušnými orgánmi alebo jednotným kontaktným miestom, pokiaľ ide o vybavovanie takýchto oznámení o incidentoch. Na účely zjednodušenia oznamovania a uplatňovania mechanizmu automatického a priameho oznamovania by členské štáty mohli v súlade s odvetvovým právnym aktom Únie používať jednotné kontaktné miesto.

(25) V odvetvových právnych aktoch Únie, v ktorých sa stanovujú opatrenia na riadenie kybernetických rizík alebo oznamovacie povinnosti, ktoré majú aspoň rovnocenný účinok ako tie, ktoré sú stanovené v tejto smernici, by sa mohlo stanoviť, že príslušné orgány podľa takýchto aktov vykonávajú svoje právomoci v oblasti dohľadu a presadzovania práva vo vzťahu k takýmto opatreniam alebo povinnostiam s pomocou príslušných orgánov podľa tejto smernice. Dotknuté príslušné orgány by na daný účel mohli uzatvárať dohody o spolupráci. V takýchto dohodách o spolupráci by sa okrem iného mohli špecifikovať postupy týkajúce sa koordinácie činností dohľadu vrátane postupov vyšetrovaní a inšpekcií na mieste v súlade s vnútroštátnym právom a mechanizmus výmeny relevantných informácií o dohľade a presadzovaní práva medzi príslušnými orgánmi vrátane prístupu ku kybernetickým informáciám, ktoré si vyžiadali príslušné orgány podľa tejto smernice.

(26) Ak sa v odvetvových právnych aktoch Únie vyžadujú alebo poskytujú stimuly pre subjekty, aby oznamovali významné kybernetické hrozby, členské štáty by mali podporovať aj výmenu informácií o významných kybernetických hrozbách s jednotkami CSIRT, príslušnými orgánmi alebo jednotnými kontaktnými miestami podľa tejto smernice, aby sa zabezpečila zvýšená úroveň informovanosti uvedených orgánov o prostredí kybernetických hrozieb a umožnilo sa im účinne a včas reagovať, ak by sa významné kybernetické hrozby naplnili.

(27) Budúce odvetvové právne akty Únie by mali náležite zohľadňovať vymedzenia pojmov a rámec dohľadu a presadzovania práva, ako sú stanovené v tejto smernici.

(28) Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 ([10]) by sa v súvislosti s touto smernicou malo považovať za odvetvový právny akt Únie, pokiaľ ide o finančné subjekty. Namiesto ustanovení tejto smernice by sa mali uplatňovať ustanovenia nariadenia (EÚ) 2022/2554 týkajúce sa riadenia rizík v oblasti informačných a komunikačných technológií (ďalej len „IKT“), riadenia incidentov súvisiacich s IKT, a najmä oznamovania závažných incidentov súvisiacich s IKT, ako aj testovania digitálnej prevádzkovej odolnosti, mechanizmov výmeny informácií a rizík týkajúcich sa IKT zabezpečovaných tretími stranami. Členské štáty by preto nemali uplatňovať ustanovenia tejto smernice týkajúce sa riadenia kybernetických rizík a oznamovacích povinností a dohľadu a presadzovania práva na finančné subjekty, na ktoré sa vzťahuje nariadenie (EÚ) 2022/2554. Zároveň je dôležité zachovať pevné vzťahy a výmenu informácií s finančným odvetvím podľa tejto smernice. Na tento účel nariadenie (EÚ) 2022/2554 umožňuje európskym orgánom dohľadu (ESA) a príslušným orgánom podľa uvedeného nariadenia zúčastňovať sa na činnostiach skupiny pre spoluprácu a vymieňať si informácie a spolupracovať s jednotnými kontaktnými miestami, ako aj s jednotkami CSIRT a príslušnými orgánmi podľa tejto smernice. Príslušné orgány podľa nariadenia (EÚ) 2022/2554 by mali tiež zasielať podrobné údaje o závažných incidentoch súvisiacich s IKT a v prípade potreby o významných kybernetických hrozbách jednotkám CSIRT, príslušným orgánom alebo jednotným kontaktným miestam podľa tejto smernice. To je možné dosiahnuť poskytnutím

([10]) 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 (pozri stranu 1 tohto úradného vestníka).

okamžitého prístupu k oznámeniam o incidentoch a ich postúpením buď priamo alebo prostredníctvom jednotného kontaktného miesta. Členské štáty by okrem toho mali naďalej začleňovať finančné odvetvie do svojich stratégií kybernetickej bezpečnosti a jednotky CSIRT môžu zahrnúť finančné odvetvie do svojich činností.

(29) Aby sa zabránilo medzerám alebo duplicite, pokiaľ ide o povinnosti v oblasti kybernetickej bezpečnosti uložené subjektom v odvetví letectva, vnútroštátne orgány podľa nariadení Európskeho parlamentu a Rady (ES) č. 300/2008 ([11]) a (EÚ) 2018/1139 ([12]) a príslušné orgány podľa tejto smernice by mali spolupracovať v súvislosti s vykonávaním opatrení na riadenie kybernetických rizík a dohľadom nad dodržiavaním týchto opatrení na vnútroštátnej úrovni. Súlad subjektu s bezpečnostnými požiadavkami stanovenými v nariadeniach (ES) č. 300/2008 a (EÚ) 2018/1139 a v príslušných delegovaných a vykonávacích aktoch prijatých podľa uvedených nariadení by príslušné orgány mohli považovať za súlad so zodpovedajúcimi požiadavkami stanovenými v tejto smernici.

(30) Vzhľadom na prepojenia medzi kybernetickou bezpečnosťou a fyzickou bezpečnosťou subjektov by sa mal zabezpečiť jednotný prístup medzi smernicou Európskeho parlamentu a Rady (EÚ) 2022/2557 ([13]) a touto smernicou. Na dosiahnutie tohto cieľa by sa subjekty identifikované ako kritické subjekty podľa smernice (EÚ) 2022/2557 mali považovať za kľúčové subjekty podľa tejto smernice. Každý členský štát by navyše mal zabezpečiť, aby sa v jeho národnej stratégii kybernetickej bezpečnosti stanovil politický rámec pre posilnenú koordináciu v rámci daného členského štátu medzi jeho príslušnými orgánmi podľa tejto smernice a jeho príslušnými orgánmi podľa smernice (EÚ) 2022/2557 v kontexte výmeny informácií o rizikách, kybernetických hrozbách a incidentoch, ako aj o nekybernetických rizikách, hrozbách a incidentoch a v kontexte plnenia úloh v oblasti dohľadu. Príslušné orgány podľa tejto smernice a príslušné orgány podľa smernice (EÚ) 2022/2557 by mali spolupracovať a vymieňať si informácie bez zbytočného odkladu, najmä pokiaľ ide o identifikáciu kritických subjektov, riziká, kybernetické hrozby a incidenty, ako aj nekybernetické riziká, hrozby a incidenty, ktoré ovplyvňujú kritické subjekty, vrátane kybernetických a fyzických opatrení prijatých kritickými subjektmi, ako aj výsledkov činností dohľadu vykonávaných v súvislosti s takýmito subjektmi.

Okrem toho, s cieľom zefektívniť činnosti dohľadu medzi príslušnými orgánmi podľa tejto smernice a príslušnými orgánmi podľa smernice (EÚ) 2022/2557 a s cieľom minimalizovať administratívnu záťaž dotknutých subjektov, by sa uvedené príslušné orgány mali usilovať zharmonizovať vzorové formuláre na oznamovanie incidentov a postupy dohľadu. V prípade potreby by príslušné orgány podľa smernice (EÚ) 2022/2557 mali mať možnosť požiadať príslušné orgány podľa tejto smernice, aby vykonávali svoje právomoci v oblasti dohľadu a presadzovania práva vo vzťahu k subjektu, ktorý je identifikovaný ako kritický subjekt podľa smernice (EÚ) 2022/2557. Na tento účel by príslušné orgány podľa tejto smernice a príslušné orgány podľa smernice (EÚ) 2022/2557 mali, podľa možnosti v reálnom čase, spolupracovať a vymieňať si informácie.

(31) Subjekty patriace do odvetvia digitálnej infraštruktúry sú v podstate založené na sieťach a informačných systémoch, a preto by sa povinnosti, ktoré týmto subjektom podľa tejto smernice, mali komplexným spôsobom zaoberať fyzickou bezpečnosťou takýchto systémov ako súčasťou ich opatrení na riadenie kybernetických rizík a oznamovacích povinností. Keďže sa na uvedené záležitosti vzťahuje táto smernica, povinnosti stanovené v kapitolách III, IV a VI smernice (EÚ) 2022/2557 sa na takéto subjekty nevzťahujú.

([11]) Nariadenie Európskeho parlamentu a Rady (ES) č. 300/2008 z 11. marca 2008 o spoločných pravidlách v oblasti bezpečnostnej ochrany civilného letectva a o zrušení nariadenia (ES) č. 2320/2002 (Ú. v. EÚ L 97, 9.4.2008, s. 72).

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

([13]) Smernica Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/114/ES (pozri stranu 164 tohto úradného vestníka).

(32) Podpora a ochrana spoľahlivého, odolného a bezpečného systému názvov domén (ďalej len „DNS“ - domain name system) sú kľúčovým faktorom zachovania integrity internetu a sú nevyhnutné pre jeho nepretržité a stabilné fungovanie, od ktorého závisí digitálne hospodárstvo a spoločnosť. Táto smernica by sa preto mala vzťahovať na správcov názvov domén najvyššej úrovne (ďalej len „TLD“ - top-level-domain) a poskytovateľov služieb DNS, ktorí sa majú chápať ako subjekty poskytujúce verejne dostupné služby rekurzívneho rozlišovania názvov domén pre koncových používateľov internetu alebo služby autoritatívneho rozlišovania názvov domén pre použitie tretími stranami. Táto smernica by sa nemala vzťahovať na koreňové názvové servery.

(33) Služby cloud computingu by mali zahŕňať digitálne služby, ktoré umožňujú správu na požiadanie a vzdialený širokopásmový prístup ku škálovateľnému a pružnému súboru zdieľateľných počítačových zdrojov, a to aj ak sa tieto zdroje nachádzajú na viacerých miestach. Počítačové zdroje zahŕňajú zdroje, ako sú siete, servery alebo iná infraštruktúra, operačné systémy, softvér, úložiská, aplikácie a služby. Modely služieb cloud computingu zahŕňajú okrem iného infraštruktúru ako službu (IaaS), platformu ako službu (PaaS), softvér ako službu (SaaS) a sieť ako službu (NaaS). Modely zavádzania cloud computingu by mali zahŕňať súkromný, komunitný, verejný a hybridný cloud. Modely služieb a nasadenia cloud computingu majú rovnaký význam ako podmienky poskytovania služieb a modely nasadenia vymedzené v norme ISO/IEC 17788:2014. Schopnosť používateľa cloud computingu jednostranne si zabezpečovať počítačové kapacity, ako je serverový čas alebo sieťové úložisko, bez ľudskej interakcie zo strany poskytovateľa služieb cloud computingu by sa mohla opísať ako správa na požiadanie.

Pojem „širokopásmový vzdialený prístup“ sa používa na opis toho, že cloudové kapacity sú poskytované cez sieť a prístupné prostredníctvom mechanizmov na podporu využívania heterogénnych tenkých alebo hrubých klientskych platforiem vrátane mobilných telefónov, tabletov, laptopov a pracovných staníc. Pojem „škálovateľné“ odkazuje na počítačové zdroje, ktoré pružne prideľuje poskytovateľ cloudových služieb bez ohľadu na zemepisnú polohu zdrojov s cieľom zvládať výkyvy v dopyte. Pojem „pružný súbor“ sa používa na označenie počítačových zdrojov, ktoré sa poskytujú a uvoľňujú na základe dopytu s cieľom rýchlo zvýšiť a znížiť dostupné zdroje v závislosti od záťaže. Pojem „zdieľateľný“ sa používa na označenie počítačových zdrojov, ktoré sa poskytujú viacerým používateľom, ktorí zdieľajú spoločný prístup k službe, ale spracúvanie sa vykonáva oddelene pre každého používateľa, hoci sa služba poskytuje z toho istého elektronického zariadenia. Pojem „distribuovaný“ sa používa na opis počítačových zdrojov, ktoré sa nachádzajú v rôznych sieťových počítačoch alebo zariadeniach a ktoré navzájom komunikujú a koordinujú sa prenosom správ.

(34) Vzhľadom na vznik inovatívnych technológií a nových obchodných modelov sa očakáva, že sa na vnútornom trhu objavia nové modely služieb a nasadenia cloud computingu v reakcii na vyvíjajúce sa potreby zákazníkov. V tejto súvislosti sa služby cloud computingu môžu poskytovať vo vysoko distribuovanej forme, ešte bližšie k miestu, kde sa údaje generujú alebo zhromažďujú, čím sa prechádza od tradičného modelu k vysoko distribuovanému modelu (edge computing).

(35) Služby ponúkané poskytovateľmi služieb dátového centra sa nemusia vždy poskytovať vo forme služby cloud computingu. Dátové centrá preto nemusia vždy tvoriť súčasť infraštruktúry cloud computingu. S cieľom riadiť všetky riziká spojené s bezpečnosťou sietí a informačných systémov by sa táto smernica preto mala vzťahovať na poskytovateľov služieb dátového centra, ktoré nie sú službami cloud computingu. Na účely tejto smernice by sa pojem „služba dátového centra“ mal vzťahovať na poskytovanie služby, ktorá zahŕňa štruktúry alebo skupiny štruktúr určené na centralizované umiestnenie, vzájomné prepojenie a prevádzku informačných technológií (IT) a sieťového vybavenia poskytujúcich služby ukladania, spracovania a prepravy dát spolu so všetkými zariadeniami a infraštruktúrami na distribúciu elektrickej energie a environmentálnu kontrolu. Pojem „služba dátového centra“ by sa nemal vzťahovať na interné podnikové dátové centrá vlastnené a prevádzkované na vlastné účely príslušného subjektu.

(36) Výskumné činnosti zohrávajú kľúčovú úlohu pri vývoji nových produktov a procesov. Mnohé z uvedených činností vykonávajú subjekty, ktoré poskytujú, šíria alebo využívajú výsledky svojho výskumu na komerčné účely. Tieto subjekty preto môžu byť dôležitými aktérmi v hodnotových reťazcoch, vďaka čomu sa bezpečnosť ich sietí a informačných systémov stáva neoddeliteľnou súčasťou celkovej kybernetickej bezpečnosti vnútorného trhu. Výskumné organizácie by sa mali chápať tak, že zahŕňajú subjekty, ktoré zameriavajú podstatnú časť svojich činností na vykonávanie aplikovaného výskumu alebo experimentálneho vývoja v zmysle príručky vydanej

Organizáciou pre hospodársku spoluprácu a rozvoj pod názvom Frascati Manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development (Usmernenia pre zber a vykazovanie údajov o výskume a experimentálnom vývoji), a to s cieľom využiť ich výsledky na komerčné účely, ako je výroba alebo vývoj výrobku či procesu, poskytovanie služby, alebo ich uvádzanie na trh.

(37) Rastúca previazanosť je výsledkom čoraz väčšej cezhraničnej a previazanej siete poskytovania služieb s využitím kľúčových infraštruktúr v celej Únii v odvetviach ako sú energetika, doprava, digitálna infraštruktúra, pitná voda a odpadová voda, zdravie, určité aspekty verejnej správy, ako aj kozmický priestor, pokiaľ ide o poskytovanie určitých služieb závislých od pozemných infraštruktúr, ktoré vlastnia, spravujú a prevádzkujú členské štáty alebo súkromné strany, a preto sa nevzťahuje na infraštruktúry vlastnené, spravované alebo prevádzkované Úniou alebo v jej mene ako súčasť jej vesmírneho programu. Táto previazanosť znamená, že akékoľvek narušenie, dokonca aj také, ktoré sa pôvodne obmedzovalo na jeden subjekt alebo jedno odvetvie, môže mať širšie kaskádovité účinky, čo môže viesť k ďalekosiahlym a dlhotrvajúcim negatívnym vplyvom na poskytovanie služieb na celom vnútornom trhu. Intenzívnejšie kybernetické útoky počas pandémie ochorenia COVID-19 ukázali zraniteľnosť čoraz previazanejších spoločností voči rizikám s nízkou pravdepodobnosťou.

(38) Vzhľadom na rozdiely vo vnútroštátnych štruktúrach riadenia a s cieľom zachovať už existujúce odvetvové dohody alebo orgány dohľadu a regulačné orgány Únie by členské štáty mali mať možnosť určiť alebo zriadiť jeden alebo viaceré príslušné orgány zodpovedné za kybernetickú bezpečnosť a úlohy dohľadu podľa tejto smernice.

(39) V záujme uľahčenia cezhraničnej spolupráce a komunikácie orgánov a s cieľom umožniť účinné vykonávanie tejto smernice je potrebné, aby každý členský štát určil jednotné kontaktné miesto zodpovedné za koordináciu záležitostí týkajúcich sa bezpečnosti sietí a informačných systémov a cezhraničnú spoluprácu na úrovni Únie.

(40) Jednotné kontaktné miesta by mali zabezpečiť účinnú cezhraničnú spoluprácu s relevantnými orgánmi iných členských štátov a v prípade potreby s Komisiou a agentúrou ENISA. Jednotné kontaktné miesta by preto na žiadosť jednotky CSIRT alebo príslušného orgánu mali byť poverené zasielaním oznámení o významných incidentoch s cezhraničným dosahom jednotným kontaktným miestam iných postihnutých členských štátov. Na vnútroštátnej úrovni by jednotné kontaktné miesta mali umožňovať bezproblémovú medziodvetvovú spoluprácu s inými príslušnými orgánmi. Jednotné kontaktné miesta by mohli byť aj adresátmi relevantných informácií o incidentoch týkajúcich sa finančných subjektov od príslušných orgánov podľa nariadenia (EÚ) 2022/2554, ktoré by mali byť podľa potreby schopné postúpiť jednotkám CSIRT alebo príslušným orgánom podľa tejto smernice.

(41) Členské štáty by mali mať primerané vybavenie, pokiaľ ide o technické a organizačné spôsobilosti, aby mohli predchádzať incidentom a rizikám, odhaľovať ich, reagovať na ne a zmierňovať ich vplyv. Členské štáty by preto mali zriadiť alebo určiť jednu alebo viacero jednotiek CSIRT podľa tejto smernice a zabezpečiť, aby mali primerané zdroje a technické kapacity. Jednotky CSIRT by mali spĺňať požiadavky stanovené v tejto smernici s cieľom zaručiť účinné a zlučiteľné kapacity na riešenie incidentov a rizík a zabezpečiť účinnú spoluprácu na úrovni Únie. Členské štáty by mali mať možnosť určiť existujúce tímy reakcie na núdzové počítačové situácie (CERT) za jednotky CSIRT. S cieľom posilniť dôverný vzťah medzi subjektmi a jednotkami CSIRT v prípadoch, keď je jednotka CSIRT súčasťou príslušného orgánu, by členské štáty mali mať možnosť zvážiť funkčné oddelenie operačných úloh poskytovaných jednotkami CSIRT, najmä pokiaľ ide o výmenu informácií a pomoc poskytovanú subjektom, od činností dohľadu príslušných orgánov.

(42) Jednotky CSIRT sú poverené riešením incidentov. To zahŕňa spracovanie veľkých objemov niekedy citlivých údajov. Členské štáty by mali zabezpečiť, aby jednotky CSIRT mali infraštruktúru na výmenu a spracovanie informácií, ako aj dobre vybavený personál, ktorý zabezpečí dôvernosť a dôveryhodnosť ich operácií. Jednotky CSIRT by v tejto súvislosti mohli prijať aj kódexy správania.

(43) Pokiaľ ide o osobné údaje, jednotky CSIRT by mali mať možnosť vykonávať v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 na žiadosť kľúčového alebo dôležitého subjektu proaktívnu kontrolu sietí a informačných systémov používaných na poskytovanie služieb subjektu. Členské štáty by sa mali podľa potreby zamerať na zabezpečenie rovnakej úrovne technických kapacít pre všetky odvetvové jednotky CSIRT. Členské štáty by pri zriaďovaní svojich jednotiek CSIRT mali mať možnosť požiadať o pomoc agentúru ENISA.

(44) Jednotky CSIRT by mali byť na žiadosť kľúčového alebo dôležitého subjektu schopné monitorovať aktíva subjektu orientované na internet v jeho priestoroch aj mimo nich s cieľom identifikovať, pochopiť a riadiť celkové organizačné riziká subjektu, pokiaľ ide o novoobjavené ohrozenia dodávateľského reťazca alebo kritické zraniteľnosti. Subjekt by sa mal nabádať, aby jednotke CSIRT oznámil, či prevádzkuje privilegované riadiace rozhranie, keďže by to mohlo ovplyvniť rýchlosť vykonávania zmierňujúcich opatrení.

(45) Vzhľadom na význam medzinárodnej spolupráce v oblasti kybernetickej bezpečnosti by sa malo jednotkám CSIRT umožniť, aby sa okrem siete jednotiek CSIRT zriadenej podľa tejto smernice mohli stať súčasťou sietí medzinárodnej spolupráce. Jednotky CSIRT a príslušné orgány by preto na účely vykonávania svojich úloh mali mať možnosť vymieňať si informácie vrátane osobných údajov s národnými jednotkami reakcie na počítačové bezpečnostné incidenty alebo príslušnými orgánmi tretích krajín za predpokladu, že sú splnené podmienky podľa práva Únie v oblasti ochrany údajov pre prenosy osobných údajov do tretích krajín, okrem iného podmienky podľa článku 49 nariadenia (EÚ) 2016/679.

(46) Je nevyhnutné zabezpečiť primerané zdroje na splnenie cieľov tejto smernice a umožniť príslušným orgánom a jednotkám CSIRT vykonávať úlohy stanovené v tejto smernici. Členské štáty môžu na vnútroštátnej úrovni zaviesť mechanizmus financovania na pokrytie potrebných výdavkov v súvislosti s plnením úloh verejných subjektov zodpovedných za kybernetickú bezpečnosť v členskom štáte podľa tejto smernice. Takýto mechanizmus by mal byť v súlade s právom Únie a mal by byť primeraný a nediskriminačný a mal by zohľadňovať rôzne prístupy k poskytovaniu bezpečných služieb.

(47) Sieť jednotiek CSIRT by mala naďalej prispievať k posilňovaniu dôvery a podporovať rýchlu a účinnú operačnú spoluprácu medzi členskými štátmi. S cieľom posilniť operačnú spoluprácu na úrovni Únie by sieť jednotiek CSIRT mala zvážiť prizývanie orgánov a agentúr Únie zapojených do politiky v oblasti kybernetickej bezpečnosti, ako je Europol, k účasti na svojej práci.

(48) Na účely dosiahnutia a udržania vysokej úrovne kybernetickej bezpečnosti by národné stratégie kybernetickej bezpečnosti požadované podľa tejto smernice mali pozostávať zo súdržných rámcov stanovujúcich strategické ciele a priority v oblasti kybernetickej bezpečnosti a systém riadenia na ich dosiahnutie. Uvedené stratégie sa môžu skladať z jedného alebo viacerých legislatívnych alebo nelegislatívnych nástrojov.

(49) Politiky kybernetickej hygieny poskytujú základy pre ochranu infraštruktúry sietí a informačných systémov, bezpečnosť hardvéru, softvéru a online aplikácií a ochranu obchodných údajov alebo údajov o koncových používateľoch, na ktoré sa subjekty spoliehajú. Politiky kybernetickej hygieny zahŕňajúce spoločný základný súbor postupov vrátane aktualizácií softvéru a hardvéru, zmeny hesiel, riadenia nových inštalácií, obmedzenia prístupových účtov na úrovni správcu a zálohovania údajov umožňujú proaktívny rámec pripravenosti a celkovej bezpečnosti a ochrany v prípade incidentov alebo kybernetických hrozieb. Agentúra ENISA by mala monitorovať a analyzovať politiky členských štátov v oblasti kybernetickej hygieny.

(50) Informovanosť o kybernetickej bezpečnosti a kybernetická hygiena sú nevyhnutné na zvýšenie úrovne kybernetickej bezpečnosti v Únii, najmä vzhľadom na rastúci počet pripojených zariadení, ktoré sa čoraz viac využívajú pri kybernetických útokoch. Malo by sa vyvinúť úsilie na zvýšenie celkovej informovanosti o rizikách súvisiacich s takýmito zariadeniami, zatiaľ čo posúdenia na úrovni Únie by mohli pomôcť zabezpečiť spoločné chápanie takýchto rizík na vnútornom trhu.

(51) Členské štáty by mali podporovať využívanie každej inovatívnej technológie vrátane umelej inteligencie, ktorej používanie by mohlo zlepšiť odhaľovanie a prevenciu kybernetických útokov, čo by umožnilo účinnejšie presmerovanie zdrojov na kybernetické útoky. Členské štáty by preto mali vo svojich národných stratégiách kybernetickej bezpečnosti podporovať činnosti v oblasti výskumu a vývoja s cieľom uľahčiť používanie takýchto technológií, najmä tých, ktoré sa týkajú automatizovaných alebo poloautomatizovaných nástrojov v oblasti kybernetickej bezpečnosti, a v prípade potreby spoločné využívanie údajov potrebných na odbornú prípravu používateľov takejto technológie a na jej zlepšenie. Používanie akejkoľvek inovatívnej technológie vrátane umelej inteligencie by malo byť v súlade s právom Únie v oblasti ochrany údajov vrátane zásad ochrany údajov, ktorými sú presnosť údajov, minimalizácia údajov, spravodlivosť a transparentnosť a bezpečnosť údajov, napríklad využitím najmodernejšieho šifrovania. Mali by sa v plnej miere využiť požiadavky na špecificky navrhnutú a štandardnú ochranu údajov stanovené v nariadení (EÚ) 2016/679.

(52) Nástroje a aplikácie kybernetickej bezpečnosti s otvoreným zdrojovým kódom môžu prispieť k vyššej miere otvorenosti a môžu mať pozitívny vplyv na efektívnosť priemyselných inovácií. Otvorené normy uľahčujú interoperabilitu medzi bezpečnostnými nástrojmi, čo je prínosom pre bezpečnosť zainteresovaných strán z oblasti priemyslu. Nástroje a aplikácie kybernetickej bezpečnosti s otvoreným zdrojovým kódom môžu mobilizovať širšiu komunitu vývojárov a umožniť diverzifikáciu dodávateľov. Otvorený zdrojový kód môže viesť k transparentnejšiemu procesu overovania nástrojov súvisiacich s kybernetickou bezpečnosťou a ku komunitnému procesu objavovania zraniteľností. Členské štáty by preto mali mať možnosť podporovať používanie softvéru s otvoreným zdrojovým kódom a otvorených noriem uplatňovaním politík týkajúcich sa využívania otvorených údajov a otvoreného zdrojového kódu ako súčasti bezpečnosti prostredníctvom transparentnosti. Politiky podporujúce zavedenie a udržateľné využívanie nástrojov kybernetickej bezpečnosti s otvoreným zdrojovým kódom majú osobitný význam pre malé a stredné podniky, ktoré čelia značným nákladom na vykonávanie, ktoré by sa mohli minimalizovať znížením potreby špecifických aplikácií alebo nástrojov.

(53) Verejnoprospešné služby sú čoraz viac napojené na digitálne siete v mestách s cieľom zlepšiť siete mestskej dopravy, modernizovať zariadenia na zásobovanie vodou a zneškodňovanie odpadu a zvýšiť efektívnosť osvetlenia a vykurovania budov. Uvedené digitalizované verejnoprospešné služby sú zraniteľné voči kybernetickým útokom a v prípade úspešného kybernetického útoku predstavujú riziko poškodenia občanov vo veľkom rozsahu z dôvodu ich vzájomnej prepojenosti. Členské štáty by mali v rámci svojej národnej stratégie kybernetickej bezpečnosti vypracovať politiku, ktorá sa bude zaoberať rozvojom takýchto prepojených alebo inteligentných miest a ich potenciálnym vplyvom na spoločnosť.

(54) V posledných rokoch Únia čelila exponenciálnemu nárastu ransomvérových útokov, pri ktorých malvér šifruje údaje a systémy a požaduje platbu výkupného za odblokovanie. Nárast frekvencie a závažnosti ransomvérových útokov môže byť spôsobený viacerými faktormi, ako sú rôzne modely útokov, kriminálne obchodné modely súvisiace s „ransomvérom ako službou“ a kryptomenami, požiadavky na výkupné a nárast útokov na dodávateľské reťazce. Členské štáty by mali v rámci svojich národných stratégií kybernetickej bezpečnosti vypracovať politiku, ktorá bude riešiť nárast ransomvérových útokov.

(55) Verejno-súkromné partnerstvá v oblasti kybernetickej bezpečnosti môžu poskytnúť vhodný rámec pre výmenu znalostí, výmenu najlepších postupov a vytvorenie spoločnej úrovne porozumenia medzi zainteresovanými stranami. Členské štáty by mali presadzovať politiky na podporu vytvárania verejno-súkromných partnerstiev zameraných špecificky na kybernetickú bezpečnosť. Pokiaľ ide o verejno-súkromné partnerstvá, uvedené politiky by mali spresniť okrem iného ich pôsobnosť a zapojené zainteresované strany, model riadenia, dostupné možnosti financovania a interakciu medzi zúčastnenými zainteresovanými stranami. Verejno-súkromné partnerstvá môžu využívať odborné znalosti subjektov súkromného sektora na pomoc príslušným orgánom pri rozvoji špičkových služieb a procesov vrátane výmeny informácií, včasného varovania, cvičení zameraných na kybernetické hrozby a incidenty, krízového riadenia a plánovania odolnosti.

(56) Členské štáty by sa mali vo svojich národných stratégiách kybernetickej bezpečnosti zaoberať osobitnými potrebami, ktoré majú v oblasti kybernetickej bezpečnosti malé a stredné podniky. Malé a stredné podniky predstavujú v celej Únii veľký percentuálny podiel priemyselného a obchodného trhu a často majú ťažkosti s prispôsobením sa novým obchodným postupom v prepojenejšom svete a digitálnemu prostrediu, v ktorom zamestnanci pracujú z domu a obchodné činnosti sa čoraz častejšie vykonávajú online. Niektoré malé a stredné podniky čelia osobitným výzvam v oblasti kybernetickej bezpečnosti, ako je nízke kybernetické povedomie, nedostatočná bezpečnosť vzdialených IT, vysoké náklady na riešenia v oblasti kybernetickej bezpečnosti a zvýšená úroveň hrozieb, ako je napríklad ransomvér, v súvislosti s ktorými by mali dostať usmernenia a podporu. Malé a stredné podniky sa čoraz viac stávajú terčom útokov na dodávateľské reťazce z dôvodu ich menej prísnych opatrení na riadenie kybernetických rizík a zvládanie útokov a skutočnosti, že majú obmedzené bezpečnostné zdroje. Takéto útoky na dodávateľské reťazce majú vplyv nielen na malé a stredné podniky a ich izolovanú činnosť, ale môžu mať aj kaskádový účinok na väčšie útoky na subjekty, ktorým poskytli dodávky. Členské štáty by mali prostredníctvom svojich národných

stratégií kybernetickej bezpečnosti pomáhať malým a stredným podnikom pri riešení výziev, ktorým čelia vo svojich dodávateľských reťazcoch. Členské štáty by mali mať kontaktné miesto pre malé a stredné podniky na národnej alebo regionálnej úrovni, ktoré buď poskytuje usmernenia a pomoc malým a stredným podnikom, alebo ich nasmeruje na príslušné orgány, ktoré im poskytnú usmernenia a pomoc, pokiaľ ide o otázky súvisiace s kybernetickou bezpečnosťou. Členské štáty sa tiež nabádajú, aby mikropodnikom a malým podnikom, ktoré nemajú takéto kapacity, ponúkali služby, ako je konfigurácia a protokolovanie webových stránok.

(57) Členské štáty by mali v rámci svojich národných stratégií kybernetickej bezpečnosti prijať politiky na podporu aktívnej kybernetickej ochrany ako súčasti širšej obrannej stratégie. Aktívna kybernetická ochrana je aktívna prevencia, odhaľovanie, monitorovanie, analýza a zmierňovanie narušení bezpečnosti siete v spojení s využitím spôsobilostí nasadených v zasiahnutej sieti a mimo nej, a nie reaktívne reagovanie. Mohla by zahŕňať poskytovanie bezplatných služieb alebo nástrojov určitým subjektom zo strany členských štátov, a to vrátane samoobslužných kontrol, detekčných nástrojov a služieb odstraňovania. Schopnosť rýchlo a automaticky si vymieňať a pochopiť informácie a analýzy týkajúce sa hrozieb, varovaní pred kybernetickou činnosťou a opatrení reakcie je zásadne dôležitá pre umožnenie jednotného úsilia o úspešnú prevenciu, odhaľovanie, riešenie a blokovanie útokov proti sieťam a informačným systémom. Aktívna kybernetická ochrana je založená na obrannej stratégii, ktorá vylučuje ofenzívne opatrenia.

(58) Keďže využívanie zraniteľností v sieťach a informačných systémoch môže spôsobiť značné narušenie a škody, rýchla identifikácia a náprava takýchto zraniteľností je dôležitým faktorom pri znižovaní rizika. Subjekty, ktoré vyvíjajú alebo spravujú siete a informačné systémy, by preto mali zaviesť vhodné postupy na riešenie zistených zraniteľností. Keďže zraniteľnosti často odhaľujú a zverejňujú tretie strany, výrobca alebo poskytovateľ produktov IKT alebo služieb IKT by mal zaviesť aj potrebné postupy na prijímanie informácií o zraniteľnosti od tretích strán. V tejto súvislosti sa v medzinárodných normách ISO/IEC 30111 a ISO/IEC 29147 poskytujú usmernenia na riešenie zraniteľností a na poskytovanie informácií o zraniteľnostiach. Na umožnenie dobrovoľného rámca pre zverejňovanie zraniteľností je obzvlášť dôležité posilnenie koordinácie medzi oznamujúcimi fyzickými a právnickými osobami a výrobcami alebo poskytovateľmi produktov IKT alebo služieb IKT. Koordinované zverejňovanie zraniteľností stanovuje štruktúrovaný proces, v rámci ktorého sa zraniteľnosti hlásia výrobcovi alebo poskytovateľovi potenciálne zraniteľných produktov IKT alebo služieb IKT takým spôsobom, ktorý mu umožňuje diagnostikovať a odstrániť zraniteľnosť pred tým, ako sa podrobné informácie o zraniteľnosti poskytnú tretím stranám alebo verejnosti. Koordinované zverejňovanie zraniteľností by malo zahŕňať aj koordináciu medzi oznamujúcou fyzickou alebo právnickou osobou a výrobcom alebo poskytovateľom potenciálne zraniteľných produktov IKT alebo služieb IKT, pokiaľ ide o načasovanie nápravy a zverejnenie zraniteľností.

(59) Komisia, agentúra ENISA a členské štáty by mali naďalej podporovať zosúlaďovanie s medzinárodnými normami a existujúcimi najlepšími odvetvovými postupmi v oblasti riadenia kybernetických rizík, napríklad v oblastiach posudzovania bezpečnosti dodávateľského reťazca, výmeny informácií a poskytovania informácií o zraniteľnostiach.

(60) Členské štáty v spolupráci s agentúrou ENISA by mali prijať opatrenia na uľahčenie koordinovaného zverejňovania zraniteľností zavedením príslušnej vnútroštátnej politiky. V rámci svojej vnútroštátnej politiky by sa členské štáty mali snažiť v súlade s vnútroštátnym právom v čo najväčšej miere riešiť výzvy, ktorým čelia výskumníci zaoberajúci sa zraniteľnosťami, vrátane ich možného vystavenia sa trestnej zodpovednosti. Vzhľadom na to, že fyzické a právnické osoby, ktoré skúmajú zraniteľnosti, by v niektorých členských štátoch mohli byť vystavené trestnej a občianskoprávnej zodpovednosti, členské štáty sa nabádajú, aby prijali usmernenia týkajúce sa nestíhania výskumníkov v oblasti bezpečnosti informácií a udelenia výnimky z občianskoprávnej zodpovednosti za ich činnosti.

(61) Členské štáty by mali určiť jednu zo svojich jednotiek CSIRT ako koordinátora, ktorý by v prípade potreby pôsobil ako dôveryhodný sprostredkovateľ medzi oznamujúcimi fyzickými alebo právnickými osobami a výrobcami alebo poskytovateľmi produktov IKT alebo služieb IKT, v prípade ktorých je pravdepodobné, že budú dotknuté danou zraniteľnosťou. Úlohy jednotky CSIRT určenej za koordinátora by mali zahŕňať identifikáciu a kontaktovanie dotknutých subjektov, pomoc fyzickým alebo právnickým osobám oznamujúcim zraniteľnosť, rokovania o harmonograme zverejňovania a riadenie zraniteľností, ktoré majú vplyv na viaceré subjekty (viacstranné

koordinované zverejňovanie zraniteľností). Ak by oznámená zraniteľnosť mohla mať významný vplyv na subjekty vo viac ako jednom členskom štáte, jednotky CSIRT určené za koordinátorov by mali podľa potreby spolupracovať v rámci siete jednotiek CSIRT.

(62) Prístup k správnym a včasným informáciám o zraniteľnostiach ovplyvňujúcich produkty IKT a služby IKT prispieva k lepšiemu riadeniu kybernetických rizík. Zdroje verejne dostupných informácií o zraniteľnostiach sú dôležitým nástrojom pre subjekty a používateľov ich služieb, ale aj pre príslušné orgány a jednotky CSIRT. Z tohto dôvodu by agentúra ENISA mala zriadiť európsku databázu zraniteľností, v ktorej by subjekty, bez ohľadu nato, či patria do rozsahu pôsobnosti tejto smernice, a ich dodávatelia sietí a informačných systémov, ako aj príslušné orgány a jednotky CSIRT, mohli dobrovoľne zverejňovať a registrovať verejne známe zraniteľnosti s cieľom umožniť používateľom prijať vhodné zmierňujúce opatrenia. Cieľom uvedenej databázy je riešiť jedinečné výzvy, ktoré riziká predstavujú pre subjekty v Únii. Agentúra ENISA by okrem toho mala zaviesť vhodný postup, pokiaľ ide o proces zverejňovania, s cieľom poskytnúť subjektom čas na prijatie opatrení na zmiernenie ich zraniteľností a zaviesť najmodernejšie opatrenia na riadenie kybernetických rizík, ako aj strojovo čitateľné súbory údajov a zodpovedajúce rozhrania. S cieľom podporiť kultúru zverejňovania zraniteľností by zverejnenie nemalo spôsobiť žiadnu ujmu oznamujúcej fyzickej alebo právnickej osobe.

(63) Hoci podobné registre alebo databázy zraniteľností existujú, ich hostiteľmi a správcami sú subjekty, ktoré nie sú usadené v Únii. Európska databáza zraniteľností vedená agentúrou ENISA by zabezpečila lepšiu transparentnosť, pokiaľ ide o proces zverejňovania pred tým, ako je daná zraniteľnosť verejne oznámená, ako aj odolnosť v prípade narušenia alebo prerušenia poskytovania podobných služieb. S cieľom v čo najväčšej miere zabrániť duplicite úsilia a usilovať sa o komplementárnosť by agentúra ENISA mala preskúmať možnosť uzatvorenia dohôd o štruktúrovanej spolupráci s podobnými registrami alebo databázami, ktoré patria do právomoci tretích krajín. Agentúra ENISA by mala preskúmať najmä možnosť úzkej spolupráce s prevádzkovateľmi systému spoločných zraniteľností a expozícií (CVE).

(64) Skupina pre spoluprácu by mala podporovať a uľahčovať strategickú spoluprácu a výmenu informácií a tiež posilňovať dôveru medzi členskými štátmi. Skupina pre spoluprácu by mala každé dva roky stanoviť pracovný program. Pracovný program by mal zahŕňať opatrenia, ktoré má skupina pre spoluprácu vykonať na plnenie svojich cieľov a úloh. Časový rámec na stanovenie prvého pracovného programu podľa tejto smernice by sa mal zosúladiť s časovým rámcom posledného pracovného programu stanoveného podľa smernice (EÚ) 2016/1148 s cieľom zabrániť možným narušeniam práce skupiny pre spoluprácu.

(65) Pri vypracúvaní usmerňujúcich dokumentov by skupina pre spoluprácu mala dôsledne zmapovať vnútroštátne riešenia a skúsenosti, posúdiť vplyv výstupov skupiny pre spoluprácu na vnútroštátne prístupy, diskutovať o výzvach pri vykonávaní a formulovať konkrétne odporúčania, najmä pokiaľ ide o uľahčenie zosúladenia pri transpozícii tejto smernice medzi členskými štátmi, ktoré sa má dosiahnuť lepším vykonávaním existujúcich pravidiel. Skupina pre spoluprácu by mohla zmapovať aj vnútroštátne riešenia s cieľom podporiť kompatibilitu riešení v oblasti kybernetickej bezpečnosti uplatňovaných v každom konkrétnom odvetví v celej Únii. Týka sa to najmä odvetví, ktoré majú medzinárodný alebo cezhraničný charakter.

(66) Skupina pre spoluprácu by mala zostať flexibilným fórom a mala by byť schopná reagovať na meniace sa a nové politické priority a výzvy a zároveň zohľadňovať dostupnosť zdrojov. Mohla by organizovať pravidelné spoločné stretnutia s príslušnými súkromnými zainteresovanými stranami z celej Únie s cieľom prediskutovať činnosti skupiny pre spoluprácu a zhromažďovať údaje a informácie o nových politických výzvach. Skupina pre spoluprácu by okrem toho mala pravidelne posudzovať súčasný stav kybernetických hrozieb alebo incidentov, ako je ransomvér. S cieľom posilniť spoluprácu na úrovni Únie by skupina pre spoluprácu mala zvážiť prizývanie

relevantných inštitúcií, orgánov, úradov a agentúr Únie zapojených do politiky v oblasti kybernetickej bezpečnosti, ako je Európsky parlament, Europol, Európsky výbor pre ochranu údajov, Agentúra Európskej únie pre bezpečnosť letectva zriadená nariadením (EÚ) 2018/1139 a Agentúra Európskej únie pre vesmírny program zriadená nariadením Európskeho parlamentu a Rady (EÚ) 2021/696 ([14]), k účasti na svojej práci.

(67) Príslušné orgány a jednotky CSIRT by mali mať možnosť zúčastňovať sa na výmenných programoch pre úradníkov z iných členských štátov na základe osobitného rámca a podľa potreby pod podmienkou požadovanej bezpečnostnej previerky úradníkov zúčastňujúcich sa na takýchto výmenných programoch, a to s cieľom zlepšovať spoluprácu a posilniť dôveru medzi členskými štátmi. Príslušné orgány by mali prijať potrebné opatrenia, ktoré úradníkom z iných členských štátov umožnia zohrávať účinnú úlohu v činnostiach hostiteľského príslušného orgánu alebo hostiteľskej jednotky CSIRT.

(68) Členské štáty by mali prispieť k vytvoreniu rámca EÚ pre reakciu na kybernetické krízy, ako sa stanovuje v odporúčaní Komisie (EÚ) 2017/1584 ([15]), prostredníctvom existujúcich sietí spolupráce, najmä Európskej siete styčných organizácií pre kybernetické krízy (ďalej len „EU-CyCLONe“), siete jednotiek CSIRT a skupiny pre spoluprácu. Sieť EU-CyCLONe a sieť jednotiek CSIRT by mali spolupracovať na základe procesných opatrení, v ktorých sa spresňujú podrobnosti danej spolupráce, pričom by sa mali vyhnúť akejkoľvek duplicite úloh. V rokovacom poriadku siete EU-CyCLONe by sa mali ďalej spresniť mechanizmy fungovania danej siete vrátane úloh siete, prostriedkov spolupráce, interakcií s inými relevantnými aktérmi a vzorových formulárov na výmenu informácií, ako aj komunikačných prostriedkov. Pokiaľ ide o krízové riadenie na úrovni Únie, príslušné strany by sa mali opierať o integrované dojednania EÚ o politickej reakcii na krízu podľa vykonávacieho rozhodnutia Rady (EÚ) 2018/1993 ([16]) (dojednania IPCR). Komisia by mala na uvedený účel využiť ARGUS – medziodvetvový krízový koordinačný proces na vysokej úrovni. Ak má kríza výrazný externý rozmer alebo sa týka spoločnej bezpečnostnej a obrannej politiky, mal by sa aktivovať mechanizmus reakcie Európskej služby pre vonkajšiu činnosť na krízy.

(69) V súlade s prílohou k odporúčaniu (EÚ) 2017/1584 by rozsiahly kybernetický incident mal znamenať incident, ktorý spôsobí narušenie na úrovni presahujúcej schopnosť členského štátu naň reagovať alebo ktorý má významný vplyv aspoň na dva členské štáty. Rozsiahle kybernetické incidenty sa v závislosti od svojej príčiny a dosahu môžu vystupňovať a naplno prepuknúť v krízu, ktorá neumožňuje riadne fungovanie vnútorného trhu alebo predstavuje vážne riziká pre verejnú bezpečnosť a ochranu subjektov alebo občanov v niekoľkých členských štátoch alebo v Únii ako celku. Vzhľadom na široký rozsah a vo väčšine prípadov cezhraničný charakter takýchto incidentov by členské štáty a príslušné inštitúcie, orgány, úrady a agentúry Únie mali spolupracovať na technickej, prevádzkovej a politickej úrovni s cieľom riadne koordinovať reakciu v celej Únii.

(70) Rozsiahle kybernetické incidenty a krízy na úrovni Únie si z dôvodu vysokého stupňa previazanosti odvetví a členských štátov vyžadujú koordinované opatrenia na zabezpečenie rýchlej a účinnej reakcie. Dostupnosť kyberneticky odolných sietí a informačných systémov a dostupnosť, dôvernosť a integrita údajov sú nevyhnutné pre bezpečnosť Únie a ochranu jej občanov, podnikov a inštitúcií pred incidentmi a kybernetickými hrozbami, ako aj pre posilnenie dôvery jednotlivcov a organizácií v schopnosť Únie podporovať a chrániť globálny, otvorený, slobodný, stabilný a bezpečný kybernetický priestor založený na ľudských právach, základných slobodách, demokracii a právnom štáte.

([14]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/696 z 28. apríla 2021, ktorým sa zriaďuje Vesmírny program Únie a Agentúra Európskej únie pre vesmírny program a ktorým sa zrušujú nariadenia (EÚ) č. 912/2010, (EÚ) č. 1285/2013 a (EÚ) č. 377/2014 a rozhodnutie č. 541/2014/EÚ (Ú. v. EÚ L 170, 12.5.2021, s. 69).

([15]) Odporúčanie Komisie (EÚ) 2017/1584 z 13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu (Ú. v. EÚ L 239, 19.9.2017, s. 36).

([16]) Vykonávacie rozhodnutie Rady (EÚ) 2018/1993 z 11. decembra 2018 o dojednaniach EÚ o integrovanej politickej reakcii na krízu (Ú. v. EÚ L 320, 17.12.2018, s. 28).

(71) Sieť EU-CyCLONe by mala fungovať ako sprostredkovateľ medzi technickou a politickou úrovňou počas rozsiahlych kybernetických incidentov a kríz a mala by posilniť spoluprácu na operačnej úrovni a podporovať rozhodovanie na politickej úrovni. V spolupráci s Komisiou a so zreteľom na právomoci Komisie v oblasti krízového riadenia by sieť EU-CyCLONe mala vychádzať zo zistení siete jednotiek CSIRT a využívať svoje vlastné kapacity na vypracovanie analýzy vplyvu rozsiahlych kybernetických incidentov a kríz.

(72) Kybernetické útoky majú cezhraničnú povahu a významný incident môže narušiť a poškodiť kritické informačné infraštruktúry, od ktorých závisí hladké fungovanie vnútorného trhu. Odporúčanie (EÚ) 2017/1584 sa zaoberá úlohami všetkých príslušných aktérov. Komisia je okrem toho v rámci mechanizmu Únie v oblasti civilnej ochrany zriadeného rozhodnutím Európskeho parlamentu a Rady č. 1313/2013/EÚ ([17]) zodpovedná za všeobecné opatrenia v oblasti pripravenosti vrátane riadenia Koordinačného centra pre reakcie na núdzové situácie a spoločného systému komunikácie a poskytovania informácií v prípade núdzových situácií, udržiavania a ďalšieho rozvoja situačnej informovanosti a analytických kapacít a vytvárania a riadenia schopnosti mobilizovať a vysielať tímy odborníkov v prípade žiadosti o pomoc z členského štátu alebo tretej krajiny. Komisia je zodpovedná aj za poskytovanie analytických správ týkajúcich sa dojednaní IPCR podľa vykonávacieho rozhodnutia (EÚ) 2018/1993, a to aj v súvislosti so situačnou informovanosťou a pripravenosťou v oblasti kybernetickej bezpečnosti, ako aj za situačnú informovanosť a reakciu na krízy v oblastiach poľnohospodárstva, nepriaznivých poveternostných podmienok, mapovania a predpovedania konfliktov, systémov včasného varovania pred prírodnými katastrofami, núdzových zdravotných situácií, dohľadu nad infekčnými chorobami, zdravia rastlín, chemických incidentov, bezpečnosti potravín a krmív, zdravia zvierat, migrácie, colníctva, jadrových a rádiologických núdzových situácií, a energetiky.

(73) Únia môže v prípade potreby v súlade s článkom 218 ZFEÚ uzatvárať medzinárodné dohody s tretími krajinami alebo medzinárodnými organizáciami, ktorými môže povoľovať a organizovať ich účasť na určitých činnostiach skupiny pre spoluprácu, siete jednotiek CSIRT a siete EU-CyCLONe. Takýmito dohodami by sa mali zabezpečiť záujmy Únie a primeraná ochrana údajov. Nemalo by sa tým vylučovať právo členských štátov spolupracovať s tretími krajinami v oblasti riadenia zraniteľností a riadenia kybernetických rizík, uľahčenia oznamovania a všeobecnej výmeny informácií v súlade s právom Únie.

(74) S cieľom uľahčiť účinné vykonávanie tejto smernice, okrem iného pokiaľ ide o riadenie zraniteľností, opatrenia na riadenie kybernetických rizík, oznamovacie povinnosti a dohody o výmene informácií o kybernetickej bezpečnosti, môžu členské štáty spolupracovať s tretími krajinami a vykonávať činnosti, ktoré sa považujú za vhodné na daný účel, vrátane výmeny informácií o kybernetických hrozbách, incidentoch, zraniteľnostiach, nástrojoch a metódach, taktikách, technikách a postupoch, pripravenosti a cvičení v oblasti zvládania kybernetických kríz, odbornej prípravy, budovania dôvery a dohôd o štruktúrovanej výmene informácií.

(75) Mali by sa zaviesť vzájomné hodnotenia s cieľom pomáhať učiť sa zo spoločných skúseností, posilňovať vzájomnú dôveru a dosahovať vysokú spoločnú úroveň kybernetickej bezpečnosti. Partnerské preskúmania môžu viesť k cenným poznatkom a odporúčaniam, ktoré posilnia celkové spôsobilosti kybernetickej bezpečnosti, čím sa vytvorí ďalšia funkčná cesta na výmenu najlepších postupov medzi členskými štátmi a prispeje k zvýšeniu úrovne vyspelosti členských štátov v oblasti kybernetickej bezpečnosti. V partnerských preskúmaniach by sa mali zohľadniť výsledky podobných mechanizmov, ako je systém partnerského preskúmania siete jednotiek CSIRT, a mali by prinášať pridanú hodnotu a vyhýbať sa duplicite. Zavedením partnerských preskúmaní by nemalo byť dotknuté právo Únie alebo vnútroštátne právo v oblasti ochrany dôverných alebo utajovaných skutočností.

(76) Skupina pre spoluprácu by mala pre členské štáty zaviesť metodiku sebahodnotenia so zámerom pokryť faktory, ako je úroveň implementácie opatrení na riadenie kybernetických rizík a oznamovacích povinností, úroveň spôsobilostí a efektívnosť výkonu úloh príslušných orgánov, operačných spôsobilostí jednotiek CSIRT, úroveň implementácie vzájomnej pomoci, úrovne implementácie dohôd o výmene informácií o kybernetickej bezpečnosti alebo špecifických otázok cezhraničnej alebo medziodvetvovej povahy. Členským štátom by sa malo odporúčať, aby pravidelne vykonávali sebahodnotenia a aby výsledky svojho sebahodnotenia prezentovali a prediskutovali v rámci skupiny pre spoluprácu.

([17]) Rozhodnutie Európskeho parlamentu a Rady č. 1313/2013/EÚ zo 17. decembra 2013 o mechanizme Únie v oblasti civilnej ochrany (Ú. v. EÚ L 347, 20.12.2013, s. 924).

(77) Zodpovednosť za zaisťovanie bezpečnosti sietí a informačných systémov nesú vo veľkej miere kľúčové a dôležité subjekty. Mala by sa podporovať a rozvíjať kultúra riadenia rizika vrátane posudzovania rizika a vykonávania takých opatrení na riadenie kybernetických rizík, ktoré sú primerané existujúcim rizikám.

(78) Opatrenia na riadenie kybernetických rizík by mali zohľadňovať stupeň závislosti kľúčového alebo dôležitého subjektu od sietí a informačných systémov a mali by zahŕňať opatrenia na identifikáciu rizika incidentov, opatrenia na predchádzanie incidentom, ich odhaľovanie, reakciu na ne a zotavenie sa z nich, ako aj opatrenia na zmiernenie ich vplyvu. Bezpečnosť sietí a informačných systémov by mala zahŕňať bezpečnosť uchovávaných, prenášaných a spracúvaných údajov. Opatrenia na riadenie kybernetických rizík by mali zabezpečovať systémovú analýzu, pri ktorej sa zohľadní ľudský faktor, s cieľom získať úplný obraz o bezpečnosti siete a informačného systému.

(79) Keďže ohrozenie bezpečnosti sietí a informačných systémov môže mať rôzny pôvod, v opatreniach na riadenie kybernetických rizík by sa mal uplatňovať prístup všetkých nebezpečenstiev, ktorého cieľom je ochrana sietí a informačných systémov a fyzické prostredie uvedených systémov pred udalosťami, ako je krádež, požiar, povodeň, výpadok telekomunikácie alebo elektrickej energie, alebo pred neoprávneným fyzickým prístupom, poškodením alebo zásahom v súvislosti s informáciami kľúčového alebo dôležitého subjektu a jeho zariadeniami na spracovanie informácií, čo by mohlo ohroziť dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov. Opatrenia na riadenie kybernetických rizík by sa preto mali zaoberať aj fyzickou a environmentálnou bezpečnosťou sietí a informačných systémov tým, že budú zahŕňať opatrenia na ochranu takýchto systémov pred systémovými zlyhaniami, ľudskými chybami, zlomyseľným konaním alebo prírodnými javmi v súlade s európskymi a medzinárodnými normami, ako sú normy uvedené v sérii ISO/IEC 27000. V tejto súvislosti by sa kľúčové a dôležité subjekty mali v rámci svojich opatrení na riadenie kybernetických rizík zaoberať aj bezpečnosťou ľudských zdrojov a mali by mať zavedené vhodné postupy kontroly prístupu. Uvedené opatrenia by mali byť v súlade so smernicou (EÚ) 2022/2557.

(80) Na účely preukázania súladu s opatreniami na riadenie kybernetických rizík a v prípade neexistencie vhodných európskych systémov certifikácie kybernetickej bezpečnosti prijatých v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2019/881 ([18]) by členské štáty mali konzultáciou so skupinou pre spoluprácu a európskou skupinou pre certifikáciu kybernetickej bezpečnosti podporovať používanie príslušných európskych a medzinárodných noriem kľúčovými a dôležitými subjektmi alebo môžu vyžadovať, aby subjekty používali certifikované produkty IKT, služby IKT a procesy IKT.

(81) S cieľom vyhnúť sa neprimeranému finančnému a administratívnemu zaťaženiu kľúčových a dôležitých subjektov by opatrenia na riadenie kybernetických rizík mali byť primerané rizikám, ktorým čelí daná sieť a daný informačný systém, a zohľadňovať najnovší technický vývoj v oblasti takýchto opatrení a podľa potreby príslušné európske a medzinárodné normy, ako aj náklady na ich vykonávanie.

(82) Opatrenia na riadenie kybernetických rizík by mali byť primerané stupňu vystavenia kľúčového alebo dôležitého subjektu rizikám a spoločenskému a hospodárskemu vplyvu, ktorý by incident mal. Pri stanovovaní opatrení na riadenie kybernetických rizík prispôsobených kľúčovým a dôležitým subjektom by sa mala náležite zohľadniť odlišná expozícia kľúčových a dôležitých subjektov voči rizikám, napríklad kritickosť subjektu, riziká vrátane spoločenských rizík, ktorým je vystavený, veľkosť subjektu a pravdepodobnosť výskytu incidentov a ich závažnosť vrátane ich spoločenského a hospodárskeho vplyvu.

([18]) 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).

(83) Kľúčové a dôležité subjekty by mali zaistiť bezpečnosť sietí a informačných systémov, ktoré používajú vo svojich činnostiach. Ide predovšetkým o súkromné siete a informačné systémy, ktoré spravujú interní IT pracovníci kľúčových a dôležitých subjektov alebo ktorých bezpečnosť zaisťujú externí dodávatelia. Opatrenia na riadenie kybernetických rizík a oznamovacie povinnosti stanovené v tejto smernici by sa mali vzťahovať na príslušné kľúčové a dôležité subjekty bez ohľadu na to, či uvedené subjekty vykonávajú údržbu svojich sietí a informačných systémov interne alebo ju zabezpečujú externe.

(84) Poskytovatelia služieb DNS, správcovia názvov TLD, poskytovatelia služieb cloud computingu, poskytovatelia služieb dátového centra, poskytovatelia sietí na sprístupňovanie obsahu, poskytovatelia riadených služieb, poskytovatelia riadených bezpečnostných služieb, poskytovatelia online trhov, internetových vyhľadávačov a platforiem služieb sociálnej siete a poskytovatelia dôveryhodných služieb by vzhľadom na svoj cezhraničný charakter mali podliehať vysokej miere harmonizácie na úrovni Únie. Vykonávanie opatrení na riadenie kybernetických rizík by sa preto malo, pokiaľ ide o uvedené subjekty, uľahčiť vykonávacím aktom.

(85) Riešenie rizík vyplývajúcich z dodávateľského reťazca subjektu a jeho vzťahu s dodávateľmi, ako sú poskytovatelia služieb ukladania a spracúvania údajov alebo poskytovatelia riadených bezpečnostných služieb a vydavatelia softvéru, je obzvlášť dôležité vzhľadom na výskyt incidentov, keď sa subjekty stali obeťami kybernetických útokov a keď páchatelia s nekalými úmyslami dokázali ohroziť bezpečnosť sietí a informačných systémov subjektu využitím zraniteľností v produktoch a službách tretích strán. Kľúčové a dôležité subjekty by preto mali posúdiť a zohľadniť celkovú kvalitu a odolnosť produktov a služieb, opatrenia na riadenie kybernetických rizík, ktoré zahŕňajú, a postupy svojich dodávateľov a poskytovateľov služieb v oblasti kybernetickej bezpečnosti vrátane ich bezpečných vývojových postupov. Kľúčové a dôležité subjekty by sa mali nabádať najmä k tomu, aby začlenili opatrenia na riadenie kybernetických rizík do zmluvných dohôd so svojimi priamymi dodávateľmi a poskytovateľmi služieb. Uvedené subjekty by mohli zvážiť riziká, ktoré vyplývajú zo strany dodávateľov a poskytovateľov služieb ďalších úrovní.

(86) Spomedzi poskytovateľov služieb zohrávajú poskytovatelia riadených bezpečnostných služieb osobitne dôležitú úlohu v pomoci subjektom v ich úsilí o prevenciu, odhaľovanie incidentov, reakciu na ne alebo zotavenie sa z nich, a to v takých oblastiach, ako je reakcia na incidenty, penetračné testovanie, bezpečnostné audity a poradenstvo. Avšak aj samotní poskytovatelia riadených bezpečnostných služieb boli cieľom kybernetických útokov a ich úzke zapojenie do činnosti subjektov predstavuje osobitné riziko. Kľúčové a dôležité subjekty by preto mali výberu poskytovateľa riadených bezpečnostných služieb venovať zvýšenú pozornosť.

(87) Príslušné orgány môžu v kontexte svojich úloh dohľadu využívať aj služby v oblasti kybernetickej bezpečnosti, ako sú bezpečnostné audity, penetračné testovanie alebo reakcie na incidenty.

(88) Kľúčové a dôležité subjekty by mali riešiť aj riziká vyplývajúce z ich interakcií a vzťahov s inými zainteresovanými stranami v rámci širšieho ekosystému, a to aj s cieľom bojovať proti priemyselnej špionáži a chrániť obchodné tajomstvo. Predovšetkým by uvedené subjekty mali prijať vhodné opatrenia, aby sa ich spolupráca s akademickými a výskumnými inštitúciami uskutočňovala v súlade s ich politikami v oblasti kybernetickej bezpečnosti a aby sa riadila osvedčenými postupmi, pokiaľ ide o bezpečný prístup k informáciám a ich šírenie vo všeobecnosti, a konkrétne o ochranu duševného vlastníctva. Podobne by kľúčové a dôležité subjekty, ak sú závislé od služieb v oblasti transformácie údajov a analýzy údajov od tretích strán, mali prijať všetky vhodné opatrenia na riadenie kybernetických rizík, a to vzhľadom na význam a hodnotu údajov pre svoju činnosť.

(89) Kľúčové a dôležité subjekty by mali prijať širokú škálu základných postupov v oblasti kybernetickej hygieny, ako sú zásady nulovej dôvery, aktualizácie softvéru, konfigurácia zariadení, segmentácia siete, správa identít a prístupu alebo informovanosť používateľov, organizovať školenia pre svojich zamestnancov a zvyšovať informovanosť o kybernetických hrozbách, phishingu alebo technikách sociálneho inžinierstva. Okrem toho by uvedené subjekty mali vyhodnotiť vlastné spôsobilosti v oblasti kybernetickej bezpečnosti a podľa potreby sa usilovať o integráciu technológií posilňujúcich kybernetickú bezpečnosť, ako sú systémy umelej inteligencie alebo strojového učenia, s cieľom posilniť svoje spôsobilosti a bezpečnosť sietí a informačných systémov.

(90) V záujme ďalšieho riešenia rizík kľúčového dodávateľského reťazca a pomoci kľúčovým a dôležitým subjektom pôsobiacim v odvetviach, na ktoré sa vzťahuje táto smernica, pri náležitom riadení rizík súvisiacich s dodávateľským reťazcom a dodávateľmi, by skupina pre spoluprácu mala v spolupráci s Komisiou a agentúrou ENISA a podľa potreby po konzultácii s relevantnými zainteresovanými stranami vrátane priemyslu vykonať koordinované posúdenia bezpečnostných rizík kritických dodávateľských reťazcov, ktoré sa už vykonali v prípade sietí 5G v nadväznosti na odporúčanie Komisie (EÚ) 2019/534 ([19]) s cieľom identifikovať za každé odvetvie kritické služby IKT, systémy IKT alebo produkty IKT, relevantné hrozby a zraniteľnosti. Takéto koordinované posúdenia bezpečnostných rizík by mali určiť opatrenia, plány zmierňovania a najlepšie postupy vo vzťahu ku kritickým závislostiam, potenciálnym jediným bodom zlyhania, hrozbám, zraniteľnostiam a ďalším rizikám spojeným s dodávateľským reťazcom a mali by preskúmať spôsoby, ako ešte viac podporiť ich širšie prijatie kľúčovými a dôležitými subjektmi. Potenciálne netechnické rizikové faktory, ako je neprimeraný vplyv tretej krajiny na dodávateľov a poskytovateľov služieb, najmä v prípade alternatívnych modelov riadenia, zahŕňajú skryté zraniteľnosti alebo zadné dvierka a potenciálne systémové narušenie dodávok, najmä v prípade odkázanosti na určitého dodávateľa technológie alebo závislosti od poskytovateľa.

(91) Pri koordinovanom posudzovaní bezpečnostných rizík v kritických dodávateľských reťazcoch by sa vzhľadom na vlastnosti dotknutého odvetvia mali zohľadniť technické a v relevantných prípadoch aj netechnické faktory vrátane tých, ktoré sú vymedzené v odporúčaní (EÚ) 2019/534, v koordinovanom posúdení rizík na úrovni EÚ v oblasti kybernetickej bezpečnosti sietí 5G a v súbore nástrojov EÚ pre kybernetickú bezpečnosť 5G, na ktorom sa dohodla skupina pre spoluprácu. Pri určovaní dodávateľských reťazcov, ktoré by mali podliehať koordinovanému posúdeniu bezpečnostných rizík, by sa mali zohľadniť tieto kritériá: i) rozsah, v akom kľúčové a dôležité subjekty využívajú konkrétne kritické služby IKT, systémy IKT alebo produkty IKT a spoliehajú sa na ne; ii) relevantnosť konkrétnych kritických služieb IKT, systémov IKT alebo produktov IKT pre vykonávanie kritických alebo citlivých funkcií vrátane spracúvania osobných údajov; iii) dostupnosť alternatívnych služieb IKT, systémov IKT alebo produktov IKT; iv) odolnosť celkového dodávateľského reťazca služieb IKT, systémov IKT alebo produktov IKT počas ich životného cyklu voči rušivým udalostiam a v) v prípade vznikajúcich služieb IKT, systémov IKT alebo produktov IKT ich potenciálny budúci význam pre činnosti subjektov. Okrem toho by sa osobitný dôraz mal klásť na služby IKT, systémy IKT alebo produkty IKT, na ktoré sa vzťahujú osobitné požiadavky, ktoré pochádzajú z tretích krajín.

(92) S cieľom zjednodušiť povinnosti uložené poskytovateľom verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb a poskytovateľom dôveryhodných služieb v súvislosti s bezpečnosťou ich sietí a informačných systémov, ako aj umožniť uvedeným subjektom a príslušným orgánom podľa smernice Európskeho parlamentu a Rady (EÚ) 2018/1972 ([20]) a nariadenia (EÚ) č. 910/2014 využívať právny rámec stanovený touto smernicou vrátane určenia jednotky CSIRT zodpovednej za riešenie incidentov a účasti dotknutých príslušných orgánov na činnostiach skupiny pre spoluprácu a siete jednotiek CSIRT, by tieto subjekty mali patriť do rozsahu pôsobnosti tejto smernice. Zodpovedajúce ustanovenia nariadenia (EÚ) č. 910/2014 a smernice (EÚ) 2018/1972 týkajúce sa stanovenia požiadaviek na bezpečnosť a oznamovanie pre uvedené typy subjektov by sa preto mali vypustiť. Pravidlami týkajúcimi sa oznamovacích povinností stanovenými v tejto smernici by nemalo byť dotknuté nariadenie (EÚ) 2016/679 a smernica 2002/58/ES.

(93) Povinnosti v oblasti kybernetickej bezpečnosti stanovené v tejto smernici by sa mali považovať za doplnkové k požiadavkám uloženým poskytovateľom dôveryhodných služieb podľa nariadenia (EÚ) č. 910/2014. Od poskytovateľov dôveryhodných služieb by sa malo vyžadovať, aby prijali všetky vhodné a primerané opatrenia na riadenie rizík ohrozujúcich ich služby, a to aj vo vzťahu k zákazníkom a spoliehajúcim sa tretím stranám, a aby oznamovali incidenty podľa tejto smernice. Takéto povinnosti v oblasti kybernetickej bezpečnosti a oznamovania by sa mali týkať aj fyzickej ochrany poskytovaných služieb. Požiadavky na kvalifikovaných poskytovateľov dôveryhodných služieb stanovené v článku 24 nariadenia (EÚ) č. 910/2014 sa naďalej uplatňujú.

([19]) Odporúčanie Komisie (EÚ) 2019/534 z 26. marca 2019 Kybernetická bezpečnosť sietí 5G (Ú. v. EÚ L 88, 29.3.2019, s. 42).

([20]) Smernica Európskeho parlamentu a Rady (EÚ) 2018/1972 z 11. decembra 2018, ktorou sa stanovuje európsky kódex elektronických komunikácií (Ú. v. EÚ L 321, 17.12.2018, s. 36).

(94) Členské štáty môžu prideliť úlohu príslušných orgánov, pokiaľ ide o dôveryhodné služby, orgánom dohľadu podľa nariadenia (EÚ) č. 910/2014 s cieľom zabezpečiť pokračovanie súčasných postupov a stavať na poznatkoch a skúsenostiach získaných pri uplatňovaní uvedeného nariadenia. V takom prípade by príslušné orgány podľa tejto smernice mali úzko a včas spolupracovať s uvedenými orgánmi dohľadu formou výmeny relevantných informácií s cieľom zabezpečiť účinný dohľad a súlad poskytovateľov dôveryhodných služieb s požiadavkami stanovenými v tejto smernici a v nariadení (EÚ) č. 910/2014. V náležitých prípadoch by jednotka CSIRT alebo príslušný orgán podľa tejto smernice mal bezodkladne informovať orgán dohľadu podľa nariadenia (EÚ) č. 910/2014 o každej oznámenej významnej kybernetickej hrozbe alebo incidente ovplyvňujúcich dôveryhodné služby, ako aj o akomkoľvek porušení tejto smernice zo strany poskytovateľa dôveryhodných služieb. Na účely oznamovania môžu členské štáty podľa potreby použiť jednotný vstupný bod zriadený v záujme dosiahnutia spoločného a automatického oznamovania incidentov orgánu dohľadu podľa nariadenia (EÚ) č. 910/2014 a jednotke CSIRT alebo príslušnému orgánu podľa tejto smernice.

(95) V prípade potreby a s cieľom zabrániť zbytočnému narušeniu by sa pri transpozícii tejto smernice mali zohľadniť existujúce vnútroštátne usmernenia prijaté na účely transpozície pravidiel týkajúcich sa bezpečnostných opatrení stanovených v článkoch 40 a 41 smernice (EÚ) 2018/1972, čím by sa stavalo na poznatkoch a skúsenostiach získaných podľa smernice (EÚ) 2018/1972 v súvislosti s bezpečnostnými opatreniami a oznamovaním incidentov. Agentúra ENISA môže vypracovať aj usmernenia zamerané na požiadavky týkajúce sa bezpečnosti a na oznamovacie povinnosti určené poskytovateľom verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb s cieľom uľahčiť harmonizáciu a prechod a minimalizovať narušenie. Členské štáty môžu prideliť úlohu príslušných orgánov pre elektronické komunikácie národným regulačným orgánom podľa smernice (EÚ) 2018/1972 s cieľom zabezpečiť pokračovanie súčasných postupov a stavať na poznatkoch a skúsenostiach získaných pri vykonávaní uvedenej smernice.

(96) Vzhľadom na rastúci význam interpersonálnych komunikačných služieb nezávislých od číslovania, ako sú vymedzené v smernici (EÚ) 2018/1972, je potrebné zabezpečiť, aby takéto služby tiež podliehali príslušným bezpečnostným požiadavkám vzhľadom na ich špecifický charakter a hospodársky význam. Keďže priestor na útoky sa naďalej rozširuje, interpersonálne komunikačné služby nezávislé od číslovania, ako sú služby zasielania správ, sa stávajú veľmi rozšírenými vektormi útokov. Páchatelia s nekalými úmyslami využívajú platformy na komunikáciu s obeťami a ich nalákanie na otvorenie napadnutých webových stránok, čím sa zvyšuje pravdepodobnosť incidentov zahŕňajúcich zneužívanie osobných údajov, čo má následne vplyv na bezpečnosť sietí a informačných systémov. Poskytovatelia interpersonálnych komunikačných služieb nezávislých od číslovania by mali zabezpečiť takú úroveň bezpečnosti sietí a informačných systémov, ktorá zodpovedá daným rizikám. Vzhľadom na to, že poskytovatelia interpersonálnych komunikačných služieb nezávislých od číslovania obyčajne nemajú skutočnú kontrolu nad prenosom signálov v sieťach, miera rizík pre takéto služby sa môže v niektorých aspektoch považovať za nižšiu ako v prípade tradičných elektronických komunikačných služieb. To isté platí pre interpersonálne komunikačné služby, ako sú vymedzené v smernici (EÚ) 2018/1972, ktoré využívajú čísla a ktoré nemajú skutočnú kontrolu nad prenosom signálu.

(97) Vnútorný trh je viac než kedykoľvek závislý od fungovania internetu. Služby takmer všetkých kľúčových a dôležitých subjektov sú závislé od služieb poskytovaných cez internet. V záujme zabezpečenia bezproblémového poskytovania služieb kľúčovými a dôležitými subjektmi je dôležité, aby všetci poskytovatelia verejných elektronických komunikačných sietí mali zavedené vhodné opatrenia na riadenie kybernetických rizík a aby oznamovali významné incidenty, ktoré sa ich týkajú. Členské štáty by mali zabezpečiť zachovanie bezpečnosti verejných elektronických komunikačných sietí a ochranu svojich životne dôležitých bezpečnostných záujmov pred sabotážou a špionážou. Keďže medzinárodná konektivita zlepšuje a urýchľuje konkurencieschopnú digitalizáciu Únie a jej hospodárstva, incidenty ovplyvňujúce podmorské komunikačné káble by sa mali oznamovať jednotke CSIRT alebo prípadne príslušnému orgánu. V národnej stratégii kybernetickej bezpečnosti by sa v prípade potreby mala zohľadňovať kybernetická bezpečnosť podmorských komunikačných káblov a mala by zahŕňať mapovanie potenciálnych kybernetických rizík a zmierňujúce opatrenia na zabezpečenie najvyššej úrovne ich ochrany.

(98) S cieľom zaistiť bezpečnosť verejných elektronických komunikačných sietí a verejne dostupných elektronických komunikačných služieb by sa malo podporovať používanie šifrovacích technológií, najmä šifrovania bez medzifáz, ako aj bezpečnostných koncepcií zameraných na údaje, ako je kartografia, segmentácia, označovanie, politika prístupu a riadenie prístupu a automatizované rozhodnutia o prístupe. V prípade potreby by malo byť používanie šifrovania, najmä šifrovania bez medzifáz, povinné pre poskytovateľov verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb v súlade so zásadami štandardnej a špecificky navrhnutej bezpečnosti a ochrany súkromia na účely tejto smernice. Používanie šifrovania bez medzifáz by sa malo zosúladiť s právomocami členských štátov na zabezpečenie ochrany ich základných bezpečnostných záujmov a verejnej bezpečnosti a na umožnenie prevencie, vyšetrovania, odhaľovania a stíhania trestných činov v súlade s právom Únie. Nemalo by to však oslabiť šifrovanie bez medzifáz, ktoré je zásadnou technológiou pre účinnú ochranu údajov a súkromia a bezpečnosti komunikácií.

(99) S cieľom zaistiť bezpečnosť a zabrániť zneužívaniu verejných elektronických komunikačných sietí a verejne dostupných elektronických komunikačných služieb a manipulácii s nimi by sa malo podporovať používanie noriem bezpečného smerovania, aby sa zabezpečila integrita a spoľahlivosť funkcií smerovania v rámci celého ekosystému poskytovateľov služieb prístupu k internetu.

(100) V záujme zabezpečenia funkčnosti a integrity internetu a podpory bezpečnosti a odolnosti DNS by sa mali príslušné zainteresované strany vrátane subjektov súkromného sektora, poskytovateľov verejne dostupných elektronických komunikačných služieb, najmä poskytovateľov služieb prístupu k internetu, a poskytovateľov internetových vyhľadávačov v Únii nabádať k tomu, aby prijali stratégiu diverzifikácie rozlišovania DNS. Členské štáty by navyše mali podporovať rozvoj a používanie verejnej a bezpečnej európskej služby resolverov DNS.

(101) V tejto smernici sa stanovuje viacfázový prístup k oznamovaniu významných incidentov s cieľom nájsť správnu rovnováhu medzi rýchlym oznamovaním na jednej strane, ktoré pomáha zmierniť potenciálne šírenie významných incidentov a umožňuje kľúčovým a dôležitým subjektom hľadať pomoc, a na druhej strane podávaním podrobných správ, ktoré poskytuje cenné ponaučenia z jednotlivých incidentov a časom zlepšuje kybernetickú odolnosť jednotlivých subjektov a celých odvetví. V tejto súvislosti by táto smernica mala zahŕňať oznamovanie incidentov, pri ktorých by sa na základe prvotného posúdenia vykonaného dotknutým subjektom mohlo predpokladať, že by mohli viesť k vážnemu narušeniu prevádzky služieb alebo finančným stratám uvedeného subjektu alebo by mohli zasiahnuť iné fyzické alebo právnické osoby tým, že by im spôsobili značnú majetkovú alebo nemajetkovú ujmu. V takomto prvotnom posúdení by sa mali zohľadniť okrem iného dotknuté siete a informačné systémy, najmä ich význam pri poskytovaní služieb subjektu, závažnosť a technické vlastnosti kybernetickej hrozby a všetky súvisiace zraniteľnosti, ktoré sa využívajú, ako aj skúsenosti subjektu s podobnými incidentmi. Ukazovatele, ako je rozsah, v akom je zasiahnuté fungovanie služby, trvanie incidentu alebo počet zasiahnutých príjemcov služieb, by mohli zohrávať dôležitú úlohu pri určovaní toho, či je narušenie prevádzky služby závažné.

(102) Keď sa kľúčové alebo dôležité subjekty dozvedia o významnom incidente, mali by byť povinné vyhlásiť včasné varovanie bezodkladne a v každom prípade do 24 hodín. Po uvedenom včasnom varovaní by malo nasledovať oznámenie o incidente. Dotknuté subjekty by mali nahlásiť incident bezodkladne a v každom prípade do 72 hodín po tom, ako sa dozvedia o významnom incidente, najmä za účelom aktualizácie informácií poskytnutých vo včasnom varovaní a s uvedením prvotného hodnotenia významného incidentu, vrátane jeho závažnosti a vplyvu, ako aj prípadných ukazovateľov narušenia. Záverečná správa by sa mala zaslať najneskôr jeden mesiac po nahlásení incidentu. Včasné varovanie by malo obsahovať len tie informácie, ktoré sú potrebné na oznámenie významného incidentu jednotke CSIRT, prípadne príslušnému orgánu, a na základe ktorých môže dotknutý subjekt v prípade potreby požiadať o pomoc. V takomto včasnom varovaní by sa malo uviesť prípadné podozrenie, či bol významný incident spôsobený konaním, ktoré je nezákonné alebo so zlým úmyslom, a či môže mať cezhraničný dosah. Členské štáty by mali zabezpečiť, aby povinnosť zaslať uvedené včasné varovanie alebo následné oznámenie

o incidente neodvádzala zdroje oznamujúceho subjektu od činností súvisiacich s riešením incidentu, ktoré by mali mať prednosť, aby pre povinnosť oznámiť incident nedochádzalo k odvádzaniu zdrojov od riešenia reakcie na významné incidenty alebo k inému ohrozeniu úsilia subjektu v uvedenej súvislosti. Ak v čase zaslania záverečnej správy incident ešte prebieha, členské štáty ba mali zabezpečiť, aby dotknuté subjekty v uvedenom čase poskytli priebežnú správu a záverečnú správu vypracovali do jedného mesiaca odo dňa, keď významný incident vyriešili.

(103) V prípade potreby by kľúčové a dôležité subjekty mali bez zbytočného odkladu informovať príjemcov svojich služieb o akýchkoľvek opatreniach alebo prostriedkoch nápravy, ktoré môžu prijať na zmiernenie rizík vyplývajúcich z významnej kybernetickej hrozby. Uvedené subjekty by mali tiež v prípade potreby, a najmä ak je pravdepodobné, že významná kybernetická hrozba sa naplní, informovať príjemcov svojich služieb aj o samotnej hrozbe. Požiadavka informovať týchto príjemcov o významných kybernetických hrozbách by sa mala splniť s vynaložením maximálneho úsilia, ale nemala by uvedené subjekty zbaviť povinnosti na vlastné náklady prijať vhodné a okamžité opatrenia na prevenciu alebo odstránenie akýchkoľvek takýchto hrozieb a obnovenie bežnej úrovne bezpečnosti služby. Takéto informácie o významných kybernetických hrozbách by sa mali príjemcom služieb poskytovať bezplatne a mali by byť formulované v ľahko zrozumiteľnom jazyku.

(104) Poskytovatelia verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb by mali uplatňovať špecificky navrhnutú a štandardnú bezpečnosť a informovať príjemcov svojich služieb o významných kybernetických hrozbách a o opatreniach, ktoré môžu prijať na ochranu bezpečnosti svojich zariadení a svojej komunikácie, napríklad použitím určitých typov softvéru alebo šifrovacích technológií.

(105) Aktívny prístup ku kybernetickým hrozbám je základnou súčasťou riadenia rizík kybernetickej bezpečnosti, ktoré by malo príslušným orgánom umožniť účinne zabrániť tomu, aby sa z kybernetických hrozieb stali incidenty, ktoré by mohli spôsobiť značnú materiálnu alebo nemateriálnu ujmu. Preto je oznamovanie kybernetických hrozieb mimoriadne dôležité. Na uvedený účel sa subjektom odporúča, aby kybernetické hrozby oznamovali dobrovoľne.

(106) S cieľom zjednodušiť oznamovanie informácií požadovaných podľa tejto smernice, ako aj znížiť administratívnu záťaž pre subjekty, členské štáty by na poskytovanie relevantných informácií, ktoré sa majú oznamovať, mali poskytnúť technické prostriedky ako jednotný kontaktné miesto, automatizované systémy, online formuláre, ľahko použiteľné rozhrania, šablóny, špecializované platformy na použitie pre subjekty, bez ohľadu na to, či patria do rozsahu pôsobnosti tejto smernice. Financovanie Únie na podporu vykonávanie tejto smernice, najmä v rámci programu Digitálna Európa zriadeného nariadením Európskeho parlamentu a Rady (EÚ) 2021/694 ([21]), by mohlo zahŕňať podporu jednotných kontaktných miest. Navyše subjekty sa často nachádzajú v situácii, keď sa konkrétny incident z dôvodu jeho charakteristík musí oznámiť rôznym orgánom v dôsledku oznamovacej povinnosti zahrnutej v rôznych právnych nástrojoch. Takéto prípady vytvárajú dodatočnú administratívnu záťaž a mohli by viesť aj k nejasnostiam, pokiaľ ide o formát a postupy takéhoto oznamovania. Ak je zriadené jednotné kontaktné miesto, členským štátom sa odporúča, aby toto jednotné kontaktné miesto používali aj na oznamovanie bezpečnostných incidentov, ktoré sa vyžaduje podľa iných právnych predpisov Únie, než je nariadenie (EÚ) 2016/679 a smernica 2002/58/ES. Používanie takéhoto 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. Agentúra ENISA v spolupráci so skupinou pre spoluprácu by mala vypracovať spoločné vzorové formuláre oznámení prostredníctvom usmernení na zjednodušenie a zefektívnenie poskytovania informácií, ktoré sa majú oznamovať podľa práva Únie, a na zníženie administratívnej záťaže pre oznamujúce subjekty.

(107) Ak existuje podozrenie, že incident súvisí so závažnou trestnou činnosťou podľa práva Únie alebo vnútroštátneho práva, členské štáty by mali nabádať kľúčové a dôležité subjekty na základe platných pravidiel trestného konania v súlade s právom Únie, aby príslušným orgánom presadzovania práva oznamovali incidenty, pri ktorých existuje podozrenie o ich súvise so závažnou trestnou činnosťou. V prípade potreby a bez toho, aby boli dotknuté pravidlá ochrany osobných údajov, ktoré sa vzťahujú na Europol, je žiaduce, aby Európske centrum boja proti počítačovej kriminalite (EC3) a agentúra ENISA uľahčili koordináciu medzi príslušnými orgánmi a orgánmi presadzovania práva jednotlivých členských štátov.

([21]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/694 z 29. apríla 2021, ktorým sa zriaďuje program Digitálna Európa a zrušuje rozhodnutie (EÚ) 2015/2240 (Ú. v. EÚ L 166, 11.5.2021, s. 1).

(108) V dôsledku incidentov je v mnohých prípadoch ohrozená ochrana osobných údajov. V uvedenej súvislosti by príslušné orgány mali spolupracovať a vymieňať si informácie o všetkých relevantných záležitostiach s orgánmi uvedenými v nariadení (EÚ) 2016/679 a smernici 2002/58/ES.

(109) Udržiavanie presných a úplných databáz registračných údajov názvov domén (údaje WHOIS) a poskytovanie zákonného prístupu k takýmto údajom je nevyhnutné na zaistenie bezpečnosti, stability a odolnosti DNS, čo zase prispieva k vysokej spoločnej úrovni kybernetickej bezpečnosti v celej Únii. Na tento konkrétny účel by sa od registrov názvov TLD a subjektov poskytujúcich služby registrácie názvov domén malo vyžadovať spracovanie určitých údajov potrebných na dosiahnutie uvedeného účelu. Takéto spracovanie by malo byť zo zákona povinné v zmysle článku 6 ods. 1 písm. c) nariadenia (EÚ) 2016/679. Uvedenou povinnosťou nie je dotknutá možnosť zhromažďovať registračné údaje názvov domén na iné účely, napríklad na základe zmluvných dojednaní alebo právnych požiadaviek ustanovených v iných právnych predpisoch Únie alebo členských štátov. Cieľom uvedenej povinnosti je získať úplný a presný súbor registračných údajov a nemala by viesť k opakovanému zberu tých istých údajov. Na zamedzenie duplicity uvedenej úlohy by registre názvov TLD a subjekty poskytujúce služby registrácie názvov domén mali navzájom spolupracovať.

(110) Dostupnosť a včasná prístupnosť registračných údajov názvov domén pre legitímnych žiadateľov o prístup je nevyhnutná na prevenciu a boj proti zneužívaniu DNS a na prevenciu a odhaľovanie incidentov a na reakciu na ne. Legitímnymi žiadateľmi o prístup sa rozumie akákoľvek fyzická alebo právnická osoba, ktorá podala žiadosť podľa práva Únie alebo vnútroštátneho práva. Môžu k nim patriť orgány, ktoré sú príslušné podľa tejto smernice, a orgány, ktoré sú podľa práva Únie alebo vnútroštátneho práva príslušné na prevenciu, vyšetrovanie, odhaľovanie alebo stíhanie trestných činov a jednotky CERT alebo CSIRT. Od registrov názvov TLD a subjektov poskytujúcich služby registrácie názvov domén by sa malo vyžadovať, aby legitímnym žiadateľom o prístup ku konkrétnym údajom o registrácii názvov domén, ktoré sú potrebné na účely žiadosti o prístup, umožnili zákonný prístup v súlade s právom Únie a členského štátu. K žiadosti oprávnených žiadateľov o prístup by malo byť pripojené odôvodnenie, ktoré umožní posúdiť potrebu prístupu k údajom.

(111) S cieľom zabezpečiť dostupnosť presných a úplných registračných údajov názvov domén by správcovia registrov názvov TLD a subjekty poskytujúce služby registrácie názvov domén mali zhromažďovať registračné údaje názvov domén a zaručovať ich integritu a dostupnosť. Správcovia registrov názvov TLD a subjekty poskytujúce služby registrácie názvov domén by mali najmä stanoviť politiky a postupy zhromažďovania a uchovávania presných a úplných registračných údajov názvov domén, ako aj predchádzania nepresným registračným údajom a ich opravy, v súlade s právom Únie v oblasti ochrany údajov. Uvedené politiky a postupy by mali v rámci možností zohľadňovať normy vypracované štruktúrami riadenia so zapojením viacerých zainteresovaných strán na medzinárodnej úrovni. Registre názvov TLD a subjekty poskytujúce služby registrácie názvov domén by mali prijať a zaviesť primerané postupy na overovanie registračných údajov názvov domén. Uvedené postupy by mali odzrkadľovať najlepšie postupy používané v tejto oblasti a v rámci možností aj pokrok v oblasti elektronickej identifikácie. K príkladom overovacích postupov môžu patriť kontroly *ex ante* vykonávané v čase registrácie a kontroly *ex post* vykonávané po registrácii. Registre názvov TLD a subjekty poskytujúce služby registrácie názvov domén by mali najmä overovať aspoň jednu možnosť kontaktu žiadateľa o registráciu.

(112) Od registrov názvov TLD a subjektov poskytujúcich služby registrácie názvov domén, by sa v súlade s úvodnými ustanoveniami nariadenia (EÚ) 2016/679 malo požadovať, aby zverejňovali registračné údaje názvov domén, ktoré nepatria do rozsahu pôsobnosti práva Únie v oblasti ochrany údajov, ako sú údaje o právnických osobách. V prípade právnických osôb by registre názvov TLD a subjekty poskytujúce služby registrácie názvov domén mali verejne sprístupniť aspoň meno/názov žiadateľa o registráciu a kontaktné telefónne číslo. Zverejnená by mala byť aj kontaktná e-mailová adresa, ak neobsahuje osobné údaje, ako je to v prípade použitia e-mailových aliasov alebo funkčných účtov. Registre názvov TLD a subjekty poskytujúce služby registrácie názvov domén by oprávneným záujemcom o prístup mali tiež umožniť zákonný prístup k špecifickým registračným údajom názvov domén týkajúcich sa fyzických osôb podľa práva Únie v oblasti ochrany údajov. Členské štáty by mali vyžadovať, aby registre názvov TLD a subjekty poskytujúce služby registrácie názvov domén bez zbytočného odkladu reagovali na žiadosti o sprístupnenie registračných údajov názvov domén od oprávnených žiadateľov o prístup. Registre názvov TLD a subjekty poskytujúce služby registrácie názvov domén by na vybavovanie žiadostí o sprístupnenie od oprávnených žiadateľov o prístup mali stanoviť politiky a postupy zverejňovania a sprístupňovania registračných údajov vrátane dohôd o úrovni poskytovaných služieb. Uvedené politiky a postupy by mali v rámci možností zohľadňovať všetky usmernenia a normy vypracované štruktúrami riadenia so zapojením viacerých

zainteresovaných strán na medzinárodnej úrovni. Súčasťou postupu sprístupnenia by mohlo byť aj použitie rozhrania, portálu alebo iného technického nástroja na zabezpečenie účinného systému na podávanie žiadostí o poskytnutie registračných údajov a prístupu k nim. Na podporu harmonizovaného postupu na celom vnútornom trhu môže Komisia bez toho, aby boli dotknuté právomoci Európskeho výboru pre ochranu údajov, poskytovať usmernenia o takýchto postupoch, ktoré pokiaľ možno zohľadnia normy vypracované viacstrannými riadiacimi štruktúrami na medzinárodnej úrovni. Členské štáty by mali zabezpečiť, aby všetky druhy prístupu k osobným a iným ako osobným registračným údajom názvov domén boli bezplatné.

(113) Subjekty patriace do rozsahu pôsobnosti tejto smernice by sa mali považovať za subjekty podliehajúce právomoci členského štátu, v ktorom sú usadené. Poskytovatelia verejných elektronických komunikačných sietí alebo poskytovatelia verejne dostupných elektronických komunikačných služieb by sa však mali považovať za poskytovateľov podliehajúcich právomoci členského štátu, v ktorom poskytujú služby. Poskytovatelia služieb DNS, správcovia názvov TLD, subjekty, ktoré poskytujú služby registrácie názvov domén pre TLD, poskytovatelia služieb cloud computingu, poskytovatelia služieb dátových centier, poskytovatelia sietí na sprístupňovanie obsahu, poskytovatelia riadených služieb, poskytovatelia riadených bezpečnostných služieb, ako aj o poskytovatelia online trhov, internetových vyhľadávačov a platforiem služieb sociálnych sietí by mali byť považovaní za subjekty podliehajúce právomoci toho členského štátu, v ktorom majú hlavnú prevádzkareň v Únii. Subjekty verejnej správy by mali podliehať právomoci členského štátu, v ktorom sú usadené. Ak subjekt poskytuje služby alebo je usadený vo viac ako jednom členskom štáte, mal by podliehať samostatnej a súbežnej právomoci každého z týchto členských štátov. Príslušné orgány uvedených členských štátov by mali spolupracovať, vzájomne si pomáhať a v prípade potreby vykonávať spoločné opatrenia dohľadu. Ak členské štáty vykonávajú právomoc, podľa zásady *ne bis in idem* by nemali ukladať opatrenia presadzovania práva alebo sankcie za rovnaké počínanie viac ako raz.

(114) S cieľom zohľadniť cezhraničnú povahu služieb a operácií poskytovateľov služieb DNS, registrov názvov TLD by subjekty poskytujúce služby registrácie názvov domén, poskytovatelia služieb cloud computingu, poskytovatelia služieb dátových centier, poskytovatelia sietí na sprístupňovanie obsahu, poskytovatelia riadených služieb, poskytovatelia riadených bezpečnostných služieb, ako aj o poskytovatelia online trhov, internetových vyhľadávačov a platforiem služieb sociálnych sietí mali podliehať právomoci iba jedného členského štátu. Právomoc by mal mať ten členský štát, v ktorom má dotknutý subjekt hlavnú prevádzkareň v Únii. Z kritéria prevádzkarne na účely tejto smernice vyplýva skutočné vykonávanie činnosti na základe stabilných dojednaní. Právna forma takýchto dojednaní, či už ide o pobočku alebo dcérsku spoločnosť s právnou subjektivitou, nie je v tomto ohľade určujúcim faktorom. Splnenie uvedeného kritéria by nemalo závisieť od toho, či sa sieť a informačné systémy fyzicky nachádzajú na danom mieste; samotná prítomnosť a používanie takýchto systémov ako takých nepredstavuje hlavnú prevádzkareň, a preto nejde o rozhodujúce kritérium na určenie hlavnej prevádzkarne. Za hlavnú prevádzkareň by sa mal považovať členský štát, kde sa najčastejšie prijímajú rozhodnutia o opatreniach na riadenie rizík kybernetickej bezpečnosti. Zvyčajne bude zodpovedať miestu ústredia subjektov v Únii. Ak takýto členský štát nemožno určiť alebo ak sa takéto rozhodnutia neprijímajú v Únii, za hlavnú prevádzkareň by sa mal považovať členský štát, v ktorom sa operácie kybernetickej bezpečnosti vykonávajú. Ak takýto členský štát nemožno určiť, za hlavnú prevádzkareň by sa mal považovať členský štát, v ktorom má subjekt prevádzkareň s najvyšším počtom zamestnancov v Únii. Ak služby vykonáva skupina podnikov, hlavná prevádzkareň riadiaceho podniku by sa mala považovať za hlavnú prevádzkareň skupiny podnikov.

(115) Ak verejne dostupnú rekurzívnu službu DNS poskytuje poskytovateľ verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb len ako súčasť služby prístupu na internet, subjekt by sa mal považovať za subjekt podliehajúci právomoci všetkých členských štátov, v ktorých sa jeho služby poskytujú.

(116) Ak poskytovateľ služieb DNS, register názvov TLD, subjekt, ktorý poskytuje služby registrácie názvov domén, poskytovateľ služieb cloud computingu, poskytovateľ služieb dátového centra, poskytovateľ sietí na sprístupňovanie obsahu, poskytovateľ riadených služieb, poskytovateľ riadených bezpečnostných služieb alebo poskytovateľ online trhu, internetového vyhľadávača a platformy služieb sociálnych sietí, ktorý nie je usadený v Únii a v Únii poskytuje služby, mal by určiť v Únii zástupcu. Aby bolo možné určiť, či takýto subjekt poskytuje služby v Únii, malo by sa zistiť, či daný subjekt mieni poskytovať služby osobám v jednom alebo vo viacerých členských štátoch. Samotná dostupnosť webového sídla subjektu alebo jeho sprostredkovateľa v Únii alebo e-mailovej adresy alebo iných kontaktných údajov alebo použitie jazyka, ktorý sa všeobecne používa v tretej krajine, v ktorej je subjekt usadený, by sa na potvrdenie takého úmyslu malo považovať za nedostatočné. Na základe faktorov, ako je používanie jazyka alebo meny bežne používaných v jednom alebo vo viacerých členských štátoch s možnosťou objednania služieb v tomto jazyku alebo zmienka o zákazníkoch alebo používateľoch, ktorí sa nachádzajú v Únii, by však mohlo byť zjavné, že subjekt hodlá poskytovať služby v Únii. Zástupca by mal konať v mene subjektu a príslušné orgány alebo jednotky CSIRT by mali mať možnosť obrátiť sa na neho. Subjekt by mal prostredníctvom písomného mandátu výslovne určiť zástupcu oprávneného konať v mene subjektu v súvislosti s jeho povinnosťami stanovenými v tejto smernici vrátane oznamovania incidentov.

(117) Na zabezpečenie jednoznačného prehľadu by poskytovatelia služieb DNS, správcovia názvov TLD, subjekty poskytujúce služby registrácie názvov domén pre TLD, poskytovatelia služieb cloud computingu, poskytovatelia služieb dátových centier, poskytovatelia sietí na sprístupňovanie obsahu, poskytovatelia riadených služieb, poskytovatelia riadených bezpečnostných služieb, ako aj o poskytovatelia online trhov, internetových vyhľadávačov a platforiem služieb sociálnych sietí, ktorí poskytujú služby v celej Únii a patria do pôsobnosti tejto smernice, by agentúra ENISA mala zriadiť a viesť register takýchto subjektov na základe informácií poskytnutých členským štátom, prípadne aj prostredníctvom vnútroštátnych mechanizmov zriadených pre subjekty, aby sa registrovali samé. Agentúre ENISA by informácie a všetky ich zmeny mali odovzdávať jednotné kontaktné miesta. Na zabezpečenie presnosti a úplnosti informácií, ktoré sa majú zapísať do uvedeného registra, môžu členské štáty zasielať agentúre ENISA informácie o týchto subjektoch dostupné v ľubovoľných vnútroštátnych registroch. Agentúra ENISA a členské štáty by mali prijať opatrenia na podporu interoperability takýchto registrov a zároveň zabezpečiť ochranu dôverných informácií alebo utajovaných skutočností. Na zaistenie bezpečnosti a dôvernosti sprístupnených informácií a obmedzenie prístupu, uchovávania a prenosu takýchto informácií predpokladaným používateľom by agentúra ENISA mala zaviesť príslušné protokoly na klasifikáciu a riadenie informácií.

(118) Ak sa informácie, ktoré sú utajované v súlade s právom Únie alebo vnútroštátnym právom, vymieňajú, oznamujú alebo inak zdieľajú podľa tejto smernice, mali by sa uplatňovať príslušné pravidlá zaobchádzania s utajovanými skutočnosťami. Agentúra ENISA by okrem toho mala mať zavedenú infraštruktúru, postupy a pravidlá pre citlivé a utajované skutočnosti v súlade s platnými bezpečnostnými predpismi na ochranu utajovaných skutočností EÚ.

(119) Keďže kybernetické hrozby sú čoraz zložitejšie a sofistikovanejšie, dobré opatrenia na odhaľovanie takýchto hrozieb a ich prevenciu do značnej miery závisia od pravidelného zdieľania spravodajských informácií o hrozbách a zraniteľnosti medzi subjektmi. Zdieľanie informácií prispieva k zvýšenej informovanosti o kybernetických hrozbách, čo zase zvyšuje schopnosť subjektov predchádzať tomu, aby sa takéto hrozby stali incidentmi, a subjektom umožňuje lepšie obmedziť vplyvy incidentov a účinnejšie sa z nich zotaviť. Keďže na úrovni Únie príslušné usmernenia neexistujú, zdá sa, že takémuto zdieľaniu spravodajských informácií bránia rôzne faktory, najmä neistá zlučiteľnosť s pravidlami hospodárskej súťaže a zodpovednosti.

(120) Členské štáty by mali subjektom odporúčať a pomáhať im v spoločnom využívaní svojich individuálnych znalostí a praktických skúseností na strategickej, taktickej a operačnej úrovni s cieľom zlepšiť si spôsobilosti na primeranú prevenciu a detekciu hrozieb, reakciu na ne alebo zotavenie z incidentov či zmiernenie ich vplyvu. Preto je potrebné umožniť na úrovni Únie vznik dobrovoľného zdieľania informácií o kybernetickej bezpečnosti. Na uvedený účel by členské štáty mali aktívne pomáhať a povzbudzovať subjekty, ako sú subjekty poskytujúce služby a výskum kybernetickej bezpečnosti, ako aj príslušné subjekty, ktoré nepatria do rozsahu pôsobnosti tejto smernice, aby sa zúčastňovali na takýchto dohodách o výmene informácií o kybernetickej bezpečnosti. Uvedené dohody by sa mali uzatvárať v súlade s pravidlami Únie pre hospodársku súťaž a právom Únie v oblasti ochrany údajov.

(121) Spracovanie osobných údajov v nevyhnutnom a primeranom rozsahu na účely zaistenia bezpečnosti sieťových a informačných systémov kľúčovými a dôležitými subjektmi by sa mohlo považovať za zákonné na základe toho, že takéto spracovanie je v súlade so zákonnou povinnosťou, ktorej podlieha prevádzkovateľ v súlade s požiadavkami článku 6 ods. 1 písm. c) a článku 6 ods. 3 nariadenia (EÚ) 2016/679. Spracovanie osobných údajov by mohlo byť potrebné aj pre oprávnené záujmy kľúčových a dôležitých subjektov, ako aj pre poskytovateľov bezpečnostných technológií a služieb, ktorí konajú v mene uvedených subjektov podľa článku 6 ods. 1 písm. f) nariadenia (EÚ) 2016/679, a to aj vtedy, keď je takéto spracovanie nevyhnutné na účely dohôd o výmene informácií o kybernetickej bezpečnosti alebo dobrovoľného zasielania relevantných informácií v súlade s touto smernicou. Opatrenia súvisiace s prevenciou, odhaľovaním, identifikáciou, obmedzovaním následkov, analýzou incidentov a reakciami na ne, opatrenia na zvýšenie informovanosti o konkrétnych kybernetických hrozbách, výmena informácií v kontexte nápravy zraniteľnosti a koordinovaného zverejňovania zraniteľností, dobrovoľná výmena informácií o týchto incidentoch a o kybernetických hrozbách a zraniteľnostiach, ukazovatele kompromitácie, taktiky, techniky a postupy, kybernetické bezpečnostné varovania a konfiguračné nástroje by mohli vyžadovať spracovanie určitých kategórií osobných údajov, ako sú IP adresy, jednotné vyhľadávače prostriedkov (URL), názvy domén, e-mailové adresy, a ak tieto prezrádzajú osobné údaje, časové pečiatky. Spracovanie osobných údajov príslušnými orgánmi, jednotnými kontaktnými miestami a jednotkami CSIRT by mohlo založiť zákonnú povinnosť alebo by sa mohlo považovať za nevyhnutné na vykonanie úlohy vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi podľa článku 1 písm. c) alebo e) a článku 6 ods. 3 nariadenia (EÚ) 2016/679 alebo na sledovanie oprávneného záujmu kľúčových a dôležitých subjektov podľa článku 6 ods.), bod f) uvedeného nariadenia. Okrem toho by sa vo vnútroštátnom práve mohli stanoviť pravidlá umožňujúce príslušným orgánom, jednotným kontaktným miestam a jednotkám CSIRT v rozsahu, ktorý je potrebný a primeraný na účely zaistenia bezpečnosti sietí a informačných systémov kľúčových a dôležitých subjektov, spracovávať osobitné kategórie osobných údajov podľa článku 9 nariadenia (EÚ) 2016/679, najmä ustanovením vhodných konkrétnych opatrení na ochranu základných práv a záujmov fyzických osôb vrátane technických obmedzení opakovaného použitia takýchto údajov a použitia najmodernejších bezpečnostných opatrení a opatrení na ochranu súkromia, ako je pseudonymizácia alebo šifrovanie, ak anonymizácia môže výrazne ovplyvniť sledovaný účel.

(122) S cieľom posilniť právomoci a opatrenia v oblasti dohľadu, ktoré pomáhajú zabezpečiť účinné dodržiavanie predpisov, by sa v tejto smernici mal stanoviť minimálny zoznam opatrení a prostriedkov dohľadu, prostredníctvom ktorých môžu príslušné orgány vykonávať dohľad nad kľúčovými a dôležitými subjektmi. Okrem toho by sa touto smernicou malo zaviesť rozlišovanie režimu dohľadu nad kľúčovými a dôležitými subjektmi s cieľom zabezpečiť spravodlivú rovnováhu povinností pre uvedené subjekty a pre príslušné orgány. Kľúčové subjekty by preto mali podliehať komplexnému režimu dohľadu *ex ante* a *ex post*, pričom dôležité subjekty by mali podliehať iba ľahkému režimu dohľadu *ex post*. Od dôležitých subjektov by sa nemalo vyžadovať, aby systematicky dokumentovali súlad s opatreniami na riadenie rizík kybernetickej bezpečnosti, pričom príslušné orgány by k dohľadu mali pristupovať reaktívne *ex post*, a preto by nemali mať všeobecnú povinnosť vykonávať dohľad nad týmito subjektmi. Dohľad nad dôležitými subjektmi ex post môžu vyvolať dôkazy, indície alebo informácie, na ktoré boli príslušné orgány upozornené a ktoré tieto orgány považujú za potenciálne porušenie tejto smernice. Takéto dôkazy, indície alebo informácie môžu byť napríklad takého druhu, aký príslušným orgánom poskytujú iné orgány, subjekty, občania, médiá alebo iné zdroje alebo verejne dostupné informácie, alebo by mohli vyplynúť z iných činností, ktoré príslušné orgány vykonávajú pri plnení svojich úloh.

(123) Výkon úloh dohľadu príslušnými orgánmi by nemal zbytočne prekážať podnikateľskej činnosti dotknutého subjektu. Ak príslušné orgány vykonávajú svoje úlohy dohľadu vo vzťahu ku kľúčovým subjektom vrátane výkonu inšpekcií na mieste a dohľadu na diaľku, vyšetrovania porušení tejto smernice a výkonu bezpečnostných auditov alebo bezpečnostných skenov, mali by minimalizovať vplyv na podnikateľskú činnosť dotknutého subjektu.

(124) Pri výkone dohľadu *ex ante* by príslušné orgány mali mať možnosť primeraným spôsobom rozhodnúť o prednostnom použití opatrení a prostriedkov v oblasti dohľadu, ktoré majú k dispozícii. To znamená, že príslušné orgány môžu rozhodnúť o prednosti na základe metodík dohľadu, ktoré by mali vychádzať z prístupu založeného na riziku. Konkrétnejšie, takéto metodiky by mohli zahŕňať kritériá alebo referenčné hodnoty na klasifikáciu kľúčových subjektov do kategórií rizík a zodpovedajúce opatrenia a prostriedky v oblasti dohľadu odporúčané pre jednotlivé kategórie rizík, ako je použitie, frekvencia alebo typy inšpekcií na mieste, cielených bezpečnostných auditov alebo bezpečnostných kontrol, druh informácií, ktoré sa majú vyžadovať, a úroveň podrobnosti týchto informácií. Takéto metodiky dohľadu by mohli byť sprevádzané pracovnými programami a môžu sa pravidelne

posudzovať a preskúmavať, a to aj pokiaľ ide o aspekty, ako je prideľovanie zdrojov a potreby na úrovni zdrojov. V súvislosti so subjektmi verejnej správy by sa právomoci v oblasti dohľadu mali vykonávať v súlade s vnútroštátnymi rámcami právnych predpisov a inštitucionálnymi rámcami.

(125) Príslušné orgány by mali zabezpečiť, aby ich úlohy dohľadu vo vzťahu kú kľúčovým a dôležitým subjektom vykonávali školení odborníci, ktorí by na výkon týchto úloh mali mať potrebnú kvalifikáciu, najmä pokiaľ ide o výkon inšpekcií na mieste a dohľadu na diaľku, vrátane identifikácie slabých miest v databázach, hardvéri, firewalloch, šifrovaní a sieťach. Uvedené inšpekcie a uvedený dohľad by sa mali vykonávať objektívnym spôsobom.

(126) V riadne odôvodnených prípadoch, keď si je príslušný orgán vedomý závažnej kybernetickej hrozby alebo hroziaceho rizika, mal by mať možnosť prijímať okamžité rozhodnutia o presadzovaní práva s cieľom zabrániť incidentu alebo reagovať naň.

(127) Aby bolo presadzovanie práva účinné, mal by sa stanoviť minimálny zoznam právomocí presadzovania práva, ktoré sa môžu uplatňovať za porušenie opatrení v oblasti riadenia rizík kybernetickej bezpečnosti a oznamovania stanovených v tejto smernici, ktorým sa stanoví jasný a konzistentný rámec pre takéto presadzovanie práva v celej Únii. Náležitá pozornosť by sa mala venovať povahe, závažnosti a trvaniu porušenia tejto smernice, spôsobenej hmotnej a nehmotnej ujme nezávisle od toho, či bolo porušenie úmyselné alebo z nedbanlivosti, opatrení prijatých na zabránenie alebo zmiernenie hmotnej alebo nehmotnej ujmy, miere zodpovednosti alebo akémukoľvek relevantnému predchádzajúcemu porušeniu, miere spolupráce s príslušným orgánom a akýmkoľvek ďalším priťažujúcim alebo poľahčujúcim faktorom. Opatrenia presadzovania práva vrátane správnych pokút by mali byť primerané a ich ukladanie by malo podliehať primeraným procesným zárukám v súlade so všeobecnými zásadami práva Únie a Charty základných práv Európskej únie (ďalej len „charta“) vrátane účinného opravného prostriedku a spravodlivého procesu, prezumpcie neviny a práva na obhajobu.

(128) Táto smernica od členských štátov nevyžaduje, aby stanovili trestnoprávnu alebo občianskoprávnu zodpovednosť v súvislosti s fyzickými osobami zodpovednými za zabezpečenie súladu subjektu s touto smernicou za škodu, ktorú tretie strany utrpeli v dôsledku porušenia tejto smernice.

(129) S cieľom zabezpečiť účinné presadzovanie povinností stanovených v tejto smernici by mal mať každý príslušný orgán právomoc uložiť správne pokuty alebo požiadať o ich uloženie.

(130) Ak sa správna pokuta ukladá kľúčovému alebo dôležitému subjektu, ktorý je podnikom, na tieto účely by sa za podnik mal považovať podnik podľa článkov 101 a 102 ZFEÚ. Ak sa správna pokuta ukladá 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 rozhodnúť, či orgány verejnej moci budú podliehať správnym pokutám a do akej miery. Uloženie správnej pokuty nemá vplyv na uplatňovanie iných právomocí príslušných orgánov alebo iných sankcií stanovených vo vnútroštátnych predpisoch, ktorými sa transponuje táto smernica.

(131) Členské štáty by mali mať možnosť stanoviť pravidlá o trestných sankciách za porušenie vnútroštátnych pravidiel, ktorými sa transponuje táto smernica. Uloženie trestných sankcií za porušenia takýchto vnútroštátnych predpisov a uloženie súvisiacich správnych sankcií by však nemalo viesť k porušeniu zásady *ne bis in idem*, ako ju vykladá Súdny dvor Európskej únie.

(132) Členské štáty by mali zaviesť systém, ktorým sa zabezpečia účinné, primerané a odrádzajúce sankcie v prípadoch, keď sa touto smernicou neharmonizujú správne sankcie alebo, ak je to potrebné, aj v iných prípadoch, napríklad v prípade závažného porušenia tejto smernice. Povaha týchto sankcií a to, či sú trestné alebo správne, by sa mala určiť podľa vnútroštátneho práva.

(133) S cieľom ďalej posilniť účinnosť a odrádzajúci účinok opatrení presadzovania práva za porušenie tejto smernice by príslušné orgány mali byť oprávnené dočasne pozastaviť a požadovať dočasné pozastavenie certifikácie alebo povolenia časti alebo všetkých relevantných služieb alebo činností, ktoré poskytuje kľúčový subjekt, a požadovať uloženie dočasného zákazu fyzickej osobe vykonávať riadiace funkcie akoukoľvek fyzickou osobou na úrovni výkonného riaditeľa alebo právneho zástupcu. Takéto dočasné pozastavenia alebo zákazy by sa vzhľadom na svoju závažnosť a vplyv na činnosti subjektov a v konečnom dôsledku na používateľov mali uplatňovať len úmerne k závažnosti porušenia a s prihliadnutím na okolnosti každého jednotlivého prípadu vrátane skutočnosti, či išlo o úmyselné alebo nedbanlivostné porušenie, a akýchkoľvek opatrení prijatých na zabránenie alebo zmiernenie vzniknutej hmotnej alebo nehmotnej ujmy. Takéto dočasné pozastavenia alebo zákazy by sa mali uplatňovať len ako posledná možnosť, teda až po vyčerpaní ostatných príslušných opatrení na presadzovanie povinností stanovených v tejto smernici, a len do vtedy, kým dotknutý subjekt neprijme potrebné opatrenia na nápravu nedostatkov alebo na splnenie požiadaviek príslušného orgánu, v prípade ktorých sa takéto dočasné pozastavenia alebo zákazy uplatnili. Ukladanie takýchto dočasných pozastavení alebo zákazov by malo podliehať primeraným procesným zárukám v súlade so všeobecnými zásadami práva Únie a charty vrátane práva na účinný prostriedok nápravy a spravodlivý proces, prezumpcie neviny a práva na obhajobu.

(134) Na účely zabezpečenia, že subjekty budú dodržiavať svoje povinnosti stanovené v tejto smernici, by členské štáty mali spolupracovať a navzájom si pomáhať, pokiaľ ide o opatrenia dohľadu a presadzovania, najmä ak subjekt poskytuje služby vo viac ako jednom členskom štáte, alebo ak sa jeho sieť a informačné systémy nachádzajú v inom členskom štáte, než v ktorom poskytuje služby. Pri poskytovaní pomoci by mal dožiadaný príslušný orgán prijať opatrenia dohľadu alebo presadzovania v súlade s vnútroštátnym právom. S cieľom zabezpečiť bezproblémové fungovanie vzájomnej pomoci podľa tejto smernice by príslušné orgány mali využívať skupinu pre spoluprácu ako fórum na diskusiu o prípadoch a konkrétnych žiadostiach o pomoc.

(135) S cieľom zabezpečiť účinný dohľad a presadzovanie práva, najmä v situácii s cezhraničným rozmerom, by členský štát, ktorému bola doručená žiadosť o vzájomnú pomoc, mal v rozsahu uvedenej žiadosti prijať primerané opatrenia v oblasti dohľadu a presadzovania práva vo vzťahu k subjektu, ktorého sa uvedená žiadosť týka a ktorý poskytuje služby alebo má sieť a informačný systém na území uvedeného členského štátu.

(136) Touto smernicou by sa mali stanoviť pravidlá spolupráce medzi príslušnými orgánmi a dozornými orgánmi podľa nariadenia (EÚ) 2016/679 s cieľom riešiť porušenia tejto smernice týkajúce sa osobných údajov.

(137) Cieľom tejto smernice by malo byť zabezpečiť vysokú úroveň zodpovednosti za opatrenia v oblasti riadenia rizík kybernetickej bezpečnosti a oznamovacích povinností na úrovni kľúčových a dôležitých subjektov. Preto by riadiace orgány kľúčových a dôležitých subjektov mali schvaľovať opatrenia na riadenie rizík kybernetickej bezpečnosti a dohliadať na ich vykonávanie.

(138) S cieľom zabezpečiť vysokú úroveň kybernetickej bezpečnosti v celej Únii na základe tejto smernice by mala byť Komisia splnomocnená prijímať akty v súlade s článkom 290 ZFEÚ na doplnenie tejto smernice tým, že bližšie určí, od ktorých kategórií kľúčových a dôležitých subjektov sa má vyžadovať, aby používali určité certifikované produkty IKT, služby IKT a procesy IKT alebo získali certifikát v rámci niektorého európskeho systému kybernetickej bezpečnosti. 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 ([22]). 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 systematický prístup na zasadnutia skupín expertov Komisie, ktoré sa zaoberajú prípravou delegovaných aktov.

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

(139) S cieľom zabezpečiť jednotné podmienky vykonávania tejto smernice by sa mali na Komisiu preniesť vykonávacie právomoci, aby stanovila procesné opatrenia potrebné na fungovanie skupiny pre spoluprácu a technické a metodické, ako aj odvetvové požiadavky týkajúce sa opatrení na riadenie kybernetických rizík, a bližšie špecifikovala druh informácií, formát a postup v prípade incidentu, kybernetických hrozieb a oznámení o situáciách, keď takmer došlo k nehode, a oznamovania významných kybernetických hrozieb, ako aj prípadov, keď sa incident považuje za významný. Uvedené právomoci by sa mali vykonávať v súlade s nariadením Európskeho parlamentu a Rady (EÚ) č. 182/2011 ([23]).

(140) Komisia by mala túto smernicu pravidelne preskúmavať a po porade so zainteresovanými stranami najmä s cieľom určiť, či je vhodné navrhnúť zmeny vzhľadom na zmeny spoločenských, politických, technologických alebo trhových podmienok. V rámci týchto preskúmaní by Komisia mala posúdiť relevantnosť veľkosti dotknutých subjektov a odvetví, pododvetví a typu subjektu, uvedených v prílohách k tejto smernici pre fungovanie hospodárstva a spoločnosti v súvislosti s kybernetickou bezpečnosťou. Komisia by mala okrem iného posúdiť, či poskytovatelia patriaci do rozsahu pôsobnosti tejto smernice, ktorí sú v zmysle článku 33 nariadenia Európskeho parlamentu a Rady (EÚ) 2022/2065 ([24]) určení ako veľmi veľké online platformy, by sa podľa tejto smernice mohli považovať za kľúčové subjekty.

(141) Táto smernica vytvára nové úlohy pre agentúru ENISA, čím sa posilňuje jej úloha, a môže viesť tiež k tomu, že agentúra ENISA bude musieť vykonávať svoje súčasné úlohy podľa nariadenia (EÚ) 2019/881 na vyššej úrovni ako predtým. S cieľom zabezpečiť, aby agentúra ENISA mala potrebné finančné a ľudské zdroje na vykonávanie súčasných a nových úloh, ako aj na dosahovanie akejkoľvek vyššej úrovne výkonu uvedených úloh vyplývajúcich z jej posilnenej úlohy, jej rozpočet by sa mal adekvátne zvýšiť. Aby sa zabezpečilo efektívne využívanie zdrojov, agentúre ENISA by sa mala navyše poskytnúť väčšia flexibilita, pokiaľ ide o spôsob, akým je schopná interne prideľovať zdroje, s cieľom efektívneho výkonu úloh a plnenia očakávaní.

(142) Keďže cieľ tejto smernice, a to dosiahnutie vysokej spoločnej úrovne kybernetickej bezpečnosti v celej Únii, nie je možné uspokojivo dosiahnuť na úrovni samotných členských štátov, ale z dôvodov účinku opatrení 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 táto smernica neprekračuje rámec nevyhnutný na dosiahnutie tohto cieľa.

(143) V tejto smernici sa rešpektujú základné práva a dodržiavajú zásady uznané v charte, najmä právo na rešpektovanie súkromného života a komunikácií, ochranu osobných údajov, slobodu podnikania, právo vlastniť majetok, právo na účinný prostriedok nápravy a na spravodlivý proces, prezumpcia neviny a právo na obhajobu. Právo na účinný prostriedok nápravy sa vzťahuje aj na príjemcov služieb poskytovaných kľúčovými a dôležitými subjektmi. Táto smernica by sa mala vykonávať v súlade s uvedenými právami a zásadami.

(144) S európskym dozorným úradníkom pre ochranu údajov sa konzultovalo v súlade s článkom 42 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 ([25]) a európsky dozorný úradník pre ochranu údajov vydal stanovisko 11. marca 2021 ([26]),

([23]) 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).

([24]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách) (Ú. v. EÚ L 277, 27.10.2022, s. 1).

([25]) 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).

([26]) Ú. v. EÚ C 183, 11.5.2021, s. 3.

PRIJALI TÚTO SMERNICU:

KAPITOLA I

VŠEOBECNÉ USTANOVENIA

Článok 1

Predmet úpravy

1. Touto smernicou sa stanovujú opatrenia, ktorých zámerom je dosiahnuť vysokú spoločnú úroveň kybernetickej bezpečnosti v celej Únii na účely lepšieho fungovania vnútorného trhu.

2. Na uvedený účel sa v tejto smernici stanovujú:

a) povinnosti, ktorými sa od členských štátov vyžaduje, aby prijali národné stratégie kybernetickej bezpečnosti a určili alebo zriadili príslušné orgány, orgány pre riadenie kybernetických kríz, jednotné kontaktné miesta pre kybernetickú bezpečnosť (jednotné kontaktné miesta) a jednotky pre riešenie počítačových bezpečnostných incidentov (jednotky CSIRT);

b) opatrenia na riadenie kybernetických rizík a oznamovacie povinnosti pre subjekty typu uvedeného v prílohe I alebo II, ako aj pre subjekty identifikované ako kritické subjekty podľa smernice (EÚ) 2022/2557;

c) pravidlá a povinnosti výmeny informácií o kybernetickej bezpečnosti;

d) povinnosti členských štátov v oblasti dohľadu a presadzovania práva.

Článok 2

Rozsah pôsobnosti

1. Táto smernica sa vzťahuje na verejné alebo súkromné subjekty typu uvedeného v prílohe I alebo II, ktoré sa považujú za stredné podniky podľa článku 2 prílohy k odporúčaniu 2003/361/ES alebo presahujú limity pre stredné podniky stanovené v odseku 1 uvedeného článku a ktoré poskytujú služby alebo vykonávajú svoje činnosti v Únii.

Na účely tejto smernice sa článok 3 ods. 4 prílohy k uvedenému odporúčaniu neuplatňuje.

2. Táto smernica sa vzťahuje aj na subjekty typu uvedeného v prílohe I alebo II bez ohľadu na ich veľkosť, ak:

a) služby poskytujú:

   i) poskytovatelia verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb;

   ii) poskytovatelia dôveryhodných služieb;

   iii) registre názvov domén najvyššej úrovne a poskytovatelia služieb systému názvov domén;

b) subjekt je v členskom štáte jediným poskytovateľom služby, ktorá je kľúčovou pre zachovanie kritických spoločenských alebo hospodárskych činností;

c) narušenie služby poskytovanej subjektom by mohlo mať významný vplyv na verejný poriadok, verejnú bezpečnosť alebo verejné zdravie;

d) narušenie služby poskytovanej subjektom by mohlo vyvolať významné systémové riziko, najmä v odvetviach, v ktorých by takéto narušenie mohlo mať cezhraničný vplyv;

e) subjekt je vzhľadom na svoj osobitný význam na vnútroštátnej alebo regionálnej úrovni kritickým pre konkrétne odvetvie alebo typ služby alebo pre iné vzájomne závislé odvetvia v členskom štáte;

f) subjekt je subjektom verejnej správy:

i) v ústrednej štátnej správe podľa definície členského štátu v súlade s vnútroštátnym právom; alebo

ii) na regionálnej úrovni podľa definície členského štátu v súlade s vnútroštátnym právom, ktorý po posúdení na základe rizík poskytuje služby, ktorých narušenie by mohlo mať významný vplyv na kritické spoločenské alebo hospodárske činnosti.

3. Táto smernica sa vzťahuje na subjekty identifikované ako kritické subjekty podľa smernice (EÚ) 2022/2557 bez ohľadu na ich veľkosť.

4. Táto smernica sa vzťahuje na subjekty poskytujúce služby registrácie názvov domén bez ohľadu na ich veľkosť.

5. Členské štáty môžu ustanoviť, že sa táto smernica vzťahuje na:

a) subjekty verejnej správy na miestnej úrovni;

b) vzdelávacie inštitúcie, najmä tie, v ktorých sa vykonávajú kritické výskumné činnosti.

6. Touto smernicou nie je dotknutá zodpovednosť členských štátov za ochranu národnej bezpečnosti ani ich právomoc chrániť iné základné funkcie štátu vrátane zabezpečenia územnej celistvosti štátu a udržiavania verejného poriadku.

7. Táto smernica sa nevzťahuje na subjekty verejnej správy, ktoré vykonávajú činnosť v oblasti národnej bezpečnosti, verejnej bezpečnosti, obrany alebo presadzovania práva vrátane prevencie, vyšetrovania, odhaľovania a stíhania trestných činov.

8. Členské štáty môžu vyňať konkrétne subjekty, ktoré vykonávajú činnosti v oblastiach národnej bezpečnosti, verejnej bezpečnosti, obrany alebo presadzovania práva vrátane prevencie, vyšetrovania, odhaľovania a stíhania trestných činov, alebo ktoré poskytujú služby výhradne subjektom verejnej správy uvedeným v odseku 7 tohto článku, v súvislosti s danými činnosťami alebo službami z povinností stanovených v článku 21 alebo článku 23. V takýchto prípadoch sa opatrenia dohľadu a presadzovania uvedené v kapitole VII v súvislosti s týmito konkrétnymi činnosťami alebo službami neuplatňujú. Ak subjekty vykonávajú činnosti alebo poskytujú služby výlučne typu uvedeného v tomto odseku, členské štáty sa môžu tiež rozhodnúť vyňať tieto subjekty z povinností stanovených v článkoch 3 a 27.

9. Ak subjekt koná ako poskytovateľ dôveryhodných služieb, odseky 7 a 8 sa neuplatňujú.

10. Táto smernica sa nevzťahuje na subjekty, ktoré členské štáty vyňali z rozsahu pôsobnosti nariadenia (EÚ) 2022/2554 v súlade s článkom 2 ods. 4 uvedeného nariadenia.

11. K povinnostiam ustanoveným v tejto smernici nepatrí poskytovanie informácií, ktorých zverejnenie by bolo v rozpore so základnými záujmami členských štátov v oblasti národnej bezpečnosti, verejnej bezpečnosti alebo obrany.

12. Táto smernica sa uplatňuje bez toho, aby bolo dotknuté nariadenie (EÚ) 2016/679, smernica 2002/58/ES, smernice Európskeho parlamentu a Rady 2011/93/EÚ ([27]) a 2013/40/EÚ ([28]) a smernica (EÚ) 2022/2557.

13. Bez toho, aby bol dotknutý článok 346 ZFEÚ, informácie, ktoré sú podľa predpisov Únie alebo vnútroštátnych predpisov dôverné, ako napríklad predpisy o obchodnom tajomstve, sa vymieňajú s Komisiou a inými príslušnými orgánmi v súlade s touto smernicou len vtedy, ak je takáto výmena potrebná na účely uplatňovania tejto smernice. Vymieňané informácie sa obmedzia na také informácie, ktoré sú relevantné a primerané účelu danej výmeny. Pri výmene informácií sa zachováva ich dôvernosť a chránia sa bezpečnostné a komerčné záujmy dotknutých subjektov.

([27]) Smernica Európskeho parlamentu a Rady 2011/93/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa nahrádza rámcové rozhodnutie Rady 2004/68/SVV (Ú. v. EÚ L 335, 17.12.2011, s. 1).

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

14. Subjekty, príslušné orgány, jednotné kontaktné miesta a jednotky CSIRT spracúvajú osobné údaje v rozsahu potrebnom na účely tejto smernice a v súlade s nariadením (EÚ) 2016/679, pričom takéto spracovanie sa opiera najmä o jeho článok 6.

Spracovanie osobných údajov podľa tejto smernice poskytovateľmi verejných elektronických komunikačných sietí alebo poskytovateľmi verejne dostupných elektronických komunikačných služieb sa vykonáva v súlade s právom Únie v oblasti ochrany údajov a právom Únie v oblasti ochrany súkromia, najmä so smernicou 2002/58/ES.

Článok 3

Kľúčové a dôležité subjekty

1. Na účely tejto smernice sa za kľúčové subjekty považujú:

a) subjekty typu uvedeného v prílohe I, ktoré presahujú limity pre stredné podniky stanovené v článku 2 ods. 1 prílohy k odporúčaniu 2003/361/ES;

b) kvalifikovaní poskytovatelia dôveryhodných služieb a registre názvov domén najvyššej úrovne, ako aj poskytovatelia služieb DNS, bez ohľadu na ich veľkosť;

c) poskytovatelia verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb, ktoré sú považované za stredné podniky podľa článku 2 prílohy k odporúčaniu 2003/361/ES;

d) subjekty verejnej správy uvedené v článku 2 ods. 2 písm. f) bode i);

e) akékoľvek iné subjekty typu uvedeného v prílohe I alebo II, ktoré členský štát označil za kľúčové subjekty podľa článku 2 ods. 2 písm. b) až e);

f) subjekty označené ako kritické subjekty podľa smernice (EÚ) 2022/2557 uvedenej v článku 2 ods. 3 tejto smernice;

g) ak tak členský štát ustanoví, subjekty, ktoré daný členský štát označil pred 16. januárom 2023 ako prevádzkovateľov základných služieb v súlade so smernicou (EÚ) 2016/1148 alebo vnútroštátnym právom.

2. Na účely tejto smernice sa subjekty typu uvedeného v prílohe I alebo II, ktoré sa nepovažujú za kľúčové subjekty podľa odseku 1 tohto článku, považujú za dôležité subjekty. Patria sem subjekty označené členskými štátmi ako dôležité subjekty podľa článku 2 ods. 2 písm. b) až e).

3. Do 17. apríla 2025 vypracujú členské štáty zoznam kľúčových a dôležitých subjektov ako aj subjektov poskytujúcich služby registrácie názvov domén. Členské štáty tento zoznam pravidelne prehodnocujú a podľa potreby aktualizujú najmenej každé dva roky po uvedenom dátume.

4. Na účely zostavenia zoznamu uvedeného v odseku 3 členské štáty požadujú od subjektov uvedených v uvedenom odseku, aby príslušným orgánom predložili aspoň tieto informácie:

a) názov subjektu;

b) adresu a aktuálne kontaktné údaje vrátane e-mailových adries, IP adries a telefónnych čísel;

c) podľa potreby príslušné odvetvie a pododvetvie uvedené v prílohe I alebo II; a

d) prípadne zoznam členských štátov, v ktorých poskytujú služby patriace do pôsobnosti tejto smernice.

Subjekty uvedené v odseku 3 bezodkladne a v každom prípade do dvoch týždňov odo dňa zmeny oznámia akékoľvek zmeny údajov zasielaných podľa prvého pododseku tohto odseku.

Komisia s pomocou Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA) bez zbytočného odkladu poskytne usmernenia a vzory súvisiace s povinnosťami stanovenými v tomto odseku.

Členské štáty môžu zaviesť vnútroštátne mechanizmy, pomocou ktorých by sa subjekty mohli zaregistrovať samé.

5. Do 17. apríla 2025 a potom každé dva roky príslušné orgány nahlasujú:

a) Komisii a skupine pre spoluprácu počet kľúčových a dôležitých subjektov uvedených v odseku 3 za každé odvetvie a pododvetvie uvedené v prílohe I alebo II; a

b) Komisii relevantné informácie o počte kľúčových a dôležitých subjektov označených podľa článku 2 ods. 2 písm. b) až e), odvetvie a pododvetvie uvedené v prílohe I alebo II, do ktorých patria, druh nimi poskytovanej služby a ustanovenie spomedzi ustanovení uvedených v článku 2 ods. 2 písm. b) až e), podľa ktorého boli označené.

6. Do 17. apríla 2025 a na žiadosť Komisie môžu členské štáty Komisii nahlásiť názvy kľúčových a dôležitých subjektov uvedených v odseku 5 písm. b).

Článok 4

Odvetvové právne akty Únie

1. Ak sa v odvetvových právnych aktoch Únie vyžaduje, aby kľúčové alebo dôležité subjekty prijali opatrenia na riadenie kybernetických rizík alebo aby nahlasovali významné incidenty, a ak majú tieto požiadavky aspoň rovnocenný účinok ako povinnosti stanovené v tejto smernici, príslušné ustanovenia tejto smernice vrátane ustanovení o dohľade a presadzovaní práva v kapitole VII sa na takéto subjekty nevzťahujú. Ak sa odvetvové právne akty Únie nevzťahujú na všetky subjekty v konkrétnom odvetví v pôsobnosti tejto smernice, príslušné ustanovenia tejto smernice sa naďalej vzťahujú na subjekty, na ktoré sa odvetvové právne akty Únie nevzťahujú.

2. Požiadavky uvedené v odseku 1 tohto článku sa považujú za rovnocenné s povinnosťami stanovenými v tejto smernici, ak:

a) opatrenia na riadenie kybernetických rizík majú prinajmenšom rovnocenný účinok ako opatrenia stanovené v článku 21 ods. 1 a 2; alebo

b) odvetvový právny akt Únie poskytuje okamžitý prístup, podľa potreby automatický a priamy, k hláseniam o incidentoch od jednotiek CSIRT, príslušných orgánov alebo jednotných kontaktných miest podľa tejto smernice a ak požiadavky na nahlasovanie závažných incidentov majú prinajmenšom rovnocenný účinok ako požiadavky stanovené v článku 23 ods. 1 až 6 tejto smernice.

3. Komisia do 17. júla 2023 poskytne usmernenia na objasnenie uplatňovania odsekov 1 a 2. Komisia uvedené usmernenia pravidelne prehodnocuje. Pri príprave uvedených usmernení Komisia zohľadňuje všetky pripomienky skupiny pre spoluprácu a agentúry ENISA.

Článok 5

Minimálna harmonizácia

Táto smernica nebráni členským štátom, aby prijali alebo ponechali v platnosti ustanovenia na zaistenie vyššej úrovne kybernetickej bezpečnosti, ak nie sú takéto ustanovenia v rozpore s povinnosťami členských štátov stanovenými v práve Únie.

Článok 6

Vymedzenie pojmov

Na účely tejto smernice sa uplatňuje toto vymedzenie pojmov:

1. „sieť a informačný systém“ je:

   a) elektronická komunikačná sieť v zmysle vymedzenia v článku 2 bodu 1 smernice (EÚ) 2018/1972;

b) každé zariadenie alebo skupina vzájomne prepojených alebo súvisiacich zariadení, z ktorých jedno alebo viaceré vykonávajú automatické spracúvanie digitálnych údajov na základe programu; alebo

c) digitálne údaje, ktoré sa ukladajú, spracúvajú, získavajú alebo prenášajú prostredníctvom prvkov uvedených v písmenách a) a b) na účely ich prevádzkovania, používania, ochrany a udržiavania;

2. „bezpečnosť sietí a informačných systémov“ je schopnosť sietí a informačných systémov odolávať na určitom stupni spoľahlivosti akejkoľvek udalosti, ktorá môže ohroziť dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov;

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

4. „národná stratégia kybernetickej bezpečnosti “ je koherentný rámec členského štátu, v ktorom sa stanovujú strategické ciele a priority v oblasti kybernetickej bezpečnosti a systém správy na ich dosiahnutie v danom členskom štáte;

5. „udalosť odvrátená v poslednej chvíli“ je udalosť, ktorá by mohla ohroziť dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov, ale ktorej vzniku sa úspešne zabránilo alebo ku ktorej nedošlo;

6. „incident“ je udalosť ohrozujúca dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov;

7. „rozsiahly kybernetický incident“ je incident, ktorý spôsobí narušenie na úrovni presahujúcej schopnosť členského štátu naň reagovať alebo ktorý má významný vplyv aspoň na dva členské štáty;

8. „riešenie incidentov“ sú akékoľvek kroky a postupy zamerané na prevenciu, odhaľovanie, analýzu a obmedzovanie incidentov alebo na reakciu na incident a zotavenie z neho;

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

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

11. „významná kybernetická hrozba“ je kybernetická hrozba, o ktorej možno na základe jej technických charakteristík predpokladať, že má potenciál mať závažný vplyv na sieť a informačné systémy subjektu alebo používateľov služieb subjektu tým, že spôsobí značnú hmotnú alebo nehmotnú ujmu;

12. „produkt IKT“ je produkt IKT v zmysle vymedzenia v článku 2 bode 12 nariadenia (EÚ) 2019/881;

13. „služba IKT“ je služba IKT v zmysle vymedzenia v článku 2 bode 13 nariadenia (EÚ) 2019/881;

14. „proces IKT“ je proces v zmysle vymedzenia v článku 2 bode 14 nariadenia (EÚ) 2019/881;

15. „zraniteľnosť“ je slabá stránka, náchylnosť alebo chyba produktov IKT alebo služieb IKT, ktorá môže byť zneužitá kybernetickou hrozbou;

16. „norma“ je norma v zmysle vymedzenia v článku 2 bode 1 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1025/2012 ([29]);

17. „technická špecifikácia“ je technická špecifikácia v zmysle vymedzenia v článku 2 bode 4 nariadenia (EÚ) č. 1025/2012;

([29]) 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).

18. „internetový prepojovací uzol“ je sieťové zariadenie, ktoré umožňuje prepojenie viac než dvoch nezávislých autonómnych sietí (autonómnych systémov) najmä na účely sprostredkovania internetového dátového toku, ktorý prepojuje len autonómne systémy a ktorý nevyžaduje, aby internetový dátový tok medzi ktoroukoľvek dvojicou zúčastnených autonómnych systémov prechádzal cez ľubovoľný tretí autonómny systém, takýto dátový tok menil alebo doň nejako nezasahoval;

19. „systém názvov domén“ alebo „DNS“ je hierarchický distribuovaný systém názvov, ktorý umožňuje identifikáciu internetových služieb a zdrojov a to, aby zariadenia koncových používateľov používali služby smerovania internetu a pripojenia na účely prístupu k týmto službám a zdrojom;

20. „poskytovateľ služieb DNS“ je subjekt, ktorý poskytuje:

    a) verejne dostupné služby rekurzívneho rozlišovania názvov domén pre koncových používateľov internetu; alebo

    b) autoritatívne služby rozlišovania názvov domén pre použitie tretích strán s výnimkou koreňových názvových serverov;

21. „správca názvov domén najvyššej úrovne“ alebo „správca názvov TLD“ je subjekt, ktorému bola pridelená osobitná doména najvyššej úrovne (TLD) a ktorý je zodpovedný za správu TLD vrátane registrácie názvov domén v rámci TLD a za technickú prevádzku TLD vrátane prevádzky názvových serverov, údržby jeho databáz a distribúcie súborov zóny TLD v rámci názvových serverov bez ohľadu na to, či ktorúkoľvek z týchto operácií vykonáva subjekt sám alebo sa vykonáva externe, avšak s vylúčením situácií, kedy názvy TLD používa správca pre vlastnú potrebu;

22. „subjekt poskytujúci služby registrácie názvov domén“ je registrátor alebo zástupca konajúci v mene registrátorov, ako napríklad poskytovateľ alebo predajca služieb registrácie súkromia alebo proxy;

23. „digitálna služba“ je služba v zmysle vymedzenia v článku 1 ods. 1 písm. b) smernice Európskeho parlamentu a Rady (EÚ) 2015/1535 ([30]);

24. „dôveryhodná služba“ je dôveryhodná služba v zmysle vymedzenia v článku 3 bode 16 nariadenia (EÚ) č. 910/2014;

25. „poskytovateľ dôveryhodných služieb“ je poskytovateľ dôveryhodných služieb v zmysle vymedzenia v článku 3 bode 19 nariadenia (EÚ) č. 910/2014;

26. „kvalifikovaná dôveryhodná služba“ je kvalifikovaná dôveryhodná služba v zmysle vymedzenia v článku 3 bode 17 nariadenia (EÚ) č. 910/2014;

27. „poskytovateľ kvalifikovaných dôveryhodných služieb“ je poskytovateľ kvalifikovaných dôveryhodných služieb v zmysle vymedzenia v článku 3 bode 20 nariadenia (EÚ) č. 910/2014;

28. „online trhovisko“ je online trhovisko v zmysle vymedzenia v článku 2 písm. n) smernice Európskeho parlamentu a Rady 2005/29/ES ([31]);

29. „internetový vyhľadávač“ je internetový vyhľadávač v zmysle vymedzenia v článku 2 bodu 5 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/1150 ([32]);

30. „služba cloud computingu“ je digitálna služba, ktoré umožňuje správu na požiadanie a vzdialený širokopásmový prístup ku škálovateľnému a pružnému súboru zdieľateľných výpočtových zdrojov, a to aj ak sa tieto zdroje nachádzajú na viacerých miestach;

([30]) Smernica Európskeho parlamentu a Rady (EÚ) 2015/1535 z 9. septembra 2015, ktorou sa stanovuje postup pri poskytovaní informácií v oblasti technických predpisov a pravidiel vzťahujúcich sa na služby informačnej spoločnosti (Ú. v. EÚ L 241, 17.9.2015, s. 1).

([31]) Smernica Európskeho parlamentu a Rady 2005/29/ES z 11. mája 2005 o nekalých obchodných praktikách podnikateľov voči spotrebiteľom na vnútornom trhu, a ktorou sa mení a dopĺňa smernica Rady 84/450/EHS, smernice Európskeho parlamentu a Rady 97/7/ES, 98/27/ES a 2002/65/ES a nariadenie Európskeho parlamentu a Rady (ES) č. 2006/2004 („smernica o nekalých obchodných praktikách“) (Ú. v. EÚ L 149, 11.6.2005, s. 22).

([32]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/1150 z 20. júna 2019 o podpore spravodlivosti a transparentnosti pre komerčných používateľov online sprostredkovateľských služieb (Ú. v. EÚ L 186, 11.7.2019, s. 57).

31. „služba dátového centra“ je služba, ktorá zahŕňa štruktúry alebo skupiny štruktúr vyhradené na centralizované umiestnenie, vzájomné prepojenie a prevádzku IT a sieťového vybavenia poskytujúcich služby ukladania, spracovania a prepravy dát spolu so všetkými zariadeniami a infraštruktúrami na distribúciu elektrickej energie a environmentálnu kontrolu;

32. „sieť na sprístupňovanie obsahu“ je sieť geograficky distribuovaných serverov na zabezpečenie vysokej dostupnosti, prístupnosti alebo rýchleho doručenia digitálneho obsahu a služieb používateľom internetu v mene poskytovateľov obsahu a služieb;

33. „platforma služieb sociálnej siete“ je platforma, ktorá koncovým používateľom umožňuje vzájomné prepojenie, zdieľanie, objavovanie a komunikáciu prostredníctvom viacerých zariadení, najmä prostredníctvom chatov, príspevkov, videí a odporúčaní;

34. „zástupca“ je fyzická alebo právnická osoba usadená v Únii, ktorá je výslovne určená konať v mene poskytovateľa služieb DNS, správcu názvov TLD, subjektu poskytujúceho služby registrácie názvov domén, poskytovateľa služieb cloud computingu, poskytovateľa služieb dátových centier, poskytovateľa siete na sprístupňovanie obsahu, poskytovateľa riadených služieb, poskytovateľa riadených bezpečnostných služieb, alebo poskytovateľa online trhoviska, internetového vyhľadávača alebo platformy služieb sociálnych sietí, ktorí nie sú usadení v Únii, a na ktorú sa príslušný orgán alebo jednotka CSIRT môžu obracať namiesto subjektu v súvislosti s jeho povinnosťami podľa tejto smernice;

35. „subjekt verejnej správy“ je subjekt, ktorý je ako taký uznaný v členskom štáte v súlade s vnútroštátnym právom, okrem súdnictva, parlamentov a centrálnych bánk, a ktorý spĺňa tieto kritériá:

    a) je zriadený na účely plnenia potrieb všeobecného záujmu a nemá priemyselný ani komerčný charakter;

    b) má právnu subjektivitu alebo je zo zákona oprávnený konať v mene iného subjektu s právnou subjektivitou;

    c) je financovaný prevažne štátnymi, regionálnymi alebo inými verejnoprávnymi orgánmi, podlieha dohľadu týchto inštitúcií alebo orgánov nad svojím riadením alebo v správnom, riadiacom alebo dozornom orgáne má viac ako polovicu členov menovaných štátnymi alebo regionálnymi orgánmi alebo inými verejnoprávnymi inštitúciami;

    d) má právomoc vydávať fyzickým alebo právnickým osobám správne alebo regulačné rozhodnutia, ktoré majú vplyv na ich práva pri cezhraničnom pohybe osôb, tovarov, služieb alebo kapitálu;

36. „verejná elektronická komunikačná sieť“ je verejná elektronická komunikačná sieť v zmysle vymedzenia v článku 2 bode 8 smernice (EÚ) 2018/1972;

37. „elektronická komunikačná služba“ je elektronická komunikačná služba v zmysle vymedzenia v článku 2 bode 4 smernice (EÚ) 2018/1972;

38. „subjekt“ je fyzická alebo právnická osoba zriadená a uznaná ako taká podľa vnútroštátneho práva v mieste svojho sídla, ktorá môže vo vlastnom mene vykonávať práva a podliehať povinnostiam;

39. „poskytovateľ riadených služieb“ je subjekt, ktorý poskytuje služby súvisiace s inštaláciou, správou, prevádzkou alebo údržbou produktov IKT, sietí, infraštruktúry, aplikácií alebo akýchkoľvek iných sietí a informačných systémov formou pomoci alebo aktívnej správy vykonávanej buď v priestoroch zákazníka alebo na diaľku;

40. „poskytovateľ riadených bezpečnostných služieb“ je poskytovateľ riadených služieb, ktorý vykonáva alebo poskytuje pomoc pre činnosti súvisiace s riadením kybernetických rizík;

41. „výskumná organizácia“ je subjekt, ktorého hlavným cieľom je vykonávať aplikovaný výskum alebo experimentálny vývoj s cieľom využiť výsledky tohto výskumu na komerčné účely, ktorého súčasťou však nie sú vzdelávacie inštitúcie.

KAPITOLA II

KOORDINOVANÉ RÁMCE KYBERNETICKEJ BEZPEČNOSTI

Článok 7

Národná stratégia kybernetickej bezpečnosti

1. Každý členský štát prijme národnú stratégiu kybernetickej bezpečnosti, v ktorej stanoví strategické ciele, zdroje potrebné na dosiahnutie týchto cieľov a vhodné politické a regulačné opatrenia na dosiahnutie a zachovanie vysokej úrovne kybernetickej bezpečnosti. Národná stratégia kybernetickej bezpečnosti sietí obsahuje:

a) ciele a priority stratégie kybernetickej bezpečnosti členského štátu najmä pre odvetvia uvedené v prílohách I a II;

b) rámec riadenia na dosiahnutie cieľov a priorít uvedených v písmene a) tohto odseku vrátane politík uvedených v odseku 2;

c) rámec riadenia na objasnenie úloh a povinností relevantných zainteresovaných strán na vnútroštátnej úrovni, ktorý je základom spolupráce a koordinácie na vnútroštátnej úrovni medzi príslušnými orgánmi, jednotnými kontaktnými miestami a jednotkami CSIRT podľa tejto smernice, ako aj koordináciu a spoluprácu medzi uvedenými orgánmi a príslušnými orgánmi podľa odvetvových právnych aktov Únie;

d) mechanizmus na identifikáciu relevantných prostriedkov a hodnotenie rizík v danom členskom štáte;

e) identifikáciu opatrení na zabezpečenie pripravenosti a schopnosti reakcie na incidenty a zotavenia z nich vrátane spolupráce medzi verejným a súkromným sektorom;

f) zoznam rôznych orgánov a zainteresovaných strán zapojených do vykonávania národnej stratégie kybernetickej bezpečnosti;

g) politický rámec pre posilnenú koordináciu medzi príslušnými orgánmi podľa tejto smernice a príslušnými orgánmi podľa smernice (EÚ) 2022/2557 za účelom výmeny informácií o rizikách, kybernetických hrozbách a incidentoch, ako aj o nekybernetických rizikách, hrozbách a incidentoch, prípadne pri plnení úloh dohľadu;

h) plán vrátane potrebných opatrení na zvýšenie všeobecnej úrovne informovanosti občanov o kybernetickej bezpečnosti.

2. Členské štáty v rámci národnej stratégie kybernetickej bezpečnosti prijmú najmä politiky:

a) so zameraním na kybernetickú bezpečnosť v dodávateľskom reťazci produktov IKT a služieb IKT, ktoré subjekty používajú na poskytovanie svojich služieb;

b) týkajúce sa zahrnutia a špecifikácie požiadaviek na kybernetickú bezpečnosť produktov IKT a služieb IKT vo verejnom obstarávaní, a to aj pokiaľ ide o certifikáciu kybernetickej bezpečnosti, šifrovanie a využívanie produktov kybernetickej bezpečnosti s otvoreným zdrojovým kódom;

c) riadenia zraniteľností vrátane podpory a sprostredkovania koordinovaného zverejňovania zraniteľností podľa článku 12 ods. 1;

d) v súvislosti s udržiavaním všeobecnej dostupnosti, integrity a dôvernosti verejného jadra otvoreného internetu, v relevantnom prípade vrátane kybernetickej bezpečnosti podmorských komunikačných káblov;

e) na podporu vývoja a integrácie relevantných pokročilých technológií so zámerom implementovať najmodernejšie opatrenia na riadenie rizík kybernetickej bezpečnosti;

f) na podporu a rozvoj vzdelávania a odbornej prípravy v oblasti kybernetickej bezpečnosti, kvalifikácií v oblasti kybernetickej bezpečnosti, zvyšovania informovanosti a výskumných a vývojových iniciatív v oblasti kybernetickej bezpečnosti, ako aj usmernenia o správnych postupoch a kontrolách kybernetickej hygieny, zamerané na občanov, zainteresované strany a subjekty;

g) na podporu akademických a výskumných inštitúcií pri vývoji, zlepšovaní a zavádzaní nástrojov kybernetickej bezpečnosti a bezpečnej sieťovej infraštruktúry;

h) vrátane príslušných postupov a vhodných nástrojov zdieľania informácií na podporu dobrovoľného zdieľania informácií o kybernetickej bezpečnosti medzi subjektmi v súlade s právom Únie;

i) na posilnenie kybernetickej odolnosti a základnej kybernetickej hygieny malých a stredných podnikov, najmä podnikov vyňatých z pôsobnosti tejto smernice, poskytovaním ľahko dostupných usmernení a pomoci pre ich špecifické potreby;

j) na podporu aktívnej kybernetickej ochrany.

3. Členské štáty oznámia Komisii svoje národné stratégie kybernetickej bezpečnosti do troch mesiacov od ich prijatia. Členské štáty môžu z takýchto oznámení vylúčiť informácie, ktoré sa týkajú ich národnej bezpečnosti.

4. Členské štáty pravidelne a aspoň každých päť rokov hodnotia svoje národné stratégie kybernetickej bezpečnosti na základe kľúčových ukazovateľov výkonnosti a v prípade potreby ich aktualizujú. Agentúra ENISA pomáha členským štátom na ich žiadosť pri vývoji alebo aktualizácii národnej stratégie kybernetickej bezpečnosti a kľúčových ukazovateľov výkonnosti na posúdenie tejto stratégie s cieľom zosúladiť ju s požiadavkami a povinnosťami stanovenými v tejto smernici.

Článok 8

Príslušné orgány a miesta jednotného kontaktu

1. Každý členský štát určí jeden alebo zriadi jeden alebo viacero príslušných orgánov zodpovedných za kybernetickú bezpečnosť a za úlohy dohľadu uvedené v kapitole VII (príslušné orgány).

2. Príslušné orgány uvedené v odseku 1 monitorujú implementáciu tejto smernice na vnútroštátnej úrovni.

3. Každý členský štát určí alebo zriadi miesto jednotného kontaktu. Ak členský štát určí alebo zriadi iba jeden príslušný orgán podľa odseku 1, uvedený príslušný orgán je aj jednotným kontaktným miestom v danom členskom štáte.

4. Každé jednotné kontaktné miesto vykonáva styčnú funkciu s cieľom zabezpečiť cezhraničnú spoluprácu orgánov daného členského štátu s príslušnými orgánmi iných členských štátov a v prípade potreby s Komisiou a agentúrou ENISA, ako aj s cieľom zabezpečiť medziodvetvovú spoluprácu s inými príslušnými orgánmi v rámci daného členského štátu.

5. Členské štáty zabezpečia, aby ich príslušné orgány a jednotné kontaktné miesta mali primerané zdroje na účinné a efektívne vykonávanie zverených úloh, a teda na plnenie cieľov tejto smernice.

6. Každý členský štát bez zbytočného odkladu informuje Komisiu o identite príslušného orgánu uvedeného v odseku 1 a jednotného kontaktného miesta uvedeného v odseku 3, o úlohách uvedených orgánov a o všetkých ich následných zmenách. Každý členský štát totožnosť svojho príslušného orgánu zverejní. Komisia zostaví verejne dostupný zoznam jednotných kontaktných miest.

Článok 9

Národné rámce pre riadenie kybernetických kríz

1. Každý členský štát určí alebo zriadi jeden alebo viac príslušných orgánov zodpovedných za riadenie rozsiahlych kybernetických incidentov a kríz (orgány pre riadenie kybernetických kríz). Členské štáty zabezpečujú, aby uvedené orgány mali primerané zdroje na účinný a efektívny výkon zverených úloh. Súlad s platnými rámcami pre všeobecné vnútroštátne krízové riadenie zabezpečujú členské štáty.

2. Ak členský štát určí alebo zriadi viac ako jeden orgán pre riadenie kybernetických kríz podľa odseku 1, jasne uvedie, ktorý z týchto príslušných orgánov má slúžiť ako koordinátor riadenia rozsiahlych kybernetických incidentov a kríz.

3. Každý členský štát určí spôsobilosti, aktíva a postupy, ktoré možno použiť na účely tejto smernice v prípade krízy.

4. Každý členský štát prijme národný plán reakcie na rozsiahle kybernetické incidenty a krízy, v ktorom sa stanovia ciele a spôsoby riadenia rozsiahlych kybernetických incidentov a kríz. V uvedenom pláne sa stanovia najmä:

a) ciele vnútroštátnych opatrení a činností v oblasti pripravenosti;

b) úlohy a povinnosti orgánov pre riadenie kybernetických kríz;

c) postupy riadenia kybernetických kríz vrátane ich začlenenia do všeobecného vnútroštátneho rámca krízového riadenia a kanálov na výmenu informácií;

d) vnútroštátne opatrenia v oblasti pripravenosti vrátane cvičení a činností odbornej prípravy;

e) príslušné verejné a súkromné zainteresované strany a potrebná infraštruktúra;

f) vnútroštátne postupy a dojednania medzi príslušnými vnútroštátnymi orgánmi a inštitúciami s cieľom zabezpečiť účinnú účasť členského štátu na koordinovanom riadení rozsiahlych kybernetických incidentov a kríz na úrovni Únie, ako aj jeho podporu tohto riadenia.

5. Do troch mesiacov od určenia alebo zriadenia orgánu pre riadenie kybernetických kríz uvedeného v odseku 1 informuje každý členský štát Komisiu o totožnosti svojho orgánu a o všetkých jeho následných zmenách. Členské štáty zasielajú Komisii a Európskej sieti kontaktných organizácií pre kybernetickú krízu (EU-CyCLONe) relevantné informácie v súvislosti s požiadavkami odseku 4 o svojich vnútroštátnych plánoch reakcie na rozsiahle kybernetické incidenty a krízy do troch mesiacov od prijatia uvedených plánov. Členské štáty môžu vylúčiť informácie v prípade a v rozsahu, v akom je takéto vylúčenie potrebné pre ich národnú bezpečnosť.

Článok 10

Jednotky pre riešenie počítačových bezpečnostných incidentov (jednotky CSIRT)

1. Každý členský štát určí alebo zriadi jednu alebo viacero jednotiek CSIRT. Jednotky CSIRT možno určiť alebo zriadiť v rámci príslušného orgánu. Jednotky CSIRT sú povinné spĺňať požiadavky stanovené v článku 11 ods. 1, pokrývať aspoň odvetvia, pododvetvia alebo druhy subjektov uvedených v prílohách I a II a zodpovedajú za riešenie incidentov podľa presne stanoveného postupu.

2. Členské štáty zabezpečia, aby každá jednotka CSIRT mala primerané zdroje na účinné plnenie svojich úloh stanovených v článku 11 ods. 3.

3. Členské štáty zabezpečia, aby každá jednotka CSIRT mala k dispozícii vhodnú, bezpečnú a odolnú komunikačnú a informačnú infraštruktúru na výmenu informácií s kľúčovými a dôležitými subjektmi a ďalšími relevantnými zainteresovanými stranami. Členské štáty na uvedený účel zabezpečia, aby každá jednotka CSIRT prispievala k zavádzaniu bezpečných nástrojov na výmenu informácií.

4. Jednotky CSIRT spolupracujú a v prípade potreby si vymieňajú relevantné informácie v súlade s článkom 29 s odvetvovými alebo medziodvetvovými komunitami kľúčových a dôležitých subjektov.

5. Jednotky CSIRT sa zúčastňujú na partnerských preskúmaniach organizovaných podľa článku 19.

6. Členské štáty zabezpečia účinnú, efektívnu a bezpečnú spoluprácu svojich jednotiek CSIRT v sieti jednotiek CSIRT.

7. Jednotky CSIRT môžu nadväzovať spoluprácu s národnými jednotkami reakcie na počítačové bezpečnostné incidenty tretích krajín. Ako súčasť takýchto vzťahov spolupráce členské štáty sprostredkujú účinnú, efektívnu a bezpečnú výmenu informácií s uvedenými národnými jednotkami reakcie na počítačové bezpečnostné incidenty z tretích krajín, pričom použijú relevantné protokoly na výmenu informácií vrátane semaforového protokolu. Jednotky CSIRT si môžu vymieňať relevantné informácie s národnými jednotkami reakcie na počítačové bezpečnostné incidenty tretích krajín vrátane osobných údajov v súlade s právom Únie v oblasti ochrany údajov.

8. Jednotky CSIRT môžu spolupracovať s národnými jednotkami reakcie na počítačové bezpečnostné incidenty tretích krajín alebo rovnocennými orgánmi tretích krajín najmä na účely poskytovania pomoci v oblasti kybernetickej bezpečnosti.

9. Každý členský štát bez zbytočného odkladu informuje Komisiu o identite jednotky CSIRT uvedenej v odseku 1 tohto článku a jednotky CSIRT určenej za koordinátora podľa článku 12 ods. 1, o úlohách uvedených orgánov v súvislosti s kľúčovými a dôležitými subjektmi a o všetkých následných zmenách.

10. Členské štáty môžu pri zriaďovaní svojich jednotiek CSIRT požiadať o pomoc agentúru ENISA.

Článok 11

Požiadavky na jednotky CSIRT a ich technické spôsobilosti a úlohy

1. Jednotky CSIRT sú povinné spĺňať tieto požiadavky:

a) zabezpečovať vysokú úroveň dostupnosti svojich komunikačných kanálov prevenciou jediných bodov zlyhania a mať k dispozícii niekoľko spôsobov, ktorými ich možno kedykoľvek kontaktovať a ktorými môžu tieto jednotky kontaktovať iných; jasne špecifikovať komunikačné kanály a oboznámiť s nimi zainteresované strany a spolupracujúcich partnerov;

b) mať svoje pracoviská a podporné informačné systémy umiestnené na zabezpečených miestach;

c) byť vybavené vhodným systémom riadenia a smerovania žiadostí, najmä na sprostredkovanie ich účinného a efektívneho odovzdávania;

d) zabezpečovať dôvernosť a dôveryhodnosť svojich operácií;

e) byť primerane personálne vybavené na zabezpečenie stálej dostupnosti svojich služieb a zabezpečovať patričnú odbornú prípravu pre svojich zamestnancov;

f) byť vybavené redundantnými systémami a záložným pracovným priestorom na zabezpečenie kontinuity svojich služieb.

Jednotky CSIRT môžu byť zapojené do sietí medzinárodnej spolupráce.

2. Členské štáty zabezpečia, aby ich jednotky CSIRT spoločne mali technické spôsobilosti potrebné na výkon úloh uvedených v odseku 3. Aby jednotky CSIRT mohli rozvíjať svoje technické spôsobilosti, členské štáty zabezpečia prídel dostatočných zdrojov pre svoje jednotky CSIRT na zaistenie primeraného počtu zamestnancov.

3. Jednotky CSIRT plnia tieto úlohy:

a) monitorujú a analyzujú kybernetické hrozby, zraniteľnosti a incidenty na vnútroštátnej úrovni a na požiadanie poskytujú pomoc dotknutým kľúčovým a dôležitým subjektom s ohľadom na monitorovanie ich sietí a informačných systémov v reálnom alebo takmer v reálnom čase;

b) zasielajú včasné varovania, výstrahy a oznámenia a šíria informácie o kybernetických hrozbách, zraniteľnostiach a incidentoch dotknutým kľúčovým a dôležitým subjektom, ako aj príslušným orgánom a ďalším relevantným zainteresovaným stranám pokiaľ možno takmer v reálnom čase;

c) podľa potreby reagujú na incidenty a poskytujú pomoc dotknutým kľúčovým a dôležitým subjektom;

d) zhromažďujú a analyzujú forenzné údaje a poskytujú dynamickú analýzu rizík a incidentov a informácie o situácii v kybernetickej bezpečnosti;

e) na žiadosť kľúčového alebo dôležitého subjektu umožňujú aktívne skenovanie siete a informačných systémov dotknutého subjektu s cieľom odhaľovať zraniteľnosti s potenciálnym významným dosahom;

f) účasť v sieti jednotiek CSIRT a poskytovanie vzájomnej pomoci podľa svojich kapacít a kompetencií ostatným členom siete jednotiek CSIRT na ich žiadosť;

g) v prípade potreby pôsobia ako koordinátor na účely koordinovaného zverejňovania zraniteľností podľa článku 12 ods. 1;

h) prispievajú k zavádzaniu bezpečných nástrojov na výmenu informácií podľa článku 10 ods. 3.

Jednotky CSIRT môžu vykonávať aktívne nerušivé skenovanie verejne prístupných sietí a informačných systémov kľúčových a dôležitých subjektov. Takéto skenovanie sa vykonáva s cieľom odhaliť zraniteľné alebo nezabezpečene nakonfigurované siete a informačné systémy a informovať dotknuté subjekty. Takéto skenovanie nesmie mať negatívny vplyv na fungovanie služieb subjektov.

Pri výkone úloh uvedených v prvom pododseku môžu jednotky CSIRT uprednostňovať konkrétne úlohy na základe prístupu založeného na rizikách.

4. Jednotky CSIRT nadviažu spoluprácu s príslušnými zainteresovanými stranami v súkromnom sektore s cieľom dosiahnuť ciele tejto smernice.

5. Jednotky CSIRT v záujme sprostredkovania spolupráce uvedenej v odseku 4 podporujú prijímanie a využívanie spoločných alebo normalizovaných postupov, režimov utajenia a taxonómie v súvislosti s:

a) postupmi riešenia incidentov;

b) krízovým riadením; a

c) koordinovaným zverejňovaním zraniteľností podľa článku 12 ods. 1.

Článok 12

Koordinované zverejňovanie zraniteľností a európska databáza zraniteľností

1. Na účely koordinovaného zverejňovania zraniteľností určí každý členský štát jednu zo svojich jednotiek CSIRT za koordinátora. Jednotka CSIRT určená za koordinátora koná ako dôveryhodný sprostredkovateľ, ktorý v prípade potreby sprostredkuje interakciu medzi fyzickou alebo právnickou osobou, ktorá na žiadosť niektorej zo strán oznamuje zraniteľnosť a výrobcom alebo poskytovateľom potenciálne zraniteľných produktov IKT alebo služieb IKT. K úlohám jednotky CSIRT určenej za koordinátora patrí:

a) identifikácia a kontaktovanie dotknutých subjektov;

b) pomoc fyzickým alebo právnickým osobám oznamujúcim zraniteľnosti a

c) vyjednávanie harmonogramu zverejňovania a riadenie zraniteľností, ktoré majú dosah na viaceré subjekty.

Členské štáty zabezpečia, aby fyzické alebo právnické osoby mohli na požiadanie nahlásiť zraniteľnosť jednotke CSIRT určenej za koordinátora anonymne. Jednotka CSIRT určená za koordinátora zabezpečí v súvislosti s oznámenou zraniteľnosťou vykonanie dôsledných následných opatrení a zabezpečí anonymitu fyzickej alebo právnickej osoby, ktorá túto zraniteľnosť oznámila. Ak by oznámená zraniteľnosť mohla by mať významný vplyv na subjekty vo viac ako jednom členskom štáte, jednotka CSIRT každého dotknutého členského štátu určená za koordinátora v prípade potreby spolupracuje s inými jednotkami CSIRT určenými za koordinátorov v rámci siete jednotiek CSIRT.

2. Po porade so skupinou pre spoluprácu agentúra ENISA vytvorí a vedie európsku databázu zraniteľností. Na uvedený účel agentúra ENISA zriaďuje a udržiava vhodné informačné systémy, politiky a postupy a prijíma nevyhnutné technické a organizačné opatrenia na zaistenie bezpečnosti a integrity európskej databázy zraniteľností, aby subjektom, bez ohľadu na to či patria do rozsahu pôsobnosti tejto smernice, a ich dodávateľom sietí a informačných systémov umožnila najmä dobrovoľne zverejňovať a do registra zaraďovať verejne známe zraniteľnosti produktov IKT alebo služieb IKT. Prístup k informáciám o zraniteľnostiach v európskej databáze zraniteľností sa poskytuje všetkým zainteresovaným stranám. Uvedená databáza obsahuje:

a) informácie s opisom zraniteľností;

b) zasiahnuté produkty IKT alebo služby IKT a závažnosť zraniteľnosti z hľadiska okolností, za ktorých ju možno zneužiť;

c) dostupnosť súvisiacich záplat a v prípade absencie dostupných záplat usmernenia poskytnuté príslušnými orgánmi alebo jednotkami CSIRT určené používateľom zraniteľných produktov IKT a služieb IKT o tom, ako možno zmierniť riziká vyplývajúce zo zverejnených zraniteľností.

Článok 13

Spolupráca na vnútroštátnej úrovni

1. Ak sú príslušné orgány, jednotné kontaktné miesto a jednotky CSIRT jedného členského štátu samostatnými subjektmi, pri plnení povinností stanovených v tejto smernici navzájom spolupracujú.

2. Členské štáty zabezpečia, aby ich jednotky CSIRT, prípadne ich príslušné orgány dostávali oznámenia o významných incidentoch podľa článku 23 a o incidentoch, kybernetických hrozbách a udalostiach odvrátených v poslednej chvíli podľa článku 30.

3. Členské štáty zabezpečia, aby ich jednotky CSIRT, prípadne príslušné orgány poskytovali ich jednotným kontaktným miestam hlásenia o incidentoch, kybernetických hrozbách a udalostiach odvrátených v poslednej chvíli zasielané podľa tejto smernice.

4. S cieľom zabezpečiť, aby sa úlohy a povinnosti príslušných orgánov, jednotných kontaktných miest a jednotiek CSIRT vykonávali efektívne, členské štáty v rámci možností zabezpečia primeranú spoluprácu medzi uvedenými orgánmi a orgánmi presadzovania práva, orgánmi na ochranu údajov, vnútroštátnymi orgánmi podľa nariadení (ES) č. 300/2008 a (EÚ) 2018/1139, dozornými orgánmi podľa nariadenia (EÚ) č. 910/2014, príslušnými orgánmi podľa nariadenia (EÚ) 2022/2554, národnými regulačnými orgánmi podľa smernice (EÚ) 2018/1972, príslušnými orgánmi podľa smernice (EÚ) 2022/2557, ako aj príslušnými orgánmi podľa iných odvetvových právnych aktov Únie v danom členskom štáte.

5. Členské štáty zabezpečia, aby ich príslušné orgány podľa tejto smernice a ich príslušné orgány podľa smernice (EÚ) 2022/2557 pravidelne spolupracovali a vymieňali si informácie, pokiaľ ide o identifikáciu kritických subjektov, o rizikách, kybernetických hrozbách a incidentoch, ako aj o nekybernetických rizikách, hrozbách a incidentoch s dosahom na kľúčové subjekty označené ako kritické podľa smernice (EÚ) 2022/2557 a o opatreniach prijatých v reakcii na takéto riziká, hrozby a incidenty. Členské štáty tiež zabezpečia, aby si ich príslušné orgány podľa tejto smernice a ich príslušné orgány podľa nariadenia (EÚ) č. 910/2014, nariadenia (EÚ) 2022/2554 a smernice (EÚ) 2018/1972 pravidelne vymieňali relevantné informácie, a to aj o relevantných incidentoch a kybernetických hrozbách.

6. Pre oznamovanie uvedené v článkoch 23 a 30 zjednodušia členské štáty oznamovanie technickými prostriedkami.

KAPITOLA III

SPOLUPRÁCA NA ÚROVNI ÚNIE A NA MEDZINÁRODNEJ ÚROVNI

Článok 14

Skupina pre spoluprácu

1. S cieľom podporiť a sprostredkovať strategickú spoluprácu a výmenu informácií medzi členskými štátmi, ako aj posilniť vzájomnú dôveru, sa zriaďuje skupina pre spoluprácu.

2. Skupina pre spoluprácu vykonáva svoje úlohy na základe dvojročných pracovných programov uvedených v odseku 7.

3. Skupinu pre spoluprácu tvoria zástupcovia členských štátov, Komisie a agentúry ENISA. Na činnostiach skupiny pre spoluprácu sa ako pozorovateľ zúčastňuje Európska služba pre vonkajšiu činnosť. Európske orgány dohľadu (ESA) a príslušné orgány podľa nariadenia (EÚ) 2022/2554 sa môžu zúčastňovať na činnostiach skupiny pre spoluprácu v súlade s článkom 47 ods. 1 uvedeného nariadenia.

Podľa potreby môže skupina pre spoluprácu prizvať k práci Európsky parlament a zástupcov príslušných zainteresovaných strán.

Sekretariát zabezpečuje Komisia.

4. Skupina pre spoluprácu plní tieto úlohy:

a) poskytuje usmernenia príslušným orgánom v súvislosti s transpozíciou a vykonávaním tejto smernice;

b) poskytuje usmernenia príslušným orgánom v súvislosti s prípravou a implementáciou politík koordinovaného zverejňovania zraniteľností, ako sa uvádza v článku 7 ods. 2 písm. c);

c) vymieňa si najlepšie postupy a informácie v súvislosti s implementáciou tejto smernice, a to aj o kybernetických hrozbách, incidentoch, zraniteľnostiach, udalostiach odvrátených v poslednej chvíli, iniciatívy na zvyšovanie informovanosti, odbornú prípravu, cvičenia a kvalifikácie, budovanie kapacít, normy a technické špecifikácie, ako aj identifikáciu kľúčových a dôležitých subjektov podľa článku 2 ods. 2 písm. b) až e);

d) vymieňa si rady a spolupracuje s Komisiou v súvislosti s novými politickými iniciatívami pre kybernetickú bezpečnosť a celkovou konzistentnosťou odvetvových požiadaviek na kybernetickú bezpečnosť;

e) vymieňa si rady a spolupracuje s Komisiou v súvislosti s návrhom delegovaných alebo vykonávacích aktov prijímaných podľa tejto smernice;

f) vymieňa si najlepšie postupy a informácie s relevantnými inštitúciami, orgánmi, úradmi a agentúrami Únie;

g) vymieňa si názory na implementáciu odvetvových právnych aktov Únie, ktoré obsahujú ustanovenia o kybernetickej bezpečnosti;

h) v prípade potreby rokuje o správach o partnerskom hodnotení uvedenom v článku 19 ods. 9 a pripravuje závery a odporúčania;

i) vykonáva koordinované hodnotenia bezpečnostných rizík kritických dodávateľských reťazcov v súlade s článkom 22 ods. 1;

j) rokuje o prípadoch vzájomnej pomoci vrátane skúseností a výsledkov z cezhraničných spoločných opatrení dohľadu uvedených v článku 37;

k) na žiadosť jedného alebo viacerých dotknutých členských štátov rokuje o konkrétnych žiadostiach o vzájomnú pomoc podľa článku 37;

l) poskytuje strategické usmernenia pre sieť jednotiek CSIRT a EU-CyCLONe v otázkach konkrétnych vznikajúcich problémov;

m) vymieňa si názory na politiku nadväzných opatrení po rozsiahlych kybernetických incidentoch a krízach na základe skúseností siete jednotiek CSIRT a EU-CyCLONe;

n) prispieva k spôsobilostiam kybernetickej bezpečnosti v celej Únii sprostredkovaním výmen vnútroštátnych úradníkov prostredníctvom programu budovania kapacít, do ktorého sú zapojení zamestnanci príslušných orgánov alebo jednotiek CSIRT;

o) organizuje pravidelné spoločné stretnutia s príslušnými súkromnými zainteresovanými stranami z celej Únie s cieľom rokovať o činnostiach skupiny a zhromažďovať informácie o nových politických výzvach;

p) rokuje o práci vykonanej v súvislosti s cvičeniami kybernetickej bezpečnosti, ako aj o práci agentúry ENISA;

q) stanovuje metodiku a organizačné aspekty partnerských preskúmaní uvedených v článku 19 ods. 1, ako aj stanovuje metodiku sebahodnotenia pre členské štáty v súlade s článkom 19 ods. 5 za pomoci Komisie a agentúry ENISA a v spolupráci s Komisiou a agentúrou ENISA vypracovať kódexy správania, ktoré budú základom pracovných metód určených expertov na kybernetickú bezpečnosť v súlade s článkom 19 ods. 6;

r) vyhotovuje správy o skúsenostiach získaných na strategickej úrovni a z partnerských preskúmaní na účely preskúmania uvedeného v článku 40;

s) pravidelne vedie diskusiu o súčasnom stave kybernetických hrozieb alebo incidentov, ako je ransomvér, a vykonávať jeho hodnotenie.

Skupina pre spoluprácu predkladá správy uvedené v prvom pododseku písm. r) Komisii, Európskemu parlamentu a Rade.

5. Členské štáty zabezpečia účinnú, efektívnu a bezpečnú spoluprácu svojich zástupcov v rámci skupiny pre spoluprácu.

6. Skupina pre spoluprácu môže od siete jednotiek CSIRT požadovať technickú správu na vybrané témy.

7. Skupina pre spoluprácu do 1. februára 2024 a potom každé dva roky zostaví pracovný program týkajúci sa činností, ktoré sa majú uskutočniť v rámci dosahovania jej cieľov a úloh.

8. Komisia môže prijať vykonávacie akty stanovujúce procesné opatrenia potrebné na fungovanie skupiny pre spoluprácu.

Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2.

Pokiaľ ide o návrhy vykonávacích aktov uvedených v prvom pododseku tohto odseku, Komisia sa radí a spolupracuje so skupinou pre spoluprácu v súlade s odsekom 4 písm. e).

9. Skupina pre spoluprácu sa pravidelne a v každom prípade aspoň raz ročne stretáva so skupinou pre odolnosť kritických subjektov zriadenou podľa smernice (EÚ) 2022/2557 s cieľom podporovať a sprostredkovať strategickú spoluprácu a výmenu informácií.

Článok 15

Sieť jednotiek CSIRT

1. S cieľom prispieť k zvyšovaniu dôvery a podporiť rýchlu a účinnú operačnú spoluprácu medzi členskými štátmi sa zriaďuje sieť národných jednotiek CSIRT.

2. Sieť jednotiek CSIRT sa skladá zo zástupcov jednotiek CSIRT určených alebo zriadených podľa článku 10 a tímu reakcie na núdzové počítačové situácie v inštitúciách, orgánoch a agentúrach Únie (CERT-EU). Komisia sa zúčastňuje na práci siete jednotiek CSIRT ako pozorovateľ. Agentúra ENISA zabezpečuje sekretariát a aktívne pomáha so spoluprácou medzi jednotkami CSIRT.

3. Sieť jednotiek CSIRT plní tieto úlohy:

a) výmena informácií o spôsobilostiach jednotiek CSIRT;

b) sprostredkovanie spoločného používania, transferu a výmeny technológií a príslušných opatrení, politík, nástrojov, procesov, najlepších postupov a rámcov medzi jednotkami CSIRT;

c) výmena relevantných informácií o incidentoch, udalostiach odvrátených v poslednej chvíli, kybernetických hrozbách, rizikách a zraniteľnostiach;

d) výmena informácií v súvislosti s publikáciami a odporúčaniami o kybernetickej bezpečnosti;

e) zabezpečovanie interoperability, pokiaľ ide o špecifikácie a protokoly výmeny informácií;

f) na žiadosť člena siete jednotiek CSIRT potenciálne zasiahnutej incidentom výmena a prediskutovanie informácií o danom incidente a súvisiacich kybernetických hrozbách, rizikách a zraniteľnostiach;

g) na žiadosť člena siete jednotiek CSIRT prediskutovanie a v rámci možností vykonanie koordinovanej reakcie na incident, ktorý bol identifikovaný v oblasti patriacej do právomoci daného členského štátu;

h) poskytovanie pomoci členským štátom pri riešení cezhraničných incidentov podľa tejto smernice;

i) spolupráca, výmena najlepších postupov a poskytovanie pomoci jednotkám CSIRT určeným za koordinátorov podľa článku 12 ods. 1, pokiaľ ide o riadenie koordinovaného zverejňovania informácií o zraniteľnostiach, ktoré by mohli mať významný dosah na subjekty vo viac ako jednom členskom štáte;

j) prediskutovanie a určovanie ďalších foriem operačnej spolupráce, a to aj v súvislosti:

   i) s kategóriami kybernetických hrozieb a incidentov;

   ii) so včasnými varovaniami;

   iii) so vzájomnou pomocou;

   iv) so zásadami a dojednaniami koordinácie pri reakcii na cezhraničné riziká a incidenty;

   v) na žiadosť členského štátu s príspevkom k národnému plánu reakcie na rozsiahle kybernetické incidenty a krízy uvedeného v článku 9 ods. 4;

k) informovanie skupiny pre spoluprácu o svojej činnosti a o ďalších formách operačnej spolupráce prediskutovaných podľa písmena j) a v prípade potreby požadovanie usmernení v tomto ohľade;

l) bilancia kybernetických bezpečnostných cvičení vrátane cvičení organizovaných agentúrou ENISA;

m) na žiadosť niektorej jednotky CSIRT prediskutovanie spôsobilostí a pripravenosti tejto jednotky CSIRT;

n) spolupráca a výmena informácií s regionálnymi a únijnými centrami bezpečnostných operácií (SOC) s cieľom zlepšiť spoločné situačné povedomie o incidentoch a kybernetických hrozbách v celej Únii;

o) v príslušných prípadoch prediskutovanie správ o partnerskom preskúmaní uvedených v článku 19 ods. 9;

p) poskytovanie usmernení s cieľom uľahčiť zbližovanie operačných postupov so zreteľom na uplatňovanie ustanovení tohto článku, pokiaľ ide o operačnú spoluprácu.

4. Na účely preskúmania uvedeného v článku 40 sieť jednotiek CSIRT do 17. januára 2025 a potom každé dva roky posúdi pokrok dosiahnutý s ohľadom na operačnú spoluprácu a prijme správu. V správe sa predovšetkým vyvodia závery a odporúčania na základe výsledkov partnerských preskúmaní uvedených v článku 19 a vykonaných v súvislosti s národnými jednotkami CSIRT. Táto správa sa predloží skupine pre spoluprácu.

5. Sieť jednotiek CSIRT prijme svoj rokovací poriadok.

6. Sieť jednotiek CSIRT a sieť EU-CyCLONe sa dohodnú na procesných opatreniach a v súlade s nimi spolupracujú.

Článok 16

Európska sieť styčných organizácií pre kybernetické krízy (EU-CyCLONe)

1. Sieť EU-CyCLONe sa zriaďuje s cieľom podporiť koordinované riadenie rozsiahlych kybernetických incidentov a kríz na operačnej úrovni a zabezpečiť pravidelnú výmenu relevantných informácií medzi členskými štátmi a inštitúciami, orgánmi, úradmi a agentúrami Únie.

2. Sieť EU-CyCLONe tvoria zástupcovia orgánov členských štátov pre riadenie kybernetických kríz a v prípadoch, keď potenciálny alebo prebiehajúci rozsiahly kybernetický incident má alebo pravdepodobne bude mať významný vplyv na služby a činnosti patriace do rozsahu pôsobnosti tejto smernice, aj zástupcovia Komisie. Vo všetkých ostatných prípadoch sa Komisia zúčastňuje na činnostiach siete EU-CyCLONe ako pozorovateľ.

Agentúra ENISA zabezpečuje sekretariát siete EU-CyCLONe, podporuje bezpečnú výmenu informácií a poskytuje potrebné nástroje na podporu spolupráce medzi členskými štátmi zaistením bezpečnej výmeny informácií.

V náležitých prípadoch môže sieť EU-CyCLONe prizvať ako pozorovateľov k svojej práci zástupcov príslušných zainteresovaných strán.

3. Sieť EU-CyCLONe plní tieto úlohy:

a) zvyšovanie úrovne pripravenosti na riadenie rozsiahlych kybernetických incidentov a kríz;

b) rozvíjanie spoločného situačného povedomia o rozsiahlych kybernetických incidentoch a krízach;

c) posudzovanie dôsledkov a vplyvu relevantných rozsiahlych kybernetických incidentov a kríz a navrhovanie možných zmierňujúcich opatrení;

d) koordinácia riadenia rozsiahlych kybernetických incidentov a kríz a podpora rozhodovania na politickej úrovni v súvislosti s takýmito incidentmi a krízami;

e) na žiadosť príslušného členského štátu prediskutovanie národných plánov reakcie na rozsiahle kybernetické incidenty a krízy uvedených v článku 9 ods. 4;

4. Sieť EU-CyCLONe prijme vlastný rokovací poriadok.

5. Sieť EU-CyCLONe podáva skupine pre spoluprácu pravidelne správy o riadení rozsiahlych kybernetických incidentov a kríz, ako aj o trendoch, pričom sa zameriava najmä na ich vplyv na kľúčové a dôležité subjekty.

6. Sieť EU-CyCLONe spolupracuje so sieťou jednotiek CSIRT na základe dohodnutých procesných opatrení stanovených v článku 15 ods. 6.

7. Sieť EU-CyCLONe do 17. júla 2024 a potom každých 18 mesiacov predloží Európskemu parlamentu a Rade správu, v ktorej posúdi svoju prácu.

Článok 17

Medzinárodná spolupráca

Únia môže v prípade potreby v súlade s článkom 218 ZFEÚ uzatvárať medzinárodné dohody s tretími krajinami alebo medzinárodnými organizáciami, ktorými môže povoľovať a organizovať ich účasť na konkrétnych činnostiach skupiny pre spoluprácu, siete jednotiek CSIRT a siete EU-CyCLONe. Takéto dohody musia byť v súlade s právom Únie v oblasti ochrany údajov.

Článok 18

Správa o stave kybernetickej bezpečnosti v Únii

1. Agentúra ENISA v spolupráci s Komisiou a skupinou pre spoluprácu prijme každé dva roky správu o stave kybernetickej bezpečnosti v Únii a predkladá a prezentuje ju Európskemu parlamentu. Správa sa vydáva aj v strojovo čitateľnom formáte a obsahuje:

a) posúdenie kybernetických rizík na úrovni Únie s prihliadnutím na panorámu kybernetických hrozieb;

b) posúdenie rozvoja spôsobilostí v oblasti kybernetickej bezpečnosti vo verejnom a súkromnom sektore v celej Únii;

c) posúdenie všeobecnej úrovne informovanosti o kybernetickej bezpečnosti a kybernetickej hygieny medzi občanmi a subjektmi vrátane malých a stredných podnikov;

d) súhrnné posúdenie výsledkov partnerského preskúmania uvedeného v článku 19;

e) súhrnné posúdenie úrovne vyspelosti spôsobilostí a zdrojov v oblasti kybernetickej bezpečnosti v celej Únii vrátane spôsobilostí a zdrojov na úrovni odvetví, ako aj rozsahu, v akom sú národné stratégie kybernetickej bezpečnosti členských štátov zosúladené.

2. Správa obsahuje konkrétne politické odporúčania na riešenie problémov a zvýšenie úrovne kybernetickej bezpečnosti v celej Únii a zhrnutie zistení za konkrétne obdobie z technických situačných správ o kybernetickej bezpečnosti v EÚ o incidentoch a kybernetických hrozbách, ktoré vypracúva agentúra ENISA v súlade s článkom 7 ods. 6 nariadenia (EÚ) 2019/881.

3. Agentúra ENISA v spolupráci s Komisiou, skupinou pre spoluprácu a sieťou jednotiek CSIRT pripraví metodiku súhrnného posúdenia uvedeného v prvom odseku písm. e) vrátane príslušných premenných, ako sú kvantitatívne a kvalitatívne ukazovatele.

Článok 19

Partnerské preskúmania

1. Skupina pre spoluprácu do 17. januára 2025 s pomocou Komisie a agentúry ENISA a v prípade potreby siete jednotiek CSIRT vypracuje metodiku a organizačné aspekty partnerských preskúmaní s cieľom čerpať zo spoločných skúseností, posilniť vzájomnú dôveru, dosiahnuť vysokú spoločnú úroveň kybernetickej bezpečnosti, ako aj posilniť spôsobilosti kybernetickej bezpečnosti a politiky členských štátov potrebné na vykonávanie tejto smernice. Účasť na partnerských preskúmaniach je dobrovoľná. Partnerské preskúmania vykonávajú experti na kybernetickú bezpečnosť. Expertov na kybernetickú bezpečnosť určia minimálne dva iné členské štáty, než je členský štát, ktorý je predmetom preskúmania.

Partnerské preskúmania sa týkajú aspoň jedného z týchto aspektov:

a) úrovne vykonávania opatrení na riadenie kybernetických rizík a oznamovacích povinností stanovených v článkoch 21 a 23;

b) úrovne spôsobilostí vrátane dostupných finančných, technických a ľudských zdrojov a účinnosť plnenia úloh príslušných orgánov;

c) operačných spôsobilostí jednotiek CSIRT;

d) úrovne vykonávania vzájomnej pomoci uvedenej v článku 37;

e) úrovne vykonávania dohôd o výmene informácií o kybernetickej bezpečnosti uvedených v článku 29;

f) konkrétnych záležitostí cezhraničného alebo medziodvetvového charakteru.

2. Metodika uvedená v odseku 1 zahŕňa objektívne, nediskriminačné, spravodlivé a transparentné kritériá, na základe ktorých členské štáty určia expertov na kybernetickú bezpečnosť oprávnených vykonávať partnerské preskúmania. Komisia agentúra ENISA sa zúčastňujú na partnerských preskúmaniach ako pozorovatelia.

3. Členské štáty môžu určiť konkrétne záležitosti uvedené v odseku 1 písm. f) na účely partnerského preskúmania.

4. Pred začatím partnerského preskúmania uvedeného v odseku 1 členské štáty oznámia zúčastneným členským štátom jeho rozsah vrátane konkrétnych záležitostí určených podľa odseku 3.

5. Pred začatím partnerského preskúmania môžu členské štáty vykonať sebahodnotenie skúmaných aspektov a toto sebahodnotenie poskytnúť určeným expertom na kybernetickú bezpečnosť. Metodiku sebahodnotenia členských štátov stanoví skupina pre spoluprácu s pomocou Komisie a agentúry ENISA.

6. Partnerské preskúmania zahŕňajú osobné alebo virtuálne návštevy na mieste a výmenu informácií na diaľku. Členský štát, ktorý je predmetom partnerského preskúmania, poskytne v súlade so zásadou dobrej spolupráce určeným expertom na kybernetickú bezpečnosť informácie potrebné na hodnotenie, a to bez toho, aby bolo dotknuté právo Únie alebo vnútroštátne právo týkajúce sa ochrany dôverných alebo utajovaných skutočností a ochrany základných funkcií štátu, ako je národná bezpečnosť. Skupina pre spoluprácu v spolupráci s Komisiou a agentúrou ENISA vypracuje vhodné kódexy správania na podporu pracovných metód určených expertov na kybernetickú bezpečnosť. Všetky informácie získané v rámci partnerského preskúmania sa použijú výlučne na uvedený účel. Experti na kybernetickú bezpečnosť, ktorí sa zúčastňujú na partnerskom preskúmaní, nesmú sprístupniť tretím stranám žiadne citlivé alebo dôverné informácie získané v priebehu tohto partnerského preskúmania.

7. Tie isté aspekty, ktoré už boli predmetom partnerského preskúmania v členskom štáte, nepodliehajú ďalšiemu partnerskému preskúmaniu v tomto členskom štáte najbližšie dva roky od ukončenia partnerského preskúmania, pokiaľ o to členský štát nepožiada alebo nedôjde k dohode po návrhu skupiny pre spoluprácu.

8. Členské štáty zabezpečia, aby každé riziko konfliktu záujmov týkajúce sa určených expertov na kybernetickú bezpečnosť bolo oznámené ostatným členským štátom, skupine pre spoluprácu, Komisii a agentúre ENISA pred začatím postupu partnerského preskúmania. Členský štát, ktorý je predmetom partnerského preskúmania, môže na základe riadne opodstatnených dôvodov, ktoré oznámi určujúcemu členskému štátu, podať námietku proti určeniu konkrétnych expertov na kybernetickú bezpečnosť.

9. Experti na kybernetickú bezpečnosť zúčastňujúci sa na partnerských preskúmaniach vypracujú správy o zisteniach a záveroch partnerských preskúmaní. Členské štáty, ktoré sú predmetom partnerského preskúmania, môžu predložiť pripomienky k návrhom správ, ktoré sa ich týkajú, a takéto pripomienky sa priložia k správam. Správy obsahujú odporúčania s cieľom umožniť zlepšenie aspektov, ktoré sú predmetom partnerského preskúmania. Správy sú v náležitých prípadoch postúpené skupine pre spoluprácu a sieti jednotiek CSIRT. Členský štát, ktorý je predmetom partnerského preskúmania, sa môže rozhodnúť, že svoju správu alebo jej upravenú verziu sprístupní verejnosti.

KAPITOLA IV

OPATRENIA NA RIADENIE KYBERNETICKÝCH RIZÍK A OZNAMOVACIE POVINNOSTI

Článok 20

Riadenie

1. Členské štáty zabezpečia, aby riadiace orgány kľúčových a dôležitých subjektov schválili opatrenia na riadenie kybernetických rizík, ktoré tieto subjekty prijali s cieľom dosiahnuť súlad s článkom 21, dohliadali na jeho vykonávanie a aby mohli byť brané na zodpovednosť, ak subjekty porušujú uvedený článok.

Uplatňovaním tohto odseku nie je dotknuté vnútroštátne právo, pokiaľ ide o pravidlá zodpovednosti uplatniteľné na verejné inštitúcie, ako aj zodpovednosť štátnych zamestnancov a volených alebo menovaných činiteľov.

2. Členské štáty zabezpečia, aby členovia riadiacich orgánov kľúčových a dôležitých subjektov boli povinní absolvovať odbornú prípravu, a kľúčové a dôležité subjekty podporia v tom, aby svojim zamestnancom pravidelne poskytovali podobnú odbornú prípravu a ich zamestnanci tak získali dostatočné znalosti a zručnosti a vedeli rozpoznať riziká a posúdiť postupy riadenia kybernetických rizík a ich vplyv na služby poskytované subjektom.

Článok 21

Opatrenia na riadenie kybernetických rizík

1. Členské štáty zabezpečia, aby kľúčové a dôležité subjekty prijali vhodné a primerané technické, operačné a organizačné opatrenia na riadenie rizík súvisiacich s bezpečnosťou sietí a informačných systémov, ktoré tieto subjekty využívajú na svoju činnosť alebo na poskytovanie svojich služieb a na prevenciu alebo minimalizáciu vplyvu incidentov na príjemcov ich služieb a na ďalšie služby.

S prihliadnutím na najnovšie, resp. na relevantné európske a medzinárodné normy, ako aj na náklady na vykonávanie sa opatreniami uvedenými v prvom pododseku zabezpečí úroveň bezpečnosti sietí a informačných systémov primeraná rizikám, ktoré predstavujú. Pri posudzovaní primeranosti týchto opatrení sa náležite zohľadní miera vystavenia subjektu rizikám, veľkosť subjektu a pravdepodobnosť výskytu incidentov a ich závažnosti vrátane ich spoločenského a hospodárskeho dosahu.

2. Opatrenia uvedené v odseku 1 sú založené na prístupe zohľadňujúcom všetky riziká, ktorého cieľom je chrániť siete a informačné systémy a fyzické prostredie uvedených systémov pred incidentmi, a zahŕňajú aspoň:

a) zásady analýzy rizík a bezpečnosti informačných systémov;

b) riešenie incidentov;

c) kontinuitu činností, ako je riadenie zálohovania a obnova systému po havárii, a krízové riadenie;

d) bezpečnosť dodávateľského reťazca vrátane bezpečnostných aspektov týkajúcich sa vzťahov medzi jednotlivými subjektmi a ich priamymi dodávateľmi alebo poskytovateľmi služieb;

e) bezpečnosť pri nadobúdaní, vývoji a údržbe siete a informačných systémov vrátane riešenia zraniteľností a zverejňovania informácií o zraniteľnostiach;

f) zásady a postupy posudzovania účinnosti opatrení na riadenie kybernetických rizík;

g) základné postupy kybernetickej hygieny a odborná príprava v oblasti kybernetickej bezpečnosti;

h) zásady a postupy používania kryptografie, prípadne šifrovania;

i) bezpečnosť ľudských zdrojov, zásady kontroly prístupu a správu aktív;

j) v prípade potreby používanie riešení viacstupňovej alebo kontinuálnej autentifikácie, zabezpečenej hlasovej, obrazovej a textovej komunikácie a zabezpečených systémov komunikácie v núdzových situáciách v rámci subjektu.

3. Členské štáty zabezpečia, aby subjekty pri zvažovaní toho, ktoré opatrenia uvedené v odseku 2 písm. d) tohto článku sú vhodné, zohľadňovali zraniteľnosti špecifické pre každého priameho dodávateľa a poskytovateľa služieb a celkovú kvalitu produktov a postupy svojich dodávateľov a poskytovateľov služieb kybernetickej bezpečnosti vrátane ich postupov bezpečného vývoja. Členské štáty tiež zabezpečia, aby subjekty pri zvažovaní toho, ktoré opatrenia uvedené v uvedenom písmene sú vhodné, boli povinné zohľadňovať výsledky koordinovaných posúdení bezpečnostných rizík kritických dodávateľských reťazcov vykonaných v súlade s článkom 22 ods. 1.

4. Členské štáty zabezpečia, aby subjekt, ktorý zistí, že nedodržiava opatrenia stanovené v odseku 2, prijal bez zbytočného odkladu všetky potrebné, vhodné a primerané nápravné opatrenia.

5. Komisia do 17. októbra 2024 prijme vykonávacie akty, ktorými stanoví technické a metodické požiadavky na opatrenia uvedené v odseku 2, pokiaľ ide o poskytovateľov služieb DNS, správcov názvov TLD, poskytovateľov služieb cloud computingu, poskytovateľov služieb dátového centra, poskytovateľov sietí na sprístupňovanie obsahu, poskytovateľov riadených služieb, poskytovateľov riadených bezpečnostných služieb, poskytovateľov online trhov, internetových vyhľadávačov a platforiem služieb sociálnej siete a poskytovateľov dôveryhodných služieb.

Komisia môže prijať vykonávacie akty, ktorými podľa potreby stanoví technické, metodické, ako aj odvetvové požiadavky na opatrenia uvedené v odseku 2, pokiaľ ide o iné kľúčové a dôležité subjekty, než sú subjekty uvedené v prvom pododseku tohto odseku.

Komisia pri príprave vykonávacích aktov uvedených v prvom a druhom pododseku tohto odseku sa v čo najväčšej možnej miere riadi európskymi a medzinárodnými normami, ako aj príslušnými technickými špecifikáciami. Komisia sa radí a spolupracuje so skupinou pre spoluprácu a agentúrou ENISA v súlade s článkom 14 ods. 4 písm. e), pokiaľ ide o návrhy vykonávacích aktov.

Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2.

Článok 22

Koordinované posúdenia bezpečnostných rizík kritických dodávateľských reťazcov na úrovni Únie

1. Skupina pre spoluprácu môže v spolupráci s Komisiou a agentúrou ENISA vykonávať koordinované posúdenia bezpečnostných rizík dodávateľských reťazcov konkrétnych kritických služieb IKT, systémov IKT alebo produktov IKT, pričom zohľadní technické a prípadne aj netechnické faktory rizík.

2. Komisia po konzultácii so skupinou pre spoluprácu a agentúrou ENISA a v prípade potreby s príslušnými zainteresovanými stranami určí konkrétne kritické služby IKT, systémy IKT alebo produkty IKT, ktoré môžu podliehať koordinovanému posúdeniu bezpečnostných rizík uvedenému v odseku 1.

Článok 23

Oznamovacie povinnosti

1. Každý členský štát zabezpečí, aby kľúčové a dôležité subjekty bez zbytočného odkladu oznámili svojej jednotke CSIRT alebo v náležitých prípadoch svojmu príslušnému orgánu v súlade s odsekom 4 každý incident s významným vplyvom na poskytovanie ich služieb ako sa uvádza v odseku 3 (významný incident). V prípade potreby dotknuté subjekty bez zbytočného odkladu oznámia príjemcom svojich služieb významné incidenty, ktoré by mohli nepriaznivo ovplyvniť poskytovanie daných služieb. Každý členský štát zabezpečí, aby tieto subjekty oznamovali okrem iného informácie umožňujúce jednotke CSIRT alebo v náležitých prípadoch príslušnému orgánu určiť cezhraničný vplyv incidentu. Samotný akt oznámenia nezakladá zvýšenú zodpovednosť oznamujúceho subjektu.

Ak dotknuté subjekty oznámia príslušnému orgánu významný incident podľa prvého pododseku, členský štát zabezpečí, aby uvedený príslušný orgán postúpil toto oznámenie po jeho prijatí jednotke CSIRT.

V prípade cezhraničného alebo medziodvetvového významného incidentu členské štáty zabezpečia, aby sa ich jednotným kontaktným miestam včas poskytli príslušné informácie oznámené v súlade s odsekom 4.

2. Členské štáty v náležitých prípadoch zabezpečia, aby kľúčové a dôležité subjekty bez zbytočného odkladu oznámili príjemcom svojich služieb, ktorí potenciálne čelia významnej kybernetickej hrozbe, všetky opatrenia alebo nápravné kroky, ktoré títo príjemcovia môžu v reakcii na danú hrozbu prijať. Subjekty v prípade potreby týchto príjemcov informujú aj o samotnej významnej kybernetickej hrozbe.

3. Incident sa považuje za významný, ak:

a) spôsobil alebo má schopnosť spôsobiť dotknutému subjektu závažné prevádzkové narušenie služieb alebo finančnú stratu;

b) zasiahol alebo má schopnosť zasiahnuť iné fyzické alebo právnické osoby tým, že im spôsobí značnú majetkovú alebo nemajetkovú ujmu.

4. Členské štáty zabezpečia, aby dotknuté subjekty na účely oznámenia podľa odseku 1 postúpili jednotke CSIRT alebo v náležitých prípadoch príslušnému orgánu:

a) bez zbytočného odkladu a v každom prípade do 24 hodín od zistenia významného incidentu včasné varovanie, v ktorom sa prípadne uvedie, či významný incident pravdepodobne spôsobilo konanie, ktoré je nezákonné alebo so zlým úmyslom, alebo či môže mať cezhraničný dosah;

b) bez zbytočného odkladu a v každom prípade do 72 hodín po tom, ako sa dozvedeli o významnom incidente, oznámenie o incidente, ktorým v prípade potreby aktualizujú informácie uvedené v písmene a) a uvedú prvotné posúdenie významného incidentu, vrátane jeho závažnosti a vplyvu, ako aj prípadne indikátory kompromitácie.

c) na žiadosť jednotky CSIRT alebo v náležitých prípadoch príslušného orgánu priebežnú správu s relevantnou aktualizáciou daného stavu;

d) najneskôr jeden mesiac po postúpení oznámenia o incidente podľa písmena b) záverečnú správu, ktorá obsahuje tieto informácie:

   i) podrobný opis incidentu vrátane jeho závažnosti a vplyvu;

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

   iii) zavedené a prebiehajúce zmierňujúce opatrenia;

   iv) v náležitých prípadoch cezhraničný vplyv incidentu;

e) v prípade, že v čase predkladania záverečnej správy uvedenej v písmene d) incident ešte prebieha, členské štáty zabezpečia, aby dotknuté subjekty predložili v uvedenom čase ďalšiu priebežnú správu a záverečnú správu do jedného mesiaca odo dňa, keď incident vyriešili.

Odchylne od prvého pododseku písm. b) poskytovateľ dôveryhodných služieb informuje jednotku CSIRT alebo v náležitých prípadoch príslušný orgán o významných incidentoch, ktoré majú vplyv na poskytovanie jeho dôveryhodných služieb, a to bez zbytočného odkladu a v každom prípade do 24 hodín od zistenia významného incidentu.

5. Jednotka CSIRT alebo príslušný orgán bez zbytočného odkladu a v rámci možností do 24 hodín od doručenia včasného varovania uvedeného v odseku 4 písm. a) poskytne oznamujúcemu subjektu odpoveď vrátane prvotnej spätnej väzby k významnému incidentu a na žiadosť subjektu usmernenie alebo operačné pokyny k vykonávaniu možných zmierňujúcich opatrení. Ak jednotka CSIRT nie je prvotným príjemcom oznámenia uvedeného v odseku 1, usmernenie poskytne príslušný orgán v spolupráci s jednotkou CSIRT. Jednotka CSIRT poskytne doplňujúcu technickú podporu, ak o to dotknutý subjekt požiada. Ak existuje podozrenie, že významný incident je trestnoprávnej povahy, jednotka CSIRT alebo príslušný orgán poskytne aj usmernenie, ako významný incident oznámiť orgánom presadzovania práva.

6. V prípade potreby, a najmä ak sa významný incident týka dvoch alebo viacerých členských štátov, jednotka CSIRT, príslušný orgán alebo jednotné kontaktné miesto bez zbytočného odkladu informuje o významnom incidente ostatné zasiahnuté členské štáty a agentúru ENISA. Takéto informácie obsahujú informácie toho typu, ktoré boli doručené v súlade s odsekom 4. Jednotka CSIRT, príslušný orgán alebo jednotné kontaktné miesto pritom v súlade s právom Únie alebo vnútroštátnymi právom chránia bezpečnosť a obchodné záujmy subjektu, ako aj dôvernosť poskytnutých informácií.

7. Po porade s dotknutým subjektom môže jednotka CSIRT, prípadne príslušný orgán členského štátu a v náležitých prípadoch jednotky CSIRT alebo príslušné orgány ďalších dotknutých členských štátov informovať o významnom incidente verejnosť alebo požiadať o to daný subjekt, ak je informovanie verejnosti potrebné na zabránenie významnému incidentu alebo riešenie prebiehajúceho incidentu alebo ak je zverejnenie významného incidentu vo verejnom záujme z iného dôvodu.

8. Na žiadosť jednotky CSIRT alebo príslušného orgánu jednotné kontaktné miesto postúpi doručené oznámenia podľa odseku 1 jednotným kontaktným miestam ostatných zasiahnutých členských štátov.

9. Jednotné kontaktné miesto predkladá agentúre ENISA každé tri mesiace súhrnnú správu s anonymizovanými a agregovanými údajmi o významných incidentoch, incidentoch, kybernetických hrozbách a udalostiach odvrátených v poslednej chvíli oznámených v súlade s odsekom 1 tohto článku a s článkom 30. S cieľom prispieť k poskytovaniu porovnateľných informácií môže agentúra ENISA prijať technické usmernenia k parametrom informácií, ktoré sa majú uvádzať v súhrnnej správe. Agentúra ENISA každých šesť mesiacov informuje skupinu pre spoluprácu a sieť jednotiek CSIRT o svojich zisteniach týkajúcich sa doručených oznámení.

10. Jednotky CSIRT alebo v náležitých prípadoch príslušné orgány poskytujú príslušným orgánom podľa smernice (EÚ) 2022/2557 informácie o významných incidentoch, incidentoch, kybernetických hrozbách a udalostiach odvrátených v poslednej chvíli, ktoré v súlade s odsekom 1 tohto článku a s článkom 30 oznámili subjekty označené ako kritické subjekty podľa smernice (EÚ) 2022/2557.

11. Komisia môže prijať vykonávacie akty, v ktorých bližšie určí druh informácií, formát a postup oznámenia predkladaného podľa odseku 1 tohto článku a článku 30 a komunikácie predkladanej podľa odseku 2 tohto článku.

Komisia do 17. októbra 2024 vo vzťahu k poskytovateľom služieb DNS, správcom názvov TLD, poskytovateľom služieb cloud computingu, poskytovateľom služieb dátového centra, poskytovateľom sietí na sprístupňovanie obsahu, poskytovateľom riadených služieb, poskytovateľom riadených bezpečnostných služieb, ako aj poskytovateľom online trhov, internetových vyhľadávačov a platforiem služieb sociálnych sietí prijme vykonávacie akty, v ktorých bližšie určí prípady, v ktorých sa incident považuje za významný, ako sa uvádza v odseku 3. Komisia môže prijať takéto vykonávacie akty vo vzťahu k iným kľúčovým a dôležitým subjektom.

Komisia sa radí a spolupracuje so skupinou pre spoluprácu v súlade s článkom 14 ods. 4 písm. e), pokiaľ ide o návrhy vykonávacích aktov uvedených v prvom a druhom pododseku tohto odseku.

Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2.

Článok 24

Používanie európskych systémov certifikácie kybernetickej bezpečnosti

1. S cieľom preukázať súlad s určitými požiadavkami článku 21 môžu členské štáty vyžadovať, aby kľúčové a dôležité subjekty používali určité produkty IKT, služby IKT a procesy IKT, ktoré vyvinul kľúčový alebo dôležitý subjekt alebo boli obstarané od tretích strán certifikovaných podľa európskych systémov certifikácie kybernetickej bezpečnosti prijatých podľa článku 49 nariadenia (EÚ) 2019/881. Členské štáty navyše podporujú kľúčové a dôležité subjekty v tom, aby využívali kvalifikované dôveryhodné služby.

2. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 38 s cieľom doplniť túto smernicu a bližšie určiť kategórie kľúčových a dôležitých subjektov, od ktorých sa má vyžadovať používanie určitých certifikovaných produktov IKT, služieb IKT a procesov IKT alebo získanie certifikátu v rámci európskeho systému certifikácie kybernetickej bezpečnosti prijatého podľa článku 49 nariadenia (EÚ) 2019/881. Uvedené delegované akty sa prijmú v prípade, že sa zistí nedostatočná úroveň kybernetickej bezpečnosti, a stanoví sa v nich obdobie vykonávania.

Komisia pred prijatím takýchto delegovaných aktov vykoná posúdenie vplyvov a uskutoční konzultácie v súlade s článkom 56 nariadenia (EÚ) 2019/881.

3. V prípadoch, keď nie je k dispozícii žiadny európsky systém certifikácie kybernetickej bezpečnosti na účely odseku 2 tohto článku, Komisia po porade so skupinou pre spoluprácu a európskou skupinou pre certifikáciu kybernetickej bezpečnosti môže požiadať agentúru ENISA, aby vypracovala kandidátsky systém podľa článku 48 ods. 2 nariadenia (EÚ) 2019/881.

Článok 25

Normalizácia

1. Členské štáty v záujme harmonizovaného vykonávania článku 21 ods. 1 a 2 a bez toho, aby ukladali povinnosť využívať určitý typ technológie alebo diskriminovali v prospech takéhoto využívania, podporujú využívanie európskych a medzinárodných noriem a technických špecifikácií, ktoré sú relevantné pre bezpečnosť sietí a informačných systémov.

2. Agentúra ENISA v spolupráci s členskými štátmi a v prípade potreby po konzultácii s príslušnými zainteresovanými stranami vypracuje odporúčania a usmernenia pre technické oblasti, ktoré sa majú zvážiť v súvislosti s odsekom 1, ako aj odporúčania a usmernenia k už existujúcim normám vrátane vnútroštátnych noriem, ktoré by sa mohli vzťahovať na uvedené oblasti.

KAPITOLA V

PRÁVOMOC A REGISTRÁCIA

Článok 26

Právomoc a teritorialita

1. Subjekty, ktoré patria do rozsahu pôsobnosti tejto smernice sa považujú za subjekty podliehajúce právomoci členského štátu, v ktorom sú usadené, s výnimkou:

a) poskytovateľov verejných elektronických komunikačných sietí alebo poskytovateľov verejne dostupných elektronických komunikačných služieb, ktorí sa považujú za poskytovateľov podliehajúcich právomoci členského štátu, v ktorom poskytujú svoje služby;

b) poskytovateľov služieb DNS, správcov názvov TLD, subjektov poskytujúcich služby registrácie názvov domén, poskytovateľov služieb cloud computingu, poskytovateľov služieb dátového centra, poskytovateľov sietí na sprístupňovanie obsahu, poskytovateľov riadených služieb, poskytovateľov riadených bezpečnostných služieb, ako aj poskytovateľov online trhov, internetových vyhľadávačov a platforiem služieb sociálnej siete, ktorí sa považujú za subjekty podliehajúce právomoci toho členského štátu, v ktorom majú hlavnú prevádzkareň v Únii podľa odseku 2;

c) subjektov verejnej správy, ktoré sa považujú za subjekty podliehajúce právomoci členského štátu, ktorý ich zriadil.

2. Na účely tejto smernice platí, že subjekt uvedený v odseku 1 písm. b) má svoju hlavnú prevádzkareň v Únii v členskom štáte, v ktorom najčastejšie prijíma rozhodnutia týkajúce sa opatrení na riadenie kybernetických rizík. Ak takýto členský štát nemožno určiť alebo ak sa takéto rozhodnutia neprijímajú v Únii, za hlavnú prevádzkareň sa považuje členský štát, v ktorom sa vykonávajú operácie kybernetickej bezpečnosti. Ak takýto členský štát nemožno určiť, za hlavnú prevádzkareň sa považuje členský štát, v ktorom má dotknutý subjekt prevádzkareň s najvyšším počtom zamestnancov v Únii.

3. Ak subjekt uvedený v odseku 1 písm. b) nie je usadený v Únii, ale ponúka služby v rámci Únie, určí zástupcu v Únii. Zástupca musí byť usadený v jednom z tých členských štátov, v ktorých subjekt ponúka služby. Takýto subjekt sa považuje za subjekt podliehajúci právomoci toho členského štátu, v ktorom je usadený jeho zástupca. Ak v Únii nie je určený zástupca podľa tohto odseku, ktorýkoľvek členský štát, v ktorom subjekt poskytuje služby, môže proti tomuto subjektu podniknúť právne kroky za porušenie tejto smernice.

4. Tým, že subjekt uvedený v odseku 1 písm. b) určí svojho zástupcu, nie sú dotknuté právne kroky, ktoré by mohli byť podniknuté proti samotnému subjektu.

5. Členské štáty, ktorým bola doručená žiadosť o vzájomnú pomoc týkajúcu sa subjektu uvedeného v odseku 1 písm. b), môžu v medziach uvedenej žiadosti prijať primerané opatrenia dohľadu a presadzovania práva vo vzťahu k dotknutému subjektu, ktorý poskytuje služby alebo má sieť a informačný systém na ich území.

Článok 27

Register subjektov

1. Agentúra ENISA zriadi a vedie register poskytovateľov služieb DNS, správcov názvov TLD, subjektov poskytujúcich služby registrácie názvov domén, poskytovateľov služieb cloud computingu, poskytovateľov služieb dátového centra, poskytovateľov sietí na sprístupňovanie obsahu, poskytovateľov riadených služieb, poskytovateľov riadených bezpečnostných služieb, ako aj poskytovateľov online trhov, internetových vyhľadávačov a platforiem služieb sociálnych sietí na základe informácií získaných od jednotných kontaktných miest v súlade s odsekom 4. Agentúra ENISA umožní príslušným orgánom na požiadanie prístup do uvedeného registra, pričom v náležitých prípadoch zabezpečí ochranu dôvernosti informácií.

2. Členské štáty do 17. januára 2025 požiadajú subjekty uvedené v odseku 1, aby príslušným orgánom predložili tieto informácie:

a) názov subjektu;

b) podľa potreby príslušné odvetvie, pododvetvie a typ subjektu, ako sú uvedené v prílohe I alebo II;

c) adresu hlavnej prevádzkarne subjektu a jeho iných zákonných prevádzkarní v Únii, alebo ak subjekt nie je usadený v Únii, adresu svojho zástupcu určeného podľa článku 26 ods. 3;

d) aktuálne kontaktné údaje vrátane e-mailových adries a telefónnych čísel subjektu a v náležitom prípade jeho zástupcu určeného podľa článku 26 ods. 3;

e) členské štáty, v ktorých subjekt poskytuje služby; a

f) rozsahy IP adries subjektu.

3. Členské štáty zabezpečia, aby subjekty uvedené v odseku 1 oznámili príslušnému orgánu všetky zmeny údajov, ktoré predložili podľa odseku 2, a to bezodkladne a v každom prípade do troch mesiacov odo dňa zmeny.

4. Po doručení informácií uvedených v odsekoch 2 a 3, s výnimkou informácií uvedených v odseku 2 písm. f), jednotné kontaktné miesto dotknutého členského štátu postúpi tieto informácie bez zbytočného odkladu agentúre ENISA.

5. Informácie uvedené v odsekoch 2 a 3 tohto článku sa prípadne podávajú prostredníctvom vnútroštátneho mechanizmu uvedeného v článku 3 ods. 4 štvrtom pododseku.

Článok 28

Databáza registračných údajov názvov domén

1. S cieľom prispieť k bezpečnosti, stabilite a odolnosti DNS členské štáty požadujú, aby správcovia názvov TLD a subjekty poskytujúce služby registrácie názvov domén s náležitou starostlivosťou zhromažďovali a uchovávali presné a úplné registračné údaje názvov domén vo vyhradenej databáze v súlade s právom Únie v oblasti ochrany údajov, pokiaľ ide o údaje, ktoré sú osobnými údajmi.

2. Na účely odseku 1 členské štáty požadujú, aby databáza registračných údajov názvov domén obsahovala nevyhnutné informácie na identifikáciu a kontaktovanie držiteľov názvov domén a kontaktných miest spravujúcich názvy domén v rámci TLD. Takéto informácie zahŕňajú:

a) názov domény;

b) dátum registrácie;

c) meno/názov žiadateľa o registráciu, kontaktnú e-mailovú adresu a telefónne číslo;

d) kontaktnú e-mailovú adresu a telefónne číslo kontaktného miesta spravujúceho názov domény v prípade, že sa líšia od adresy a čísla žiadateľa o registráciu.

3. Členské štáty požadujú, aby správcovia názvov TLD a subjekty poskytujúce služby registrácie názvov domén mali zavedené politiky a postupy vrátane postupov overovania s cieľom zabezpečiť, aby databázy uvedené v odseku 1 obsahovali presné a úplné informácie. Členské štáty požadujú, aby takéto politiky a postupy boli verejne dostupné.

4. Členské štáty požadujú, aby správcovia názvov TLD a subjekty poskytujúce služby registrácie názvov domén bez zbytočného odkladu po registrácii názvu domény zverejnili registračné údaje názvu domény, ktoré nie sú osobnými údajmi.

5. Členské štáty požadujú, aby správcovia názvov TLD a subjekty poskytujúce služby registrácie názvov domén poskytovali prístup k špecifickým registračným údajom názvov domén na základe zákonných a riadne odôvodnených žiadostí oprávnených záujemcov o prístup v súlade s právom Únie v oblasti ochrany údajov. Členské štáty požadujú, aby správcovia názvov TLD a subjekty poskytujúce služby registrácie názvov domén odpovedali bez zbytočného odkladu a v každom prípade do 72 hodín od doručenia akýchkoľvek žiadostí o prístup. Členské štáty požadujú, aby politiky a postupy zverejňovania takýchto údajov boli verejne dostupné.

6. Dodržiavanie povinností stanovených v odsekoch 1 až 5 nesmie viesť k duplicitnému zberu registračných údajov názvov domén. Na tento účel členské štáty požadujú, aby správcovia názvov TLD a subjekty poskytujúce služby registrácie názvov domén navzájom spolupracovali.

KAPITOLA VI

VÝMENA INFORMÁCIÍ

Článok 29

Dohody o výmene informácií o kybernetickej bezpečnosti

1. Členské štáty zabezpečia, aby si subjekty, ktoré patria do rozsahu pôsobnosti tejto smernice, a v náležitých prípadoch ďalšie subjekty, ktoré nepatria do rozsahu pôsobnosti tejto smernice, mohli dobrovoľne medzi sebou vymieňať relevantné informácie o kybernetickej bezpečnosti vrátane informácií o kybernetických hrozbách, udalostiach odvrátených v poslednej chvíli, zraniteľnostiach, technikách a postupoch, indikátoroch kompromitácie, nepriateľských taktikách, informácie špecifické pre jednotlivé hrozby a aktérov, výstrahy a odporúčania týkajúce sa konfigurácie kybernetických bezpečnostných nástrojov na odhaľovanie kybernetických útokov, ak takáto výmena informácií:

a) má za cieľ predchádzať incidentom, odhaľovať ich, reagovať na ne alebo zotaviť sa z nich, alebo zmierniť ich vplyv;

b) zvyšuje úroveň kybernetickej bezpečnosti, najmä zvyšovaním informovanosti o kybernetických hrozbách, obmedzovaním alebo zabraňovaním možnosti šírenia takýchto hrozieb, podporou celej škály obranných spôsobilostí, nápravou zraniteľností a zverejňovaním informácií o nich, odhaľovaním hrozieb, technikami na zamedzenie ich šírenia a na ich predchádzanie, stratégiami zmierňovania alebo fázami reakcie a zotavenia, resp. podporou spoločného výskumu kybernetických hrozieb verejnými a súkromnými subjektmi.

2. Členské štáty zabezpečia, aby sa výmena informácií uskutočňovala v rámci komunít kľúčových a dôležitých subjektov, prípadne ich dodávateľov alebo poskytovateľov služieb. Takáto výmena sa uskutočňuje na základe dohôd o výmene informácií o kybernetickej bezpečnosti s ohľadom na potenciálne citlivú povahu vymieňaných informácií.

3. Uzavretie dohôd o výmene informácií o kybernetickej bezpečnosti uvedených v odseku 2 tohto článku sprostredkujú členské štáty. V takýchto dohodách sa môžu špecifikovať operačné prvky vrátane využívania špecializovaných platforiem IKT a nástrojov automatizácie, ako aj obsah a podmienky dohôd o výmene informácií. Tým, že členské štáty stanovia podrobnosti o zapojení orgánov verejnej moci do takýchto dohôd, môžu uložiť podmienky zverejňovania informácií príslušnými orgánmi alebo jednotkami CSIRT. Členské štáty pomáhajú s uplatňovaním takýchto dohôd v súlade so svojimi politikami uvedenými v článku 7 ods. 2 písm. h).

4. Členské štáty zabezpečia, aby kľúčové a dôležité subjekty oznamovali príslušným orgánom svoju účasť na dohodách o výmene informácií o kybernetickej bezpečnosti uvedených v odseku 2 hneď, ako takéto dohody uzatvoria, prípadne ich odstúpenie od takýchto dohôd hneď, ako odstúpenie nadobudne účinnosť.

5. Agentúra ENISA poskytuje pomoc pri uzatváraní dohôd o výmene informácií o kybernetickej bezpečnosti uvedených v odseku 2 tým, že umožňuje výmenu najlepších postupov a poskytuje rady.

Článok 30

Dobrovoľné oznámenie relevantných informácií

1. Členské štáty zabezpečia, aby okrem oznamovacej povinnosti stanovenej v článku 23 mohli jednotkám CSIRT alebo prípadne príslušným orgánom podávať oznámenia dobrovoľne tieto subjekty:

a) kľúčové a dôležité subjekty v súvislosti s incidentmi, kybernetickými hrozbami a udalosťami odvrátenými v poslednej chvíli;

b) iné subjekty, než sú subjekty uvedené v písmene a), bez ohľadu na to, či patria do rozsahu pôsobnosti tejto smernice, v súvislosti s významnými incidentmi, kybernetickými hrozbami a udalosťami odvrátenými v poslednej chvíli.

2. Členské štáty spracujú oznámenie uvedené v odseku 1 tohto článku v súlade s postupom stanoveným v článku 23. Členské štáty môžu spracovanie povinných oznámení uprednostniť pred dobrovoľnými oznámeniami.

V prípade potreby jednotky CSIRT a v náležitom prípade príslušné orgány poskytnú jednotným kontaktným miestam informácie o oznámeniach doručených podľa tohto článku, pričom zabezpečia dôvernosť a primeranú ochranu informácií poskytnutých oznamujúcim subjektom. Bez toho, aby bola dotknutá prevencia, vyšetrovanie, odhaľovanie a stíhanie trestných činov, oznamujúcemu subjektu nevznikajú v dôsledku dobrovoľného oznámenia žiadne ďalšie povinnosti, ktoré by sa naň neboli vzťahovali, ak by oznámenie nepodal.

KAPITOLA VII

DOHĽAD A PRESADZOVANIE PRÁVA

Článok 31

Všeobecné aspekty dohľadu a presadzovania práva

1. Členské štáty zabezpečia, aby ich príslušné orgány účinne dohliadali a prijímali opatrenia potrebné na zabezpečenie súladu s touto smernicou.

2. Členské štáty môžu povoliť svojim príslušným orgánom, aby uprednostnili úlohy dohľadu. Takéto uprednostňovanie vychádza z prístupu založeného na rizikách. Príslušné orgány môžu na tento účel pri vykonávaní svojich úloh dohľadu stanovených v článkoch 32 a 33 stanoviť metodiky dohľadu, ktoré umožnia uprednostnenie takýchto úloh podľa prístupu založeného na rizikách.

3. Príslušné orgány pri riešení incidentov, ktoré majú za následok porušenie ochrany osobných údajov, úzko spolupracujú s orgánmi dohľadu podľa nariadenia (EÚ) 2016/679 bez toho, aby boli dotknuté kompetencie a úlohy orgánov dohľadu podľa uvedeného nariadenia.

4. Bez toho, aby boli dotknuté vnútroštátne legislatívne a inštitucionálne rámce, členské štáty zabezpečia, aby príslušné orgány mali pri dohľade nad dodržiavaním tejto smernice subjektami verejnej správy a pri ukladaní opatrení presadzovania práva v súvislosti s porušeniami tejto smernice primerané právomoci na plnenie takýchto úloh s operačnou nezávislosťou od dohliadaných subjektov verejnej správy. Členské štáty môžu rozhodnúť o uložení vhodných, primeraných a účinných opatrení v oblasti dohľadu a na presadzovanie práva vo vzťahu k týmto subjektom v súlade s vnútroštátnymi legislatívnymi a inštitucionálnymi rámcami.

Článok 32

Opatrenia dohľadu a presadzovania práva týkajúce sa kľúčových subjektov

1. Členské štáty zabezpečia, aby opatrenia dohľadu alebo presadzovania práva uložené kľúčovým subjektom v súvislosti s povinnosťami stanovenými v tejto smernici boli účinné, primerané a odrádzajúce a zároveň zohľadňovali okolnosti každého jednotlivého prípadu.

2. Členské štáty zabezpečia, aby príslušné orgány pri vykonávaní svojich úloh dohľadu nad kľúčovými subjektmi mali právomoc podrobiť tieto subjekty prinajmenšom:

a) inšpekciám na mieste a dohľadu na diaľku vrátane náhodných kontrol, ktoré vykonávajú vyškolení odborníci;

b) pravidelným a cieleným bezpečnostným auditom, ktoré vykonáva nezávislý orgán alebo príslušný orgán;

c) auditom ad hoc, a to v prípadoch odôvodnených významným incidentom alebo porušením tejto smernice kľúčovým subjektom;

d) bezpečnostným kontrolám podľa objektívnych, nediskriminačných, spravodlivých a transparentných kritérií posudzovania rizík, v prípade potreby v spolupráci s dotknutým subjektom;

e) žiadostiam o informácie potrebné na posúdenie opatrení na riadenie kybernetických rizík, ktoré dotknutý subjekt prijal, vrátane zdokumentovaných politík kybernetickej bezpečnosti, ako aj dodržiavania povinnosti predložiť informácie príslušným orgánom podľa článku 27;

f) žiadostiam o prístup k údajom, dokumentom a informáciám potrebným na plnenie ich úloh dohľadu;

g) žiadostiam o dôkazy vykonávania politík kybernetickej bezpečnosti, ako sú výsledky bezpečnostných auditov uskutočnených kvalifikovaným audítorom a príslušné podkladové dôkazy.

Cielené bezpečnostné audity uvedené v prvom pododseku písm. b) sú založené na posúdeniach rizík, ktoré vypracoval príslušný orgán alebo auditovaný subjekt, alebo na iných dostupných informáciách týkajúcich sa rizík.

Výsledky každého cieleného bezpečnostného auditu sa sprístupnia príslušnému orgánu. Náklady na takýto cielený bezpečnostný audit, ktorý vykonáva nezávislý orgán, hradí auditovaný subjekt, s výnimkou riadne odôvodnených prípadov, keď príslušný orgán rozhodne inak.

3. Príslušné orgány pri vykonávaní svojich právomocí podľa odseku 2 písm. e), f) alebo g) uvedú účel žiadosti a konkretizujú požadované informácie.

4. Členské štáty zabezpečia, aby ich príslušné orgány pri vykonávaní svojich právomocí presadzovania práva v súvislosti s kľúčovými subjektmi mali právomoc prinajmenšom:

a) vydávať varovania o porušeniach tejto smernice dotknutými subjektmi;

b) prijímať záväzné pokyny, a to aj v súvislosti s opatreniami potrebnými na prevenciu alebo nápravu incidentu, ako aj lehotami na vykonávanie takýchto opatrení a podávanie správ o ich vykonávaní, alebo príkaz, ktorým sa od dotknutých subjektov vyžaduje napraviť zistené nedostatky alebo porušenia tejto smernice;

c) nariadiť dotknutým subjektom, aby upustili od konania, ktoré porušuje túto smernicu, a takéto konanie neopakovali;

d) nariadiť dotknutým subjektom, aby určeným spôsobom a v určenej lehote zosúladili svoje opatrenia na riadenie kybernetických rizík s článkom 21 alebo splnili oznamovacie povinnosti stanovené v článku 23;

e) nariadiť dotknutým subjektom, aby informovali fyzické alebo právnické osoby, v súvislosti s ktorými poskytujú služby alebo vykonávajú činnosti, ktoré sú potenciálne zasiahnuté významnou kybernetickou hrozbou, o povahe hrozby, ako aj o akýchkoľvek možných ochranných alebo nápravných opatreniach, ktoré môžu tieto fyzické alebo právnické osoby prijať v reakcii na danú hrozbu;

f) nariadiť dotknutým subjektom, aby v primeranej lehote vykonali odporúčania poskytnuté na základe bezpečnostného auditu;

g) určiť monitorujúceho úradníka s presne vymedzenými úlohami na určité obdobie, ktorý bude dohliadať na dodržiavanie článkov 21 a 23 dotknutými subjektmi;

h) nariadiť dotknutým subjektom, aby určeným spôsobom zverejnili aspekty porušovania tejto smernice;

i) uložiť správnu pokutu podľa článku 34 alebo požiadať o jej uloženie príslušné orgány, súdy alebo tribunály v súlade s vnútroštátnym právom, a to popri ktoromkoľvek z opatrení uvedených v písmenách a) až h) tohto odseku.

5. Ak sa opatrenia na presadzovanie práva prijaté podľa odseku 4 písm. a) až d) a f) ukážu ako neúčinné, členské štáty zabezpečia, aby ich príslušné orgány mali právomoc stanoviť lehotu, v rámci ktorej je kľúčový subjekt povinný prijať potrebné opatrenia na nápravu nedostatkov alebo splniť požiadavky týchto orgánov. Ak sa požadované opatrenie v stanovenej lehote neprijme, členské štáty zabezpečia, aby ich príslušné orgány mali právomoc:

a) dočasne pozastaviť certifikáciu alebo povoľovanie alebo požiadať certifikačný alebo povoľujúci subjekt, súd, alebo tribunál v súlade s vnútroštátnym právom, aby dočasne pozastavil certifikáciu alebo povoľovanie časti alebo všetkých relevantných služieb, ktoré kľúčový subjekt poskytuje, alebo činností, ktoré kľúčový subjekt vykonáva;

b) od príslušných orgánov, súdov alebo tribunálov v súlade s vnútroštátnym právom požadovať uloženie dočasného zákazu vykonávať riadiace funkcie v tomto kľúčovom subjekte, a to akejkoľvek fyzickej osobe zodpovednej za vykonávanie riadiacich úloh na úrovni výkonného riaditeľa alebo právneho zástupcu v tomto kľúčovom subjekte.

Dočasné pozastavenia alebo zákazy podľa tohto odseku sa uplatňujú len dovtedy, kým dotknutý subjekt neprijme potrebné opatrenia na nápravu nedostatkov alebo nesplní požiadavky príslušného orgánu, ktorý takéto opatrenia presadzovania práva uložil. Ukladanie takýchto dočasných pozastavení alebo zákazov musí podliehať primeraným procesným zárukám podľa všeobecných zásad práva Únie a charty vrátane práva na účinný prostriedok nápravy a na spravodlivý proces, prezumpciu neviny a práva na obhajobu.

Opatrenia presadzovania práva stanovené v tomto odseku sa neuplatňujú na subjekty verejnej správy, na ktoré sa vzťahuje táto smernica.

6. Členské štáty zabezpečia, aby každá fyzická osoba zodpovedná za kľúčový subjekt alebo konajúca ako jeho právny zástupca na základe právomoci zastupovať ho, prijímať rozhodnutia v jeho mene alebo vykonávať kontrolu nad ním mala právomoc zabezpečiť dodržiavanie tejto smernice. Členské štáty zabezpečia, aby bolo možné brať takéto fyzické osoby na zodpovednosť za porušenie ich úloh zabezpečovať dodržiavanie tejto smernice.

Pokiaľ ide o subjekty verejnej správy, týmto odsekom nie je dotknuté vnútroštátne právo, pokiaľ ide o zodpovednosť štátnych zamestnancov a volených alebo menovaných činiteľov.

7. Príslušné orgány pri prijímaní ktoréhokoľvek z opatrení na presadzovanie práva uvedených v odseku 4 alebo 5 dodržiavajú právo na obhajobu a zohľadňujú okolnosti každého jednotlivého prípadu a prinajmenšom náležite zohľadňujú:

a) závažnosť porušenia a dôležitosť porušených ustanovení, pričom za závažné porušenie sa okrem iného považujú v každom prípade tieto porušenia:

   i) opakované porušenia;

   ii) neoznámenie významných incidentov alebo nevykonanie ich nápravy;

   iii) nevykonanie nápravy nedostatkov po prijatí záväzných pokynov príslušných orgánov;

   iv) marenie auditov alebo monitorovacích činností nariadených príslušným orgánom na základe zistenia porušenia;

   v) poskytovanie nepravdivých alebo hrubo nepresných informácií týkajúcich sa opatrení na riadenie kybernetických rizík alebo oznamovacích povinností stanovených v článkoch 21 a 23;

b) dĺžku trvania porušenia;

c) akékoľvek relevantné predchádzajúce prípady porušenia dotknutého subjektu;

d) akúkoľvek spôsobenú majetkovú alebo nemajetkovú ujmu vrátane finančných alebo hospodárskych strát, účinkov na iné služby a počtu dotknutých používateľov;

e) akýkoľvek úmysel alebo nedbanlivosť páchateľa porušenia;

f) akékoľvek opatrenia, ktoré subjekt prijal na zabránenie alebo zmiernenie majetkovej alebo nemajetkovej ujmy;

g) akékoľvek dodržiavanie schválených kódexov správania alebo schválených mechanizmov certifikácie;

h) úrovne spolupráce zodpovednej fyzickej alebo právnickej osoby s príslušným orgánom.

8. Príslušné orgány uvedú podrobné odôvodnenie svojich opatrení na presadzovanie práva. Príslušné orgány pred prijatím takýchto opatrení oznámia dotknutým subjektom svoje predbežné zistenia. Takisto poskytnú týmto subjektom primeraný čas na predloženie pripomienok, s výnimkou riadne odôvodnených prípadov, ak by to bránilo prijatiu okamžitých opatrení na predchádzanie incidentom alebo reakciu na ne.

9. Členské štáty zabezpečia, aby ich príslušné orgány podľa tejto smernice informovali relevantné príslušné orgány v tom istom členskom štáte podľa smernice (EÚ) 2022/2557 vtedy, keď vykonávajú svoje právomoci v oblasti dohľadu a presadzovania práva, ktorých cieľom je zabezpečiť, aby subjekt identifikovaný ako kritický subjekt podľa smernice (EÚ) 2022/2557 dodržiaval túto smernicu. Príslušné orgány podľa smernice (EÚ) 2022/2557 môžu v náležitých prípadoch požiadať príslušné orgány podľa tejto smernice o vykonanie ich právomocí dohľadu a presadzovania práva vo vzťahu k subjektu, ktorý je identifikovaný ako kritický subjekt podľa smernice (EÚ) 2022/2557.

10. Členské štáty zabezpečia, aby ich príslušné orgány podľa tejto smernice spolupracovali s relevantnými príslušnými orgánmi dotknutého členského štátu podľa nariadenia (EÚ) 2022/2554. Členské štáty najmä zabezpečia, aby ich príslušné orgány podľa tejto smernice informovali fórum pre dozor zriadený podľa článku 32 ods. 1 nariadenia (EÚ) 2022/2554 pri vykonávaní svojich právomocí dohľadu a presadzovania práva, ktorých cieľom je zabezpečiť, aby kľúčový subjekt, ktorý je identifikovaný ako externý poskytovateľ kritických IKT služieb podľa článku 31 nariadenia (EÚ) 2022/2554, dodržiaval túto smernicu.

Článok 33

Opatrenia dohľadu a presadzovania práva týkajúce sa dôležitých subjektov

1. Ak členské štáty získajú dôkaz, indíciu alebo informáciu, že dôležitý subjekt údajne nedodržiava túto smernicu, a najmä jej články 21 a 23, zabezpečia, aby príslušné orgány konali v prípade potreby prostredníctvom *ex post* opatrení v oblasti dohľadu. Členské štáty zabezpečia, aby tieto opatrenia boli účinné, primerané a odrádzajúce, pričom zohľadnia okolnosti každého jednotlivého prípadu.

2. Členské štáty zabezpečia, aby príslušné orgány pri vykonávaní svojich úloh dohľadu nad dôležitými subjektmi mali právomoc podrobiť tieto subjekty prinajmenšom:

a) inšpekciám na mieste a *ex post* dohľadu na diaľku, ktoré vykonávajú vyškolení odborníci;

b) cieleným bezpečnostným auditom, ktoré vykonáva nezávislý orgán alebo príslušný orgán;

c) bezpečnostným kontrolám založeným na objektívnych, nediskriminačných, spravodlivých a transparentných kritériách posudzovania rizík, v prípade potreby v spolupráci s dotknutým subjektom;

d) žiadostiam o informácie potrebné na *ex post* posúdenie opatrení na riadenie kybernetických rizík, ktoré dotknutý subjekt prijal, vrátane zdokumentovaných politík kybernetickej bezpečnosti, ako aj dodržiavania povinnosti predkladať informácie príslušným orgánom podľa článku 27;

e) žiadostiam o prístup k údajom, dokumentom a informáciám potrebným na plnenie ich úloh dohľadu;

f) žiadostiam o dôkazy vykonávania politík kybernetickej bezpečnosti, ako sú výsledky bezpečnostných auditov uskutočnených kvalifikovaným audítorom a príslušné podkladové dôkazy.

Cielené bezpečnostné audity uvedené v prvom pododseku písm. b) sú založené na posúdení rizík, ktoré vykonal príslušný orgán alebo auditovaný subjekt, alebo na iných dostupných informáciách týkajúcich sa rizík.

Výsledky každého cieleného bezpečnostného auditu sa sprístupnia príslušnému orgánu. Náklady na takýto cielený bezpečnostný audit, ktorý vykonáva nezávislý orgán, hradí auditovaný subjekt, s výnimkou riadne odôvodnených prípadov, keď príslušný orgán rozhodne inak.

3. Príslušné orgány pri vykonávaní svojich právomocí podľa odseku 2 písm. d), e) alebo f) uvedú účel žiadosti a konkretizujú požadované informácie.

4. Členské štáty zabezpečia, aby príslušné orgány pri vykonávaní svojich právomocí presadzovania práva v súvislosti s dôležitými subjektmi mali právomoc prinajmenšom:

a) vydávať varovania o porušeniach tejto smernice dotknutými subjektmi;

b) prijímať záväzné pokyny alebo príkaz, ktorým sa od dotknutých subjektov vyžaduje napraviť zistené nedostatky alebo porušenie tejto smernice;

c) nariadiť dotknutým subjektom, aby upustili od konania, ktoré porušuje túto smernicu, a neopakovali takéto konanie;

d) nariadiť dotknutým subjektom, aby určeným spôsobom a v určenej lehote zabezpečili zosúladenie svojich opatrení na riadenie kybernetických rizík s článkom 21 alebo splnili oznamovacie povinnosti stanovené v článku 23;

e) nariadiť dotknutým subjektom, aby informovali fyzické alebo právnické osoby, v súvislosti s ktorými poskytujú služby alebo vykonávajú činnosti, ktoré sú potenciálne zasiahnuté významnou kybernetickou hrozbou, o povahe hrozby, ako aj o akýchkoľvek možných ochranných alebo nápravných opatreniach, ktoré môžu tieto fyzické alebo právnické osoby prijať v reakcii na túto hrozbu;

f) nariadiť dotknutým subjektom, aby v primeranej lehote vykonali odporúčania vydané na základe bezpečnostného auditu;

g) nariadiť dotknutým subjektom, aby určeným spôsobom zverejnili aspekty porušovania tejto smernice;

h) uložiť správnu pokutu podľa článku 34 alebo požiadať o jej uloženie príslušné orgány, súdy alebo tribunály v súlade s vnútroštátnym právom, a to popri ktoromkoľvek z opatrení uvedených v písmenách a) až g) tohto odseku.

5. *Článok 32* ods. 6, 7 a 8 sa uplatňuje *mutatis mutandis* na opatrenia dohľadu a presadzovania práva stanovené v tomto článku v súvislosti s dôležitými subjektmi.

6. Členské štáty zabezpečia, aby ich príslušné orgány podľa tejto smernice spolupracovali s relevantnými príslušnými orgánmi dotknutého členského štátu podľa nariadenia (EÚ) 2022/2554. Členské štáty najmä zabezpečia, aby ich príslušné orgány podľa tejto smernice informovali fórum pre dozor zriadený podľa článku 32 ods. 1 nariadenia (EÚ) 2022/2554 pri vykonávaní svojich právomocí dohľadu a presadzovania práva, ktorých cieľom je zabezpečiť, aby dôležitý subjekt, ktorý je identifikovaný ako externý poskytovateľ kritických IKT služieb podľa článku 31 nariadenia (EÚ) 2022/2554, dodržiaval túto smernicu.

Článok 34

Všeobecné podmienky ukladania správnych pokút kľúčovým a dôležitým subjektom

1. Členské štáty zabezpečia, aby správne pokuty uložené kľúčovým a dôležitým subjektom podľa tohto článku v súvislosti s porušeniami tejto smernice boli účinné, primerané a odrádzajúce a zároveň zohľadňovali okolnosti každého jednotlivého prípadu.

2. Správne pokuty sa ukladajú navyše ku ktorémukoľvek z opatrení uvedených v článku 32 ods. 4 písm. a) až h), článku 32 ods. 5 a článku 33 ods. 4 písm. a) až g).

3. Pri rozhodovaní o uložení správnej pokuty, ako aj pri rozhodovaní o jej výške v každom jednotlivom prípade sa náležite zohľadnia aspoň prvky stanovené v článku 32 ods. 7.

4. Členské štáty zabezpečia, aby kľúčovým subjektom v prípade porušenia článku 21 alebo 23 boli v súlade s odsekmi 2 a 3 tohto článku uložené správne pokuty v maximálnej výške aspoň 10 000 000 EUR alebo v maximálnej výške aspoň 2 % celkového celosvetového ročného obratu v predchádzajúcom finančnom roku podniku, ku ktorému kľúčový subjekt patrí, podľa toho, ktorá suma je vyššia.

5. Členské štáty zabezpečia, aby dôležitým subjektom v prípade porušenia článku 21 alebo 23 boli v súlade s odsekmi 2 a 3 tohto článku uložené správne pokuty v maximálnej výške aspoň 7 000 000 EUR alebo v maximálnej výške aspoň 1,4 % celkového celosvetového ročného obratu v predchádzajúcom finančnom roku podniku, ku ktorému dôležitý subjekt patrí, podľa toho, ktorá suma je vyššia.

6. Členské štáty môžu stanoviť právomoc ukladať pravidelné penále s cieľom prinútiť kľúčový alebo dôležitý subjekt, aby prestal porušovať túto smernicu v súlade s predchádzajúcim rozhodnutím príslušného orgánu.

7. Bez toho, aby boli dotknuté právomoci príslušných orgánov podľa článkov 32 a 33, každý členský štát môže stanoviť pravidlá, či a v akom rozsahu sa správne pokuty môžu uložiť subjektom verejnej správy.

8. Ak sa v právnom systéme členského štátu nestanovujú správne pokuty, uvedený členský štát zabezpečí, aby sa tento článok uplatňoval tak, že uloženie pokuty iniciuje príslušný orgán a uložia ju príslušné vnútroštátne súdy alebo tribunály, pričom sa zabezpečí, aby tieto právne prostriedky nápravy boli účinné a mali rovnocenný účinok ako správne pokuty ukladané príslušnými orgánmi. Ukladané pokuty musia byť v každom prípade účinné, primerané a odrádzajúce. Členský štát oznámi Komisii ustanovenia právnych predpisov, ktoré prijíma podľa tohto odseku, do 17. októbra 2024 a bezodkladne všetky následné pozmeňujúce právne predpisy či zmeny, ktoré sa ich týkajú.

Článok 35

Porušenia povinností, pri ktorých došlo k porušeniu ochrany osobných údajov

1. Ak príslušné orgány počas výkonu dohľadu alebo presadzovania práva zistia, že porušenie povinností stanovených v článkoch 21 a 23 tejto smernice kľúčovým alebo dôležitým subjektom môže mať za následok porušenie ochrany osobných údajov, ako je vymedzené v článku 4 bode 12 nariadenia (EÚ) 2016/679, pričom takéto porušenie sa oznamuje podľa článku 33 uvedeného nariadenia, bez zbytočného odkladu o tom informujú orgány dohľadu podľa článku 55 alebo 56 uvedeného nariadenia.

2. Ak orgány dohľadu uvedené v článku 55 alebo 56 nariadenia (EÚ) 2016/679 uložia správnu pokutu podľa článku 58 ods. 2 písm. i) uvedeného nariadenia, príslušné orgány neuložia správnu pokutu podľa článku 34 tejto smernice za porušenie uvedené v odseku 1 tohto článku spôsobené rovnakým konaním, ktoré bolo dôvodom správnej pokuty podľa článku 58 ods. 2 písm. i) nariadenia (EÚ) 2016/679. Príslušné orgány však môžu uložiť opatrenia na presadzovanie práva stanovené v článku 32 ods. 4 písm. a) až h), v článku 32 ods. 5 a v článku 33 ods. 4 písm. a) až g) tejto smernice.

3. Ak je orgán dohľadu, príslušný podľa nariadenia (EÚ) 2016/679, usadený v inom členskom štáte než príslušný orgán, príslušný orgán informuje orgán dohľadu so sídlom v jeho vlastnom členskom štáte o možnom porušení ochrany údajov podľa odseku 1.

Článok 36

Sankcie

Členské štáty stanovia pravidlá, pokiaľ ide o sankcie uplatniteľné pri porušení vnútroštátnych opatrení prijatých podľa tejto smernice, a prijmú všetky opatrenia potrebné na zabezpečenie ich uplatňovania. Stanovené sankcie musia byť účinné, primerané a odrádzajúce. Členské štáty o týchto pravidlách a opatreniach do 17. januára 2025 informujú Komisiu a bezodkladne jej oznámia každú nasledujúcu zmenu, ktorá ich ovplyvní.

Článok 37

Vzájomná pomoc

1. Ak subjekt poskytuje služby vo viac ako jednom členskom štáte alebo poskytuje služby v jednom alebo viacerých členských štátoch a jeho siete a informačné systémy sú umiestnené v niektorom inom alebo vo viacerých iných členských štátoch, príslušné orgány dotknutých členských štátov spolupracujú a v prípade potreby si navzájom pomáhajú. Táto spolupráca zahŕňa aspoň tieto prvky:

a) príslušné orgány, ktoré uplatňujú opatrenia dohľadu alebo presadzovania práva v členskom štáte, informujú prostredníctvom jednotného kontaktného miesta príslušné orgány v ostatných dotknutých členských štátoch a konzultujú s nimi prijaté opatrenia dohľadu a presadzovania práva;

b) príslušný orgán môže požiadať iný príslušný orgán, aby prijal opatrenia dohľadu alebo presadzovania práva;

c) príslušný orgán po prijatí odôvodnenej žiadosti od iného príslušného orgánu poskytne tomuto inému príslušnému orgánu vzájomnú pomoc primeranú jeho vlastným zdrojom, aby sa opatrenia dohľadu alebo presadzovania práva mohli vykonávať účinne, efektívne a konzistentne.

Vzájomná pomoc uvedená v prvom pododseku písm. c) sa môže vzťahovať na žiadosti o informácie a na opatrenia v oblasti dohľadu vrátane žiadostí o vykonanie inšpekcií na mieste alebo dohľadu na diaľku, alebo cielených bezpečnostných auditov. Príslušný orgán, ktorému je adresovaná žiadosť o pomoc, túto žiadosť neodmietne, pokiaľ sa nepreukáže, že nemá právomoc poskytnúť požadovanú pomoc, že požadovaná pomoc nie je primeraná úlohám príslušného orgánu v oblasti dohľadu, alebo že sa žiadosť týka informácií alebo zahŕňa činnosti, ktoré by v prípade zverejnenia alebo vykonania boli v rozpore so základnými záujmami členských štátov v oblasti národnej bezpečnosti, verejnej bezpečnosti alebo obrany. Príslušný orgán pred zamietnutím takejto žiadosti konzultuje s ostatnými dotknutými príslušnými orgánmi a v prípade, že o to jeden z dotknutých členských štátov požiada, aj s Komisiou a agentúrou ENISA.

2. V prípade potreby a po vzájomnej dohode môžu príslušné orgány z rôznych členských štátov vykonávať spoločné opatrenia v oblasti dohľadu.

KAPITOLA VIII

DELEGOVANÉ A VYKONÁVACIE AKTY

Článok 38

Vykonávanie delegovania právomoci

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

2. Právomoc prijímať delegované akty uvedené v článku 24 ods. 2 sa Komisii udeľuje na obdobie piatich rokov od 16. januára 2023.

3. Delegovanie právomoci uvedené v článku 24 ods. 2 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 expertami 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 24 ods. 2 nadobudne účinnosť, len ak Európsky parlament alebo Rada voči nemu nevzniesli námietku v lehote dvoch mesiacov odo dňa oznámenia uvedeného aktu Európskemu parlamentu a Rade alebo ak pred uplynutím uvedenej lehoty Európsky parlament a Rada informovali Komisiu o svojom rozhodnutí nevzniesť námietku. Na podnet Európskeho parlamentu alebo Rady sa táto lehota predĺži o dva mesiace.

Článok 39

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, uvedený postup sa ukončí bez výsledku, ak tak v rámci lehoty na vydanie stanoviska rozhodne predseda výboru alebo ak o to požiada člen výboru.

KAPITOLA IX

ZÁVEREČNÉ USTANOVENIA

Článok 40

Preskúmanie

Komisia do 17. októbra 2027 a následne každých 36 mesiacov preskúma fungovanie tejto smernice a podá o tom správu Európskemu parlamentu a Rade. V správe sa posúdi najmä relevantnosť veľkosti dotknutých subjektov a odvetví, pododvetví a typov subjektu uvedených v prílohách I a II pre fungovanie hospodárstva a spoločnosti v súvislosti s kybernetickou bezpečnosťou. Na tento účel a s cieľom ďalej napredovať v strategickej a operačnej spolupráci Komisia zohľadní správy skupiny pre spoluprácu a siete jednotiek CSIRT o skúsenostiach získaných na strategickej a operačnej úrovni. K správe sa podľa potreby pripojí legislatívny návrh.

Článok 41

Transpozícia

1. Členské štáty prijmú a uverejnia do 17. októbra 2024 opatrenia potrebné na dosiahnutie súladu s touto smernicou. Bezodkladne o tom informujú Komisiu.

Tieto opatrenia sa uplatňujú od 18. októbra 2024.

2. Členské štáty uvedú priamo v prijatých opatreniach uvedených v odseku 1 alebo pri ich úradnom uverejnení odkaz na túto smernicu. Podrobnosti o odkaze upravia členské štáty.

Článok 42

Zmena nariadenia (EÚ) č. 910/2014

V nariadení (EÚ) č. 910/2014 sa vypúšťa článok 19 s účinnosťou od 18. októbra 2024.

Článok 43

Zmena smernice (EÚ) 2018/1972

V smernici (EÚ) 2018/1972 sa vypúšťajú články 40 a 41 s účinnosťou od 18. októbra 2024.

Článok 44

Zrušenie

Smernica (EÚ) 2016/1148 sa zrušuje s účinnosťou od 18. októbra 2024.

Odkazy na zrušenú smernicu sa považujú za odkazy na túto smernicu a znejú v súlade s tabuľkou zhody uvedenou v prílohe III.

Článok 45

Nadobudnutie účinnosti

Táto smernica nadobúda účinnosť dvadsiatym dňom nasledujúcim po jej uverejnení v *Úradnom vestníku Európskej únie*.

Článok 46

Adresáti

Táto smernica je určená členským štátom.

V Štrasburgu 14. decembra 2022

Za Európsky parlament	*Za Radu*
predsedníčka	*predseda*
R. METSOLA	M. BEK

PRÍLOHA I

ODVETVIA S VYSOKOU ÚROVŇOU KRITICKOSTI

Odvetvie	Pododvetvie	Typ subjektu
1. Energetika	a) elektrická energia	— elektroenergetické podniky, ako sú vymedzené v článku 2 bode 57 smernice Európskeho parlamentu a Rady (EÚ) 2019/944 ([1]), ktoré vykonávajú funkciu „dodávky“, ako je vymedzená v článku 2 bode 12 uvedenej smernice
		— prevádzkovatelia distribučnej sústavy, ako sú vymedzení v článku 2 bode 29 smernice (EÚ) 2019/944
		— prevádzkovatelia prenosovej sústavy, ako sú vymedzení v článku 2 bode 35 smernice (EÚ) 2019/944
		— výrobcovia, ako sú vymedzení v článku 2 bode 38 smernice (EÚ) 2019/944
		— nominovaní organizátori trhu s elektrinou, ako sú vymedzení v článku 2 bode 8 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/943 ([2]) — účastníci trhu, ako sú vymedzení v článku 2 bode 25 nariadenia (EÚ) 2019/943, ktorí poskytujú služby agregácie, riadenia odberu alebo uskladňovania energie, ako sú vymedzené v článku 2 bodoch 18, 20 a 59 smernice (EÚ) 2019/944 — prevádzkovatelia nabíjacieho bodu, ktorí sú zodpovední za správu a prevádzku nabíjacieho bodu, ktorý koncovým používateľom poskytuje nabíjaciu službu, a to aj v mene a na účet poskytovateľa služieb mobility
	b) diaľkové vykurovanie a chladenie	— prevádzkovatelia diaľkového vykurovania alebo diaľkového chladenia, ako sú vymedzení v článku 2 bode 19 smernice Európskeho parlamentu a Rady (EÚ) 2018/2001 ([3])
	c) ropa	— prevádzkovatelia ropovodov
		— prevádzkovatelia zariadení na ťažbu, rafinovanie a spracovanie ropy, jej skladovanie a prepravu
		— ústredné subjekty správy zásob, ako sú vymedzené v článku 2 písm. f) smernice Rady 2009/119/ES ([4])
	d) plyn	— dodávateľské podniky, ako sú vymedzené v článku 2 bode 8 smernice Európskeho parlamentu a Rady 2009/73/ES ([5])
		— prevádzkovatelia distribučnej siete, ako sú vymedzení v článku 2 bode 6 smernice 2009/73/ES
		— prevádzkovatelia prepravnej siete, ako sú vymedzení v článku 2 bode 4 smernice 2009/73/ES
		— prevádzkovatelia zásobníkov, ako sú vymedzení v článku 2 bode 10 smernice 2009/73/ES
		— prevádzkovatelia zariadení LNG, ako sú vymedzení v článku 2 bode 12 smernice 2009/73/ES
		— plynárenské podniky, ako sú vymedzené v článku 2 bode 1 smernice 2009/73/ES
		— prevádzkovatelia zariadení na rafinovanie a spracovanie zemného plynu
	e) vodík	— prevádzkovatelia zariadení na výrobu, skladovanie a prepravu vodíka

Odvetvie	Pododvetvie	Typ subjektu
2. Doprava	a) letecká doprava	— leteckí dopravcovia, ako sú vymedzení v článku 3 bode 4 nariadenia (ES) č. 300/2008, využívaní na komerčné účely
		— riadiace orgány letiska, ako sú vymedzené v článku 2 bode 2 smernice Európskeho parlamentu a Rady 2009/12/ES ([6]), letiská, ako sú vymedzené v článku 2 bode 1 uvedenej smernice, vrátane hlavných letísk uvedených v oddiele 2 prílohy II k nariadeniu Európskeho parlamentu a Rady (EÚ) č. 1315/2013 ([7]), a subjekty prevádzkujúce pomocné zariadenia nachádzajúce sa na letiskách
		— prevádzkovatelia kontroly riadenia dopravy poskytujúci služby riadenia letovej prevádzky (ATC), ako sú vymedzení v článku 2 bode 1 nariadenia Európskeho parlamentu a Rady (ES) č. 549/2004 ([8])
	b) železničná doprava	— manažéri infraštruktúry, ako sú vymedzení v článku 3 bode 2 smernice Európskeho parlamentu a Rady 2012/34/EÚ ([9])
		— železničné podniky, ako sú vymedzené v článku 3 bode 1 smernice 2012/34/EÚ, vrátane prevádzkovateľov servisných zariadení, ako sú vymedzené v článku 3 bode 12 uvedenej smernice
	c) vodná doprava	— spoločnosti prevádzkujúce vnútrozemskú, námornú a pobrežnú osobnú a nákladnú vodnú dopravu, ako sú vymedzené pre námornú dopravu v prílohe I k nariadeniu Európskeho parlamentu a Rady (ES) č. 725/2004 ([10]), bez jednotlivých plavidiel, ktoré tieto spoločnosti prevádzkujú
		— riadiace orgány prístavov, ako sú vymedzené v článku 3 bode 1 smernice Európskeho parlamentu a Rady 2005/65/ES ([11]), vrátane ich prístavných zariadení, ako sú vymedzené v článku 2 bode 11 nariadenia (ES) č. 725/2004, a subjekty prevádzkujúce činnosti a zariadenia v rámci prístavu
		— prevádzkovatelia plavebno-prevádzkových služieb (VTS), ako sú vymedzené v článku 3 písm. o) smernice Európskeho parlamentu a Rady 2002/59/ES ([12])
	d) cestná doprava	— cestné orgány, ako sú vymedzené v článku 2 bode 12 delegovaného nariadenia Komisie (EÚ) 2015/962 ([13]), zodpovedné za kontrolu riadenia dopravy, s výnimkou verejných subjektov, v prípade ktorých je riadenie dopravy alebo prevádzkovanie inteligentných dopravných systémov nepodstatnou súčasťou ich celkovej činnosti
		— prevádzkovatelia inteligentných dopravných systémov, ako sú vymedzené v článku 4 bode 1 smernice Európskeho parlamentu a Rady 2010/40/EÚ ([14])
3. Bankovníctvo		úverové inštitúcie, ako sú vymedzené v článku 4 bode 1 nariadenia Európskeho parlamentu a Rady (EÚ) č. 575/2013 ([15])
4. Infraštruktúra finančných trhov		— prevádzkovatelia obchodných miest, ako sú vymedzení v článku 4 bode 24 smernice Európskeho parlamentu a Rady 2014/65/EÚ ([16])
		— centrálne protistrany (CCP), ako sú vymedzené v článku 2 bode 1 nariadenia Európskeho parlamentu a Rady (EÚ) č. 648/2012 ([17])

Odvetvie	Pododvetvie	Typ subjektu
5. Zdravotníctvo		— poskytovatelia zdravotnej starostlivosti, ako sú vymedzení v článku 3 písm. g) smernice Európskeho parlamentu a Rady 2011/24/EÚ ([18])
		— referenčné laboratóriá EÚ uvedené v článku 15 nariadenia Európskeho parlamentu a Rady (EÚ) .../... ([19])
		— subjekty vykonávajúce činnosti vo výskume a vývoji liekov, ako sú vymedzené v článku 1 bode 2 smernice Európskeho parlamentu a Rady 2001/83/ES ([20]) — subjekty vyrábajúce základné farmaceutické výrobky a farmaceutické prípravky uvedené v sekcii C divízii 21 NACE Rev. 2 — subjekty vyrábajúce zdravotnícke pomôcky považované za kritické v núdzovej situácii v oblasti verejného zdravia (ďalej len „zoznam kritických pomôcok v núdzovej situácii v oblasti verejného zdravia“) v zmysle článku 22 nariadenia Európskeho parlamentu a Rady (EÚ) 2022/123 ([21])
6. Pitná voda		dodávatelia a distribútori vody určenej na ľudskú spotrebu, ako je vymedzená v článku 2 bode 1 písm. a) smernice Európskeho parlamentu a Rady (EÚ) 2020/2184 ([22]), s výnimkou distribútorov, pre ktorých je distribúcia vody určenej na ľudskú spotrebu nepodstatnou súčasťou ich celkovej činnosti v oblasti distribúcie iných komodít a tovaru
7. Odpadová voda		podniky zaoberajúce sa zberom, likvidáciou alebo úpravou komunálnych odpadových vôd, odpadových vôd z domácností alebo priemyselných odpadových vôd, ako sú vymedzené v článku 2 bodoch 1, 2 a 3 smernice Rady 91/271/EHS ([23]), s výnimkou podnikov, pre ktoré je zber, likvidácia alebo úprava komunálnych odpadových vôd, odpadových vôd z domácností alebo priemyselných odpadových vôd nepodstatnou súčasťou ich celkovej činnosti
8. Digitálna infraštruktúra		— poskytovatelia internetových prepojovacích uzlov
		— poskytovatelia služieb DNS, s výnimkou prevádzkovateľov koreňových názvových serverov
		— správcovia názvov TLD
		— poskytovatelia služieb cloud computingu
		— poskytovatelia služieb dátového centra
		— poskytovatelia sietí na sprístupňovanie obsahu
		— poskytovatelia dôveryhodných služieb
		— poskytovatelia verejných elektronických komunikačných sietí
		— poskytovatelia verejne dostupných elektronických komunikačných služieb
9. Riadenie služieb IKT (medzi podnikmi)		— poskytovatelia riadených služieb — poskytovatelia riadených bezpečnostných služieb

Odvetvie	Pododvetvie	Typ subjektu
10. Verejná správa		— subjekty verejnej správy na úrovni ústrednej štátnej správy, ako ich vymedzuje členský štát v súlade s vnútroštátnym právom
		— subjekty verejnej správy na regionálnej úrovni, ako ich vymedzuje členský štát v súlade s vnútroštátnym právom
11. Vesmír		prevádzkovatelia pozemnej infraštruktúry, ktorú vlastnia, riadia a prevádzkujú členské štáty alebo súkromné subjekty, ktorí prispievajú k poskytovaniu vesmírnych služieb, s výnimkou poskytovateľov verejných elektronických komunikačných sietí

([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).
([2]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/943 z 5. júna 2019 o vnútornom trhu s elektrinou (Ú. v. EÚ L 158, 14.6.2019, s. 54).
([3]) Smernica Európskeho parlamentu a Rady (EÚ) 2018/2001 z 11. decembra 2018 o podpore využívania energie z obnoviteľných zdrojov (Ú. v. EÚ L 328, 21.12.2018, s. 82).
([4]) Smernica Rady 2009/119/ES zo 14. septembra 2009, ktorou sa členským štátom ukladá povinnosť udržiavať minimálne zásoby ropy a/alebo ropných výrobkov (Ú. v. EÚ L 265, 9.10.2009, s. 9).
([5]) Smernica Európskeho parlamentu a Rady 2009/73/ES z 13. júla 2009 o spoločných pravidlách pre vnútorný trh so zemným plynom, ktorou sa zrušuje smernica 2003/55/ES (Ú. v. EÚ L 211, 14.8.2009, s. 94).
([6]) Smernica Európskeho parlamentu a Rady 2009/12/ES z 11. marca 2009 o letiskových poplatkoch (Ú. v. EÚ L 70, 14.3.2009, s. 11).
([7]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1315/2013 z 11. decembra 2013 o usmerneniach Únie pre rozvoj transeurópskej dopravnej siete a o zrušení rozhodnutia č. 661/2010/EÚ (Ú. v. EÚ L 348, 20.12.2013, s. 1).
([8]) Nariadenie Európskeho parlamentu a Rady (ES) č. 549/2004 z 10. marca 2004, ktorým sa stanovuje rámec na vytvorenie jednotného európskeho neba (rámcové nariadenie) (Ú. v. EÚ L 96, 31.3.2004, s. 1).
([9]) Smernica Európskeho parlamentu a Rady 2012/34/EÚ z 21. novembra 2012, ktorou sa zriaďuje jednotný európsky železničný priestor (Ú. v. EÚ L 343, 14.12.2012, s. 32).
([10]) Nariadenie Európskeho parlamentu a Rady (ES) č. 725/2004 z 31. marca 2004 o zvýšení bezpečnosti lodí a prístavných zariadení (Ú. v. EÚ L 129, 29.4.2004, s. 6).
([11]) Smernica Európskeho parlamentu a Rady 2005/65/ES z 26. októbra 2005 o zvýšení bezpečnosti prístavov (Ú. v. EÚ L 310, 25.11.2005, s. 28).
([12]) Smernica Európskeho parlamentu a Rady 2002/59/ES z 27. júna 2002, ktorou sa zriaďuje monitorovací a informačný systém spoločenstva pre lodnú dopravu a ktorou sa zrušuje smernica Rady 93/75/EHS (Ú. v. ES L 208, 5.8.2002, s. 10).
([13]) Delegované nariadenie Komisie (EÚ) 2015/962 z 18. decembra 2014, ktorým sa dopĺňa smernica Európskeho parlamentu a Rady 2010/40/EÚ, pokiaľ ide o poskytovanie informačných služieb o doprave v reálnom čase v celej EÚ (Ú. v. EÚ L 157, 23.6.2015, s. 21).
([14]) Smernica Európskeho parlamentu a Rady 2010/40/EÚ zo 7. júla 2010 o rámci na zavedenie inteligentných dopravných systémov v oblasti cestnej dopravy a na rozhrania s inými druhmi dopravy (Ú. v. EÚ L 207, 6.8.2010, s. 1).
([15]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 575/2013 z 26. júna 2013 o prudenciálnych požiadavkách na úverové inštitúcie a o zmene nariadenia (EÚ) č. 648/2012 (Ú. v. EÚ L 176, 27.6.2013, s. 1).
([16]) Smernica Európskeho parlamentu a Rady 2014/65/EÚ z 15. mája 2014 o trhoch s finančnými nástrojmi, ktorou sa mení smernica 2002/92/ES a smernica 2011/61/EÚ (Ú. v. EÚ L 173, 12.6.2014, s. 349).
([17]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 zo 4. júla 2012 o mimoburzových derivátoch, centrálnych protistranách a archívoch obchodných údajov (Ú. v. EÚ L 201, 27.7.2012, s. 1).
([18]) Smernica Európskeho parlamentu a Rady 2011/24/EÚ z 9. marca 2011 o uplatňovaní práv pacientov pri cezhraničnej zdravotnej starostlivosti (Ú. v. EÚ L 88, 4.4.2011, s. 45).

([19]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2371 z 23. novembra 2022 o závažných cezhraničných ohrozeniach zdravia, ktorým sa zrušuje rozhodnutie č. 1082/2013/EÚ (Ú. v. EÚ L 314, 6.12.2022, s. 26).

([20]) Smernica Európskeho parlamentu a Rady 2001/83/ES zo 6. novembra 2001, ktorou sa ustanovuje zákonník spoločenstva o humánnych liekoch (Ú. v. ES L 311, 28.11.2001, s. 67).

([21]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/123 z 25. januára 2022 o posilnenej úlohe Európskej agentúry pre lieky z hľadiska pripravenosti na krízy a krízového riadenia v oblasti liekov a zdravotníckych pomôcok (Ú. v. EÚ L 20, 31.1.2022, s. 1).

([22]) Smernica Európskeho parlamentu a Rady (EÚ) 2020/2184 zo 16. decembra 2020 o kvalite vody určenej na ľudskú spotrebu (Ú. v. EÚ L 435, 23.12.2020, s. 1).

([23]) Smernica Rady 91/271/EHS z 21. mája 1991 o čistení komunálnych odpadových vôd (Ú. v. ES L 135, 30.5.1991, s. 40).

PRÍLOHA II

INÉ KRITICKÉ ODVETVIA

Odvetvie	Pododvetvie	Typ subjektu
1. Poštové a kuriérske služby		poskytovatelia poštových služieb, ako sú vymedzení v článku 2 bode 1a smernice 97/67/ES, vrátane poskytovateľov kuriérskych služieb
2. Odpadové hospodárstvo		podniky vykonávajúce činnosti nakladania s odpadom, ako je vymedzené v článku 3 bodu 9 smernice Európskeho parlamentu a Rady 2008/98/ES ([1]), s výnimkou podnikov, pre ktoré nakladanie s odpadom nepredstavuje hlavnú hospodársku činnosť
3. Výroba a distribúcia chemických látok		podniky vyrábajúce látky a distribuujúce látky alebo zmesi, ako je uvedené v článku 3 bodoch 9 a 14 nariadenia Európskeho parlamentu a Rady (ES) č. 1907/2006 ([2]), a podniky vyrábajúce výrobky, ako sú vymedzené v článku 3 bode 3 uvedeného nariadenia, z látok a zmesí
4. Výroba, spracovanie a distribúcia potravín		potravinárske podniky, ako sú vymedzené v článku 3 bode 2 nariadenia Európskeho parlamentu a Rady (ES) č. 178/2002 ([3]), ktoré sa zaoberajú veľkoobchodnou distribúciou a priemyselnou výrobou a spracovaním
5. Výroba	a) výroba zdravotníckych pomôcok a diagnostických zdravotníckych pomôcok *in vitro*	subjekty vyrábajúce zdravotnícke pomôcky, ako sú vymedzené v článku 2 bode 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2017/745 ([4]), a subjekty vyrábajúce diagnostické zdravotnícke pomôcky in vitro, ako sú vymedzené v článku 2 bode 2 nariadenia Európskeho parlamentu a Rady (EÚ) 2017/746 ([5]), s výnimkou subjektov vyrábajúcich zdravotnícke pomôcky uvedených v piatej zarážke bodu 5 prílohy I tejto smernice
	b) výroba počítačových, elektronických a optických výrobkov	subjekty vykonávajúce akúkoľvek hospodársku činnosť uvedenú v sekcii C divízii 26 NACE Rev. 2
	c) výroba elektrických zariadení	subjekty vykonávajúce akúkoľvek hospodársku činnosť uvedenú v sekcii C divízii 27 NACE Rev. 2
	d) výroba strojov a zariadení i. n.	subjekty vykonávajúce akúkoľvek hospodársku činnosť uvedenú v sekcii C divízii 28 NACE Rev. 2
	e) výroba motorových vozidiel, návesov a prívesov	subjekty vykonávajúce akúkoľvek hospodársku činnosť uvedenú v sekcii C divízii 29 NACE Rev. 2
	f) výroba ostatných dopravných prostriedkov	subjekty vykonávajúce akúkoľvek hospodársku činnosť uvedenú v sekcii C divízii 30 NACE Rev. 2

Odvetvie	Pododvetvie	Typ subjektu
6. Poskytovatelia digitálnych služieb		— poskytovatelia online trhov
		— poskytovatelia internetových vyhľadávačov
		— poskytovatelia platforiem služieb sociálnej siete
7. Výskum		výskumné organizácie

([1]) Smernica Európskeho parlamentu a Rady 2008/98/ES z 19. novembra 2008 o odpade a o zrušení určitých smerníc (Ú. v. EÚ L 312, 22.11.2008, s. 3).

([2]) Nariadenie Európskeho parlamentu a Rady (ES) č. 1907/2006 z 18. decembra 2006 o registrácii, hodnotení, autorizácii a obmedzovaní chemikálií (REACH) a o zriadení Európskej chemickej agentúry, o zmene a doplnení smernice 1999/45/ES a o zrušení nariadenia Rady (EHS) č. 793/93 a nariadenia Komisie (ES) č. 1488/94, smernice Rady 76/769/EHS a smerníc Komisie 91/155/EHS, 93/67/EHS, 93/105/ES a 2000/21/ES (Ú. v. EÚ L 396, 30.12.2006, s. 1).

([3]) Nariadenie Európskeho parlamentu a Rady (ES) č. 178/2002 z 28. januára 2002, ktorým sa ustanovujú všeobecné zásady a požiadavky potravinového práva, zriaďuje Európsky úrad pre bezpečnosť potravín a stanovujú postupy v záležitostiach bezpečnosti potravín (Ú. v. ES L 31, 1.2.2002, s. 1).

([4]) 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).

([5]) 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).

PRÍLOHA III

TABUĽKA ZHODY

Smernica (EÚ) 2016/1148	Táto smernica
článok 1 ods. 1	článok 1 ods. 1
článok 1 ods. 2	článok 1 ods. 2
článok 1 ods. 3	–
článok 1 ods. 4	článok 2 ods. 12
článok 1 ods. 5	článok 2 ods. 13
článok 1 ods. 6	článok 2 ods. 6 a 11
článok 1 ods. 7	článok 4
článok 2	článok 2 ods. 14
článok 3	článok 5
článok 4	článok 6
článok 5	–
článok 6	–
článok 7 ods. 1	článok 7 ods. 1 a 2
článok 7 ods. 2	článok 7 ods. 4
článok 7 ods. 3	článok 7 ods. 3
článok 8 ods. 1 až 5	článok 8 ods. 1 až 5
článok 8 ods. 6	článok 13 ods. 4
článok 8 ods. 7	článok 8 ods. 6
článok 9 ods. 1, 2 a 3	článok 10 ods. 1, 2 a 3
článok 9 ods. 4	článok 10 ods. 9
článok 9 ods. 5	článok 10 ods. 10
článok 10 ods. 1, 2 a 3 prvý pododsek	článok 13 ods. 1, 2 a 3
článok 10 ods. 3 druhý pododsek	článok 23 ods. 9
článok 11 ods. 1	článok 14 ods. 1 a 2
článok 11 ods. 2	článok 14 ods. 3
článok 11 ods. 3	článok 14 ods. 4 prvý pododsek písm. a) až q) a písm. s) a ods. 7
článok 11 ods. 4	článok 14 ods. 4 prvý pododsek písm. r) a druhý pododsek
článok 11 ods. 5	článok 14 ods. 8
článok 12 ods. 1 až 5	článok 15 ods. 1 až 5
článok 13	článok 17
článok 14 ods. 1 a 2	článok 21 ods. 1 až 4
článok 14 ods. 3	článok 23 ods. 1
článok 14 ods. 4	článok 23 ods. 3
článok 14 ods. 5	článok 23 ods. 5, 6 a 8

Smernica (EÚ) 2016/1148	Táto smernica
článok 14 ods. 6	článok 23 ods. 7
článok 14 ods. 7	článok 23 ods. 11
článok 15 ods. 1	článok 31 ods. 1
článok 15 ods. 2 prvý pododsek písm. a)	článok 32 ods. 2 písm. e)
článok 15 ods. 2 prvý pododsek písm. b)	článok 32 ods. 2 písm. g)
článok 15 ods. 2 druhý pododsek	článok 32 ods. 3
článok 15 ods. 3	článok 32 ods. 4 písm. b)
článok 15 ods. 4	článok 31 ods. 3
článok 16 ods. 1 a 2	článok 21 ods. 1 až 4
článok 16 ods. 3	článok 23 ods. 1
článok 16 ods. 4	článok 23 ods. 3
článok 16 ods. 5	–
článok 16 ods. 6	článok 23 ods. 6
článok 16 ods. 7	článok 23 ods. 7
článok 16 ods. 8 a 9	článok 21 ods. 5 a článok 23 ods. 11
článok 16 ods. 10	–
článok 16 ods. 11	článok 2 ods. 1, 2 a 3
článok 17 ods. 1	článok 33 ods. 1
článok 17 ods. 2 písm. a)	článok 32 ods. 2 písm. e)
článok 17 ods. 2 písm. b)	článok 32 ods. 4 písm. b)
článok 17 ods. 3	článok 37 ods. 1 písm. a) a b)
článok 18 ods. 1	článok 26 ods. 1 písm. b) a ods. 2
článok 18 ods. 2	článok 26 ods. 3
článok 18 ods. 3	článok 26 ods. 4
článok 19	článok 25
článok 20	článok 30
článok 21	článok 36
článok 22	článok 39
článok 23	článok 40
článok 24	–
článok 25	článok 41
článok 26	článok 45
článok 27	článok 46
príloha I bod 1	článok 11 ods. 1
príloha I bod 2 písm. a) podbody i) až iv)	článok 11 ods. 2 písm. a) až d)

Smernica (EÚ) 2016/1148	Táto smernica
príloha I bod 2 písm. a) podbod v)	článok 11 ods. 2 písm. f)
príloha I bod 2 písm. b)	článok 11 ods. 4
príloha I bod 2 písm. c) podbody i) a ii)	článok 11 ods. 5 písm. a)
príloha II	príloha I
príloha III body 1 a 2	príloha II bod 6
príloha III bod 3	príloha I bod 8